Multi-layered Regulation of Phishing Attacks – A Taiwan Case Study

A Thesis Submitted for the Degree of PhD to the University of Warwick

School of Law

Chuan-Chi, KUO

November 2014

ACKNOWLEDGEMENTS

This thesis would not have been possible without the assistance of many people.

First of all, I would like to record my gratitude to Professor Abdul Paliwala for his supervision and constant encouragement throughout my research. I am indebted to Professor Philip Leith and Professor John McEldowney for providing greatly crucial perspectives on this thesis. I would particularly like to thank the interviewees who took part in this research and also the people who have ever helped me with my study.

Finally, I would like to thank my family and my partner David for their love and full support. Most importantly, I would like to mention my mother, for whom this work is dedicated. Her pride in this achievement made all the effort worthwhile.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF DIAGRAMS

ABBREVIATION

ARO	Accessing Rate Online
APEC	Asia-Pacific Economic Cooperation
APJ	Asia Pacific/Japan
APNOW	Anti-Phishing Notification Window
APWG	Anti-Phishing Working Group
ARPANET	Advanced Research Projects Agency Network
CANTINA	Carnegie Mellon Anti-Phishing and Network Analysis Tool
C&C Server	Command and Control Server
CERT	Computer Emergency Response Team
CIB	Criminal Investigation Bureau
CoE	Council of Europe
CPIL	Switzerland’s Federal Code on Private International Law
CPPDP Law	Computer-Processed Personal Data Protection Law
CRS	Congressional Research Service
DDoS	Distributed Denial of Service
DHA	Directory Harvest Attack
DMCA	1998 U.S. Digital Millennium Copyright Act
DNS	Domain Name System or Server
ECHR	European Convention on Human Rights
ECOSOC	United Nations Economics and Social Council
ECSG	APEC Electronic Commerce Steering Group
EU	European Union
FIP	Fair Information Practices
FTC	Federal Trade Commission
G8	The Group of Eight
GG	The Basic Law for the Federal Public of Germany
G-ISAC	Government Information Sharing and Analysis Center
GLB	Gramm-Leach-Bliley Act
GUI	Graphical User Interface
G-SOC	Government Security Operation Center
HTCN	High Tech Crime Network
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICANN	The Internet Corporation for Assigned Names and Numbers
ICCPR	UN International Covenant on Civil and Political Rights

ICPO-INTERPOL	International Criminal Police Organization
ICST	Information and Communication Security Technology Center
IRC	Internet Relay Chat
IP	Internet Protocol
ISP	Internet Service Provider
MIC	The Market Intelligence & Consulting Institute
MLA	Mutual legal assistance
MOJ	The Ministry of Justice
NCC	The National Communications Commission
NCRP	National Central Reference Point
NICST	National Information and Communication Security Taskforce
NTD	New Taiwan Dollars
OECD	Organization for Economic Cooperation and Development
PDCA	Plan-Do-Check-Act
PEI	Public Education Initiatives
PIP Act	Personal Information Protection Act
PPC	Pay-Per-Click
UDHR	1948 Universal Declaration of Human Rights
UNICEF	Nations International Children's Emergence Fund
URL	Uniform Resource Locator
SMBs	Small and Medium-Sized Businesses
SMTP	Simple Mail Transfer Protocol
SNSs	Social Networking Sites
SOC	Security Operation Center
SPF	Sender Policy Framework
SQL	Structured Query Language
TAHR	Taiwan Association for Human Rights
TANet CERT	Taiwan Academic Network CERT
TAPWG	Taiwan Anti-Phishing Working Group
TCP	Transmission Control Protocol
TF-IDF	Term Frequency–Inverse Document Frequency
TOC Convention	UN Convention against Transnational Organized Crime
TWCERT/CC	Taiwan Computer Emergency Response Team / Coordination Center
TWIA	Taiwan Internet Association
TWNCERT	Taiwan National CERT
TWNIC	Taiwan Network Information Center
WEIS	Workshop on the Economics of Information Security
XSS	Cross-Site Scripting

GLOSSARY

Backdoor A method of bypassing normal authentication to secure illegal remote access to a computer

Botnet A zombie army constituted by multiple compromised computers that are exploited to perform extensive malicious activities, including phishing, spam, DDoS attack and click fraud

Click Fraud An act that purposely sends fraudulent clicks generated via automated technology methods, for example a bot, or via manual clicking on an ad without having any actual interest in that ad's link but only for the purpose of earn the per click fee for the advertiser

Cross-Site Scripting (XSS) A type of web application vulnerability which allows attackers to bypass the security mechanisms imposed on web content by browsers

Cybercrime Any criminal activity that takes place within or by using networks of electronic communication such as the Internet

Data Breach Any unintentional exposure, disclosure or loss of data

Domain Name System (DNS) A hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network

Distributed Denial of Service (DDoS) An assault on a network by using multiple computers those act as zombies and work together to send extensive fictitious messages abnormally to increase the amount of the targeted network to slow down or interrupt its service for a certain period

Computer Hacking An activity which intentionally access to or interference with computer systems without authorisation

Hypertext Markup Language (HTML) A standardized system for tagging text files to achieve font, color, graphic, and hyperlink effects on World Wide Web pages

Hypertext Transfer Protocol Secure (HTTP) A communications protocol for secure communication over a computer network, with especially wide deployment on the Internet

Internet Service Provider (ISP) A company that provides customers with access to the Internet and other related services, such as website building and virtual hosting, through connections using copper, wireless or fiber optics

JavaScript A scripting language and functional programming language which is primarily implemented as part of a web browser in order to provide enhanced user interfaces and dynamic websites

Malicious Software (Malware) Software programmes designed to damage or do other injurious actions on a computer system, for example, viruses, worms, Trojan horses, and spyware

Netizen Somebody who is a good citizen of an online community

Plan-Do-Check-Act (PDCA) An iterative four-step management method used in business for the control and continuous improvement of processes and products

Uniform Resource Locator (URL) A specific character string that constitutes a reference to a resource.

Simple Mail Transfer Protocol (SMTP) An Internet standard for email transmission across IP networks

Sender Policy Framework (SPF) An email validation system designed to prevent email spoofing by verifying envelope sender addresses

Social Engineering An art that relies on human interaction for the purpose of manipulating people into performing actions or giving away confidential information

Republic of China (ROC) Calendar The system of numbering years currently used in Taiwan. The first year of ROC Calendar is 1912, the founding year of the ROC. For example, 2013 is the 102nd year of the ROC. Taiwanese judgments in this thesis are described in the ROC year.

ABSTRACT

This research examines the regulation of phishing in Taiwan, particularly focusing on legal regulation but within a context of a multi-dimensional regulatory framework which also necessarily includes an examination of international regulation and the interaction between international and Taiwan regulatory interfaces given the transnational nature of phishing. Phishing is a malicious cyber activity which targets the acquisition of various types of confidential information by deception through the use of spoofed emails and/or websites. The increasing threat of phishing to information security has inspired a growing demand for regulation. Significant effort has been made in academic research and by industry to develop regulatory measures for phishing, which is dominated by technological work with comparatively little research on legal regulation. The current legal discussion of phishing, both international and Taiwan, very often concentrates on the criminal liability of phishers and pays little attention to the alternative role of law in the regulation of phishing. Thus this research suggests a broader approach to legal regulation that goes beyond criminal law and particularly addresses the role of information privacy law which constrains phishing by ensuring the protection of personal information. Phishing has posed crucial challenges to the traditional system in terms of both criminalization and legal enforcement. The solution that has been mostly addressed by the existing research is cooperation. As phishing is frequently a global phenomenon, this research suggests that an international approach involving coordination of legal standards and cross-border cooperation of law enforcement is necessary to tackle phishing, and also suggests that the fundamental step lies in a converged regulation of phishing consistent with its true context.

Weak legal enforcement is a major deterrent to the effectiveness of legal regulation which highlights a need for a broad form of regulation that goes beyond law. In addition, a successful phishing episode involves a complex of factors including not only weakness in law but also vulnerability of technical infrastructure, administrative system and user awareness. A single solution is thus unlikely to deal with phishing. This research therefore suggests a multi-dimensional regulatory framework comprising different countermeasures developed especially in the areas of law, technology, education, and institutional network. It examines the anti-phishing approach undertaken in Taiwan employing qualitative methods to supplement the doctrinal research. In the context of a shortage of Taiwan scholarship on this subject, the research provides a set of suggestions to Taiwan development of a multi-dimensional regulatory scheme.

CHAPTER 1 INTRODUCTION

1.1. Research Questions

This thesis examines the regulation of phishing in Taiwan from a perspective which focuses on law but within a context which also involves examination of other multi-dimensional forms of regulation such as technical, educational and institutional networking. Inevitably, because of the transnational nature of phishing, it is also necessary to examine the interaction between Taiwan and international regulatory interfaces. The main questions are: what kinds of regulation are we currently offered to tackle phishing and what kind of regulation can really help to combat phishing effectively?

Phishing, a term that first appeared in the 1990s, refers to malicious cyber activity which targets the acquisition of various types of confidential information, such as credit card or bank account details, usernames, passwords, or financial or personal sensitive information. Although the study of regulation has been long dominated by economists,[1] the concept of regulation has evolved and become a multi-disciplinary field.[2] This thesis adopts a broad concept of 'regulation', which is different from traditional top-down, command and control system[3] and is not limited to government intervention in the private domain[4] or a legal rule that implements that intervention[5]

[1] Robson, William Alexander (1962), *Nationalized industry and public ownership* (G. Allen & Unwin);Veljanovski, Cento (2010), 'Economic approaches to regulation', in Robert Baldwin, Martin Cave, and Martin Lodge (eds.), *The Oxford Handbook of Regulation* (Oxford: Oxford University Press), 17-38.

[2] Baldwin, Robert, Cave, Martin, and Lodge, Martin (2010), 'Introduction: Regulation—the Field and the Developing Agenda', in Robert Baldwin, Martin Cave, and Martin Lodge (eds.), *The Oxford Handbook of Regulation* (Oxford: Oxford University Press), 3-13.

[3] Trubek, David M and Trubek, Louise G (2007), 'New Governance & Legal Regulation: Complementarity, Rivalry, and Transformation', *Columbia Journal of European Law, Summer*.

[4] Mill, John Stuart (1848), 'Principles of Political Economy With Some of Their Applications to Social Philosophy. 1857', *George Routledge and Sons, Manchester*.

but refers to any form of force that constrains, controls or adjusts certain behaviour or activity. In the context of phishing, ‘regulation’ involves any force that makes it possible to prevent phishing or which helps to diminish the potential damage which phishing is likely to cause by increasing the cost or difficulty of performing phishing and/or making phishing attacks less productive. A regulation of phishing, in this sense, can be any form of countermeasures against phishing; for example, hard law and soft law, hardware and software what Lessig called ‘Code’,[6] network governance[7] such as administrative networking of domains and websites connected by public or private sectors, or education and training programmes.[8]

For the purposes of this thesis, the forms of regulation are categorized into four: law, technology, institutional network, and education. In particular, because of the transnational nature of phishing, it is necessary to consider both national and international regulation. The focus is on legal regulation, including national and international laws, both hard and soft law, law enforcement and other legal approaches that have been adopted against phishing, in order to provide a fuller picture of the regulation of phishing. Nevertheless, it is suggested that legal regulation must be considered in the context of other forms of regulation.

It is not easy to know the solutions that phishing really demands if we do not have an adequate understanding about the nature of phishing – how phishing is organized and practiced, the potential damage that phishing may cause, and why phishing can succeed. It is also necessary to consider the functions, limitations and interactions of different kinds of regulation, so that we can have a better idea of the extent to which each regulation is able to address phishing and the efforts that should be prioritized or improved to effectively combat phishing.

[5] Baron, David P (1989), 'Design of regulatory mechanisms and institutions', in Richard Schmalensee and Robert Willig (eds.), *Handbook of industrial organization* (2), 1347-447.

[6] Lessig, L (2006), *Code: version 2.0* (2 edn.: New York: Basic Books).

[7] Castells, Manuel (2011), 'Network Theory| A Network Theory of Power', *International Journal of Communication,* 5, 15.

[8] The scope of regulation will be further discussed in Chapter 7, section 7.3.1.

A number of factors have led to the selection of Taiwan as a case study. Taiwan has a well-developed information technology infrastructure, with many similarities to the developed East Asian countries. It also has a high incidence of phishing and a strong demand for effective regulation, but yet, it faces particular difficulties in establishing an effective regulatory regime. Also, as my home country, it has provided me with a good understanding of the situation and access to the necessary resources involved in this research.

As phishing is frequently a transnational phenomenon, apart from the primary domain of Taiwan, it is necessary to consider other jurisdictions and especially forms of cross-border cooperation. Therefore, this research includes exploration of global and Asia-Pacific regulatory regimes of personal data protection and the harmonization of legal standards between different levels. It also includes examination of the legal frameworks that have been developed against phishing or identity-related cybercrime nationally and internationally and the international initiatives that have been proposed to enhance cross-border investigation and prosecution.

To provide an analysis of the practical engagement of different stakeholders in Taiwanese anti-phishing work, it was considered necessary to conduct an empirical study through holding interviews with the experts selected from various fields to supplement the doctrinal research given the shortage of Taiwanese research-based literature on this subject. ‘Stakeholder’ herein refers to any person or entity which is, in certain aspects, directly related to phishing, such as potential victims, financial institutions, domain registrars or registries, ISPs (Internet services provider), CERTs (Computer Emergency Response Teams), technology industry, and law enforcement agencies.

This research involves examination of

a. What phishing is, how it works, and why it can be successful

b. Why Taiwan has been in the peculiar dilemma of combating phishing and why Taiwan's experience in regulating phishing is valuable to anti-phishing research

c. Whether Taiwanese laws, in particular the Criminal Code, are capable of adequately dealing with phishing and the extent to which they are able to address phishing

d. Why information privacy protection is important to the regulation of phishing

e. What specific requirements for personal information protection have arisen from phishing, how these requirements have been addressed in Taiwan legislation as well as the global and regional legal regimes, and the harmonization of national and international legal standards in relation to personal data protection

f. What challenges have been posed by phishing to legal systems and law enforcement and the legal responses that have been made, both nationally and internationally

g. Why a multi-dimensional regulatory framework is necessary to deal with phishing, how different forms of regulation function and interact and whether they are effective

h. What progress Taiwan has made to develop an anti-phishing scheme based on the joint efforts of various stakeholders, how and to what extent the major stakeholders engage in this work, how they assess the work, and what improvements may be required for future work

1.2. Related Research

It is necessary to examine the previous research efforts related to this subject before highlight the contribution that this thesis aims to make. The academic work on phishing has been diverse, and the book by Jakobsson and Myers[9] which provides an explicit analysis of phishing and its

[9] Jakobsson, Markus and Myers, Steven (2007), *Phishing and countermeasures: understanding the increasing problem of electronic identity theft* (John Wiley & Sons).

countermeasures can be a very useful starting point. Researchers have tried to understand the costs that phishing may incur,[10] the techniques employed by phishers,[11] the reasons why people fall for phish,[12] and who are more likely to fall victim.[13] Significant research efforts have been devoted to the development of phishing countermeasures within various spheres. Several researchers have provided an overview of different types of anti-phishing measures.[14] A variety of technical tools have been proposed to prevent phishing messages from reaching users by phishing email filters[15] or

[10] Anderson, Ross, et al. (2013), 'Measuring the Cost of Cybercrime', in Rainer Böhme (ed.), *The Economics of Information Security and Privacy*, 265-300;Herley, Cormac and Florencio, Dinei (2009), 'A profitless endeavor: phishing as tragedy of the commons', *Proceedings of the 2008 workshop on New security paradigms* (ACM), 59-70;Levi, Michael and Burrows, John (2008), 'Measuring the Impact of Fraud in the UK A Conceptual and Empirical Journey', *British Journal of Criminology,* 48 (3), 293-318;Myers, Steven (2006), 'Introduction to Phishing', in Markus Jakobsson and Steven Myers (eds.), *Phishing and countermeasures: understanding the increasing problem of electronic identity theft* (John Wiley & Sons).

[11] Bose, Indranil and Leung, Alvin Chung Man (2007), 'Unveiling the mask of phishing: threats, preventive measures, and responsibilities', *Communications of the Association for Information Systems,* 19;Claburn, Thomas (2010), ''Tabnapping' attack simplifies phishing ', *InformationWeek,* 25 May 2010;Emigh, Aaron (2005), 'Online identity theft: phishing technology, chokepoints and countermeasures', *ITTC Report on Online Identity Theft Technology and Countermeasures*;Grebb, Michael (2005), 'Crime: Crooks Get Behind Plow: 'Pharming' harvests a new crop of thieves', *Bank Technology News,* 1 March 2005;Holz, Thorsten, et al. (2008), 'Measuring and Detecting Fast-Flux Service Networks', *NDSS*;Irani, Danesh, et al. (2008), 'Evolutionary study of phishing', *eCrime Researchers Summit, 2008* (IEEE), 1-10;Karlof, Chris, et al. (2007), 'Dynamic pharming attacks and locked same-origin policies for web browsers', *Proceedings of the 14th ACM conference on Computer and communications security* (Alexandria, VA, USA: ACM), 58-71;McMillan, Robert (2006), 'Who or what is 'Rock Phish' and why should you care?', *PCWorld*. <http://www.pcworld.com/article/128175/article.html>, accessed September 16 2014;Milletary, Jason (2005), 'Technical trends in phishing attacks', (CERT Coordination Center, Carnegie Mellon University);Nazario, Jose and Holz, Thorsten (2008), 'As the net churns: Fast-flux botnet observations', *3rd International Conference on Malicious and Unwanted Software 2008 (MALWARE 2008)* (IEEE), 24-31;Parmar, Bimal (2012), 'Protecting against spear-phishing', *Computer Fraud & Security,* 2012 (1), 8-11;Stamm, Sid, Ramzan, Zulfikar, and Jakobsson, Markus (2007), 'Drive-by pharming', in Hideki Imai and Gullin Wang (eds.), *Information and Communications Security* (Springer), 495-506;Vijayalekshmi, S and Rabara, S Albert (2010), 'Fending finanicial transaction from phishing attack', *The 2nd International Conference on Trendz in Information Sciences & Computing (TISC), 2010* (Chennai, India: IEEE), 171-75.

[12] Bakhshi, Taimur, Papadaki, Maria, and Furnell, Steven (2009), 'Social engineering: assessing vulnerabilities in practice', *Information management & computer security,* 17 (1), 53-63;MacEwan, Neil (2013), 'A Tricky Situation: Deception in Cyberspace', *The Journal of Criminal Law,* 77 (5), 417-32;Workman, Michael (2008), 'Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security', *Journal of the American Society for Information Science and Technology,* 59 (4), 662-74.

[13] Ademaj, Ilir and Schuck, Amie M. (2009), 'Internet security: Who is leaving the 'virtual door' open and why?', *First Monday,* 14 (1), 1-1;Kumaraguru, Ponnurangam, et al. (2008), 'Lessons from a real world evaluation of anti-phishing training', *eCrime Researchers Summit, 2008* (IEEE), 1-12;Martin, Tim (2009), 'Phishing for answers: Factors influencing a participant's ability to categorize email', *Comput. Changing World, Portland, OR*;Sheng, Steve, et al. (2010), 'Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, USA: ACM), 373-82.

[14] Bose and Leung (2007), op. cit;Emigh (2005), op. cit;Hong, Jason (2012), 'The state of phishing attacks', *Communications of the ACM,* 55 (1), 74-81;Huang, Huajun, Tan, Junshan, and Liu, Lingxi (2009), 'Countermeasure techniques for deceptive phishing attack', *International Conference on New Trends in Information and Service Science (NISS'09)* (Beijing, China: IEEE), 636-41;Jakobsson and Myers (2007), op. cit;Purkait, Swapan (2012), 'Phishing counter measures and their effectiveness - literature review', *Information Management & Computer Security,* 20 (5), 382-420.

[15] Abu-Nimeh, Saeed, et al. (2007), 'A comparison of machine learning techniques for phishing detection', *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (Pittsburgh, PA, USA: ACM), 60-69;Basnet,

email sender authentication[16] or block phishing websites through the use of anti-phishing toolbars[17] or heuristic-based classification by URL features[18] or website content.[19] Some researchers have

Ram, Mukkamala, Srinivas, and Sung, Andrew H (2008), 'Detection of phishing attacks: A machine learning approach', in Bhanu Prasad (ed.), *Soft Computing Applications in Industry* (Springer), 373-83;Bergholz, André, et al. (2010), 'New filtering approaches for phishing email', *Journal of computer security,* 18 (1), 7-35;Ceesay, Ebrima N (2008), 'Mitigating phishing attacks: a detection, response and evaluation framework', (University of California at Davis);Chandrasekaran, Madhusudhanan, Narayanan, Krishnan, and Upadhyaya, Shambhu (2006), 'Phishing email detection based on structural properties', *NYS Cyber Security Conference*, 1-7;Fette, Ian, Sadeh, Norman, and Tomasic, Anthony (2007), 'Learning to detect phishing emails', *Proceedings of the 16th international conference on World Wide Web* (Banff, Alberta, Canada: ACM), 649-56;Fette, Sadeh, and Tomasic (2007), op. cit;Islam, Rafiqul and Abawajy, Jemal (2013), 'A multi-tier phishing detection and filtering approach', *Journal of Network and Computer Applications,* 36 (1), 324-35.

[16] Adida, Ben, Hohenberger, Susan, and Rivest, Ronald L (2005), 'Fighting phishing attacks: A lightweight trust architecture for detecting spoofed emails', in Drew Dean and Markus Jakobsson (eds.), *DIMACS Workshop on Theft in E-Commerce: Content, Identity, and Service* (University, Piscataway, NJ, USA);Garfinkel, Simson L, et al. (2005), 'How to make secure email easier to use', in Wendy Kellogg, et al. (eds.), *Proceedings of the SIGCHI conference on Human factors in computing systems* (Portland, OR, USA: ACM), 701-10;Herzberg, Amir (2009b), 'DNS-based email sender authentication mechanisms: A critical review', *Computers & security,* 28 (8), 731-42;Lininger, Rachael and Vines, Russell Dean (2005), *Phishing: cutting the identity theft line* (John Wiley & Sons);Watson, Brett (2004), 'Beyond Identity: Addressing Problems that Persist in an Electronic Mail System with Reliable Sender Identification', *The First Confernece on Email and Anti-Spam (CEAS)* (Mountain view, California, USA).

[17] Apple 'Safari: phishing website warning', <http://support.apple.com/kb/PH17210>, accessed August 15 2014;Chou, Neil, et al. (2004), 'Client-Side Defense Against Web-Based Identity Theft', in Clifford Neuman, Michael Reiter, and Dan Boneh (eds.), *The 11th Annual Network and Distributed System Security Symposium (NDSS Symposium 2004)* (San Diego, California, USA);Google 'Google safe browsing for firefox', <http://www.google.com/tools/firefox/safebrowsing/>, accessed August 15 2014;Kirda, Engin and Kruegel, Christopher (2005), 'Protecting users against phishing attacks with antiphish', *29th Annual International Computer Software and Applications Conference (COMPSAC)* (1; Hong Kong, China: IEEE), 517-24;McAfee 'McAfee SiteAdvisor', <http://www.siteadvisor.com/howitworks/index.html>, accessed August 16 2014;Microsoft 'SmartScreen Filter', <http://www.microsoft.com/en-gb/security/online-privacy/smartscreen.aspx>, accessed August 15 2014;NETCRAFT 'Netcraft anti-phishing toolbar', <http://toolbar.netcraft.com/>, accessed August 15 2014.

[18] Alsalman, Rami (2012), 'MALURLS: A Lightweight Malicious Website Classification Based on URL Features', *Journal of Emerging Technologies in Web Intelligence,* 4 (2), 128-33;Garera, Sujata, et al. (2007), 'A framework for detection and measurement of phishing attacks', in Christopher Kruegel (ed.), *Proceedings of the 2007 ACM workshop on Recurring malcode* (Alexandria, VA, USA: ACM), 1-8;Hsu, Cheng-Hsin, Wang, Polo, and Pu, Samuel (2011), 'Identify fixed-path phishing attack by STC', in Vidyasagar Potdar (ed.), *Proceedings of the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference* (Perth, Australia: ACM), 172-75.

[19] Chen, Kuan-Ta, et al. (2009), 'Fighting phishing with discriminative keypoint features', *Internet Computing, IEEE,* 13 (3), 56-63;Chen, Teh-Chung, Dick, Scott, and Miller, James (2010), 'Detecting visually similar Web pages: Application to phishing detection', *ACM Transactions on Internet Technology (TOIT),* 10 (2), 5;Liu, Wenyin, et al. (2006), 'An antiphishing strategy based on visual similarity assessment', *Internet Computing, IEEE,* 10 (2), 58-65;Ludl, Christian, et al. (2007), 'On the effectiveness of techniques to detect phishing sites', in Bernhard M. Hämmerli and Robin Sommer (eds.), *Detection of Intrusions and Malware, and Vulnerability Assessment* (4579: Springer), 20-39;Medvet, Eric, Kirda, Engin, and Kruegel, Christopher (2008), 'Visual-similarity-based phishing detection', *Proceedings of the 4th international conference on Security and privacy in communication netowrks* (Istanbul, Turkey: ACM), 22;Nirmal, K, Ewards, SE Vinodh, and Geetha, K (2010), 'Maximizing online security by providing a 3 factor authentication system to counter-attack'Phishing'', *2010 International Conference on Emerging Trends in Robotics and Communication Technologies (INTERACT)* (IEEE), 388-92;Pan, Ying and Ding, Xuhua (2006), 'Anomaly based web phishing page detection', in Bob Werner (ed.), *22nd Annual Computer Security Applications Conference (ACSAC'06)* (Miami Beach, Florida, USA IEEE), 381-92;Wenyin, Liu, et al. (2005), 'Detection of phishing webpages based on visual similarity', *Special interest tracks and posters of the 14th international conference on World Wide Web* (Chiba, Japna: ACM), 1060-61;Xiang, Guang and Hong, Jason I (2009), 'A hybrid phish detection approach by identity discovery and keywords retrieval', *Proceedings of the 18th international conference on World wide web* (Madrid, Spain: ACM), 571-80;Zhang, Yue, Hong, Jason I, and Cranor, Lorrie F (2007a), 'Cantina: a content-based approach to detecting phishing web sites', *Proceedings of the 16th international conference on World Wide Web* (Banff, AB, Canada: ACM),

focused on the strategy of ‘notice-and-takedown’ to remove phishing websites as soon as they are detected to break the chain of a phishing attack.[20] Teaching users to spot spoofed emails or websites and enabling them to engage in online secure behaviours by education or training is another important method proposed by researchers to combat phishing.[21] While nearly all the proposed methods claimed to have shown very good performance in combating phishing, some researchers have tried to assess the usability and effectiveness of phishing countermeasures, including technical tools,[22] education[23] and takedown strategy,[24] and indicate various weaknesses

639-48;Zhang, Haijun, et al. (2011), 'Textual and visual content-based anti-phishing: a Bayesian approach', *Neural Networks, IEEE Transactions on,* 22 (10), 1532-46.

[20] Moore, Tyler and Clayton, Richard (2007), 'Examining the impact of website take-down on phishing', *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (Pittsburgh, PA, USA: ACM), 1-13;--- (2008), 'The consequence of non-cooperation in the fight against phishing', *eCrime Researchers Summit, 2008* (IEEE), 1-14;--- (2009), 'The impact of incentives on notice and take-down', in M. Eric Johnson (ed.), *Managing Information Risk and the Economics of Security* (Springer), 199-223;Nero, Philip J, et al. (2011), 'Phishing: Crime that pays', *eCrime Researchers Summit, 2011* (San Diego, USA: IEEE), 1-10;NETCRAFT 'Phishing Site Takedown & Countermeasures', *Netcraft Inc.* <http://www.netcraft.com/anti-phishing/phishing-site-takedown/>, accessed August 15 2014.

[21] Jerram, Cate, et al. (2012), 'Why do some people manage phishing e-mails better than others?', *Information Management & Computer Security,* 20 (1), 18-28;Kumaraguru et al. (2008), op. cit;Kumaraguru, Ponnurangam (2009), *Phishguru: a system for educating users about semantic attacks* (ProQuest);Kumaraguru, Ponnurangam, et al. (2009), 'School of phish: a real-world evaluation of anti-phishing training', *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS)* (Google in Mountain View, CA, USA: ACM), 3;Kumaraguru, Ponnurangam, et al. (2010), 'Teaching Johnny not to fall for phish', *ACM Transactions on Internet Technology (TOIT),* 10 (2), 7;Robila, Stefan A and Ragucci, James W (2006), 'Don't be a phish: steps in user education', *ACM SIGCSE Bulletin* (38: ACM), 237-41;Sheng, Steve, et al. (2007), 'Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish', *Proceedings of the 3rd symposium on Usable privacy and security* (Pittsburgh, PA, USA: ACM), 88-99;Sheng et al. (2010), op. cit;von Solms, R. (2013), 'Phishing for phishing awareness', *Behaviour & Information Technology,* 32 (6), 584-93;Von Solms (2013), op. cit;Yang, Che-Ching, et al. (2012), 'Building an Anti-phishing Game to Enhance Network Security Literacy Learning', in Ignacio Aedo, et al. (eds.), *2012 IEEE 12th International Conference on Advanced Learning Technologies (ICALT)* (Rome, Italy: IEEE), 121-23.

[22] Aburrous, Maher, et al. (2010), 'Experimental case studies for investigating e-banking phishing techniques and attack strategies', *Cognitive Computation,* 2 (3), 242-53;Dhamija, Rachna, Tygar, J Doug, and Hearst, Marti (2006), 'Why phishing works', in Rebecca Grinter, et al. (eds.), *Proceedings of the SIGCHI conference on Human Factors in computing systems* (Montreal, Canada: ACM), 581-90;Downs, Julie S, Holbrook, Mandy B, and Cranor, Lorrie Faith (2006), 'Decision strategies and susceptibility to phishing', *Proceedings of the second symposium on Usable privacy and security* (ACM), 79-90;Egelman, Serge, Cranor, Lorrie Faith, and Hong, Jason (2008), 'You've been warned: an empirical study of the effectiveness of web browser phishing warnings', in Mary Czerwinski, Arnie Lund, and Desney Tan (eds.), *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy: ACM), 1065-74;Herzberg, Amir (2009a), 'Why Johnny can't surf (safely)? Attacks and defenses for web users', *Computers & Security,* 28 (1), 63-71;Schechter, Stuart E, et al. (2007), 'The emperor's new security indicators', *2007 IEEE Symposium on Security and Privacy* (Oakland, California, USA: IEEE), 51-65;Wu, Min, Miller, Robert C, and Garfinkel, Simson L (2006b), 'Do security toolbars actually prevent phishing attacks?', in Rebecca Grinter, et al. (eds.), *Proceedings of the SIGCHI conference on Human Factors in computing systems* (Montreal, Canada: ACM), 601-10;Zhang, Yue, et al. (2007b), 'Phinding phish: Evaluating anti-phishing tools', *Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS 2007)* (San Diego, CA, USA).

[23] Anandpara, Vivek, et al. (2007), 'Phishing IQ tests measure fear, not ability', in Sven Dietrich and Rachna Dhamija (eds.), *Financial Cryptography and Data Security* (Springer), 362-66;Davinson, Nicola and Sillence, Elizabeth (2010), 'It won't happen to me: Promoting secure behaviour among internet users', *Computers in Human Behavior,* 26 (6), 1739-47.

in different types of countermeasures Every countermeasure has its strengths and weaknesses which may prove that a single perfect solution may not exist. Therefore, it has been suggested by researchers that a combined approach incorporating strategies from multiple interfaces may be the only solution to phishing.[25]

However, in comparison with the above countermeasures, there are much fewer studies of legal approaches on this subject, most of which have concentrated on the examination of criminal laws in terms of liability rules and legal reforms.[26] A similar state of anti-phishing research development can be sensed in Taiwan too. While Taiwanese scholarship on phishing countermeasures could barely be found prior to 2008, with only a few research proposals of authentication protocol for spoofed emails and websites,[27] the existing scholarship which has increased in volume but is significantly dominated by the studies of technical methods for detection of phishing websites.[28]

[24] Moore and Clayton (2009), op. cit;Varghese, Thomas 'Phishing Site Takedown Services – Does this really prevent identity theft?', (updated 31 August 2008) <https://blogs.oracle.com/BornIdentity/entry/phishing_site_takedown_service>, accessed 10 July 2014.

[25] Lynch, Jennifer (2005), 'Identity theft in cyberspace: crime control methods and their effectiveness in combating phishing attacks', *Berkeley Tech. LJ,* 20, 259;McNealy, Jasmine E (2008), 'Angling for phishers: legislative responses to deceptive e-mail', *Comm. L. & Pol'y,* 13 (2), 275-300;Sullins, Lauren L (2006), 'Phishing for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft', *Emory Int'l L. Rev.,* 20, 397;Wilson, Carly and Argles, David (2011), 'The fight against phishing: Technology, the end user and legislation', *2011 International Conference on Information Society (i-Society)* (IEEE), 501-04.

[26] Almerdas, Suhail (2014), 'The Criminalisation of Identity Theft under the Saudi Anti-Cybercrime Law 2007', *Journal of International Commercial Law and Technology,* 9 (2), 80-93;Bainbridge, David (2007), 'Criminal law tackles computer fraud and misuse', *Computer Law & Security Review,* 23 (3), 276-81;Dinna, NMN, et al. (2007), 'Managing legal, consumers and commerce risks in phishing', *Proceedings of World Academy of Science Engineering and Technology* (26: ACM Press), 562-7;Granova, Anna and Eloff, JHP (2005), 'A legal overview of phishing', *Computer Fraud & Security,* 2005 (7), 6-11;Lynch (2005), op. cit;McGowan, Laura (2006), 'Criminal Law Legislation Update', *J. Crim. L.,* 71, 184;Mcnealy (2008), op. cit;Nappinai, NS (2009), 'Cyber crime law in india: Has law kept pace with emerging trends? an empirical study', *Journal of International Commercial Law and Technology,* 5 (1), 22-28.

[27] Chang, Kai-Jie and Chang, Chin-Chen (2007), 'An e-mail signature protocol for anti-spam work-in-progress', in Li Jianzhong, Lee Wang-Chien, and Fabrizio Silvestri (eds.), *Proceedings of the 2nd international conference on Scalable information systems* (Suzhou, China: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering)), 1-2;Fang, Wen-Pinn (2007), 'Visual Cryptography in reversible style', *The Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2007)* (1: IEEE), 519-24.

[28] Chen et al. (2009), op. cit;Hsu, Wang, and Pu (2011), op. cit;Huang, Chun-Ying, et al. (2010), 'Mitigate web phishing using site signatures', *TENCON 2010-2010 IEEE Region 10 Conference* (Fukuoka, Japan: IEEE), 803-08;Lee, Wei-Bin, et al. (2011), 'An Anti-phishing User Authentication Scheme without Using a Sensitive Key Table', in Xiamu Niu, et al. (eds.), *2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)* (Dalian, China: IEEE), 141-44;Lin, Chia-Chen and Chiang, Po-Hsuan (2009), 'A Novel Mutual Authentication Based on Data Embedding Technique', in Jeng-Shyang Pan, Yen-Wei Chen, and Lahmi C. Jain (eds.), *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'09)* (Kyoto, Japan: IEEE), 274-77;Lin, Min-Sheng, et al. (2013), 'Malicious URL filtering—A big data application', in Xiaohua Hu, et al. (eds.), *2013 IEEE*

Only one piece of scholarly work could be found that directly addresses the legal regulation of phishing, but this only focuses on criminal liability.[29] In 2010, Taiwan manifested its ambition to combat phishing through joint efforts of the stakeholders from various regulatory interfaces by introducing two important anti-phishing initiatives, Taiwan Anti-Phishing Working Group and Anti-Phishing Notification Window. This is a milestone in the progress of Taiwan's anti-phishing work but has not received any attention from researchers. There is a lack of research that examines the practical engagement of different stakeholders in current anti-phishing work.

Sheng et al.[30] conducted the first study that integrated the opinions of the experts from various areas on the state of phishing attacks, the countermeasures need to implemented, and the incentives of various stakeholders in relation to anti-phishing work by carrying out 31 semi-structured interviews. The field work that I have conducted is similar to Sheng's work in the sense that both invited the experts from different fields and sought their opinions on phishing countermeasures that have been implemented and should be complemented. However, the Sheng et al study represented a US-centric view and its focus was on where the efforts should be placed to achieve effective action by asking the experts to specifically prioritize the recommendations on a list compiled by the authors, whereas my study represented a view of Taiwan aiming to examine the role of each stakeholder in the fight against phishing through interviews by using the interview questionnaires designed individually for each interviewee given the differences in their working background.[31]

1.3. Research Contribution

International Conference on Big Data (Santa Clara, CA, USA: IEEE), 589-96.

[29] Hsueh, Chih-Jen (2013), 'Criminal Penalties for Phishing', *Soochow Law Review,* 24 (3), 149-85.

[30] Sheng, Steve, et al. (2009a), 'Improving phishing countermeasures: An analysis of expert interviews', *Proceedings of the 4th APWG eCrime Researchers Summit,* 2, 4.

[31] More discussion of the study of Sheng et al., see Chapter 7, section 7.8.2.

1.3.1. A fuller picture of legal regulation of phishing

Law has been a typical regulator prevalently adopted in both real and virtual world to constrain certain behaviours by setting rules and imposing sanctions on the rule violators. Legal prohibition is an essential element to make a phishing attacker accountable for his attempt, and law may also serve other roles in the regulation of phishing. The unique function of law in combating phishing should be properly addressed. However, after a review of the related work, we can find an apparent shortage of legal research on the regulation of phishing. The current legal debates over phishing mostly focus on legal reform for phishing or application of existing criminal rules to phishing but with inadequate understanding about the characteristics of phishing and little consideration of the complex legal nature of phishing. This thesis aims to contribute a fuller picture of legal regulation of phishing by exploring the compatibility of the elements of the relevant provisions and the conduct of phishing and investigating the effectiveness of law enforcement in order to understand the extent to which legal regulation is capable of dealing with phishing. Although this exploration is based on Taiwanese legal regulation, it also looks into the national laws in other domains and international laws, both hard and soft law, in relation to phishing and particularly addresses the harmonization of legal standards set up at different levels and legal enforcement cooperation across borders.

1.3.2. A broader legal regulation of phishing beyond criminal laws

Another contribution this thesis aims to make is to highlight the relationship between information privacy and phishing and provide an analysis of the role of personal information protection laws in combating phishing in multiple dimensions. As aforementioned, the current legal studies of phishing very often concentrate on the function of criminal laws. While criminal law has an important role in standard setting to determine the boundaries of permissible behaviour and penalize those who do not comply, its regulatory power over phishing is usually restricted by weak legal enforcement, which is especially true in the case of Taiwan. This thesis argues that phishing demands a broader thinking of legal regulation that goes beyond criminal laws and suggests that the role of substantial personal information protection should be properly addressed to achieve effective regulation of phishing.

1.3.3. Multi-dimensional regulatory framework of phishing

A successful phishing attack not only exposes the weakness in legal protection but also unveils the vulnerabilities existing in technical infrastructure, inadequate awareness and knowledge of information security, and weak administration of domain and websites. Legal solutions may be part of the answer; however, these alone are not able to adequately address the problem of phishing especially in the context of weak legal enforcement. This highlights a need for seeking a broader form of regulation that goes beyond laws. A specific contribution of this thesis is to propose a multi-dimensional regulatory framework which comprises four interacting forms of countermeasure: law, technology, education, and institutional network. Each form of regulation has its particular role in combating phishing and functions differently against each step of the process of a phishing attack.

Laws, especially criminal laws, have been a regulator employed to deter phishing attempts by imposing a threat of punishment on the perpetrator. Technology is important in the regulation of phishing, as it can physically constrain phishers from performing attacks through the codes embedded in the hardware or software. Institutional networks regulate phishing by interrupting the performance of phishing attacks through close connection and cooperation between different organizations involved. The best example of institutional network for phishing is notice-and-takedown strategy of phishing websites. Teaching users to spot phishing and act as educated users about information security is also an important measure to curb phishing activities, as it helps users to protect themselves and other users which in turn reduces the success probabilities of phishing attacks.

Although each form of regulation has its strengths and weaknesses, a combined approach incorporating different forms of regulation may be the best solution which maximums their regulatory power while minimizes the problems that may impede their effectiveness. However, it should be borne in mind that the proposed framework is not intended to be an elixir strategy but provide a basic model containing the key elements of developing forms of regulation.

1.3.4. An empirical analysis of experts' interviews

The thesis provides an analysis of the roles of different stakeholders in Taiwan's anti-phishing work by conducting an empirical study through holding interviews with the key persons selected from different fields, including legal, technological, and administrative experts, to learn about their practical engagement in the anti-phishing work and seek their expertise on the performance of the current work as well as their suggestions for future work. This is a small-scale field work, but is the first study that synthesizes the opinions of Taiwanese experts from different fields, and examines the efforts that various stakeholders have devoted and are expected to devote to the Taiwanese anti-phishing work.

1.4. Research Methodology

The goal of this research is to analyze the multi-dimensional regulation of phishing, with a particular focus on the legal regulation of cybercrime and personal information protection in Taiwan and the interaction between the regulatory interfaces on different levels. The examination of multi-dimensional regulatory schemes on national and international levels is primarily based on existing documents and resources. However, Taiwanese scholarship on the regulation of phishing, as I have mentioned in section 2.1, is largely dominated by the discussions of technology with very little attention to other dimensions. In order to provide a deeper understanding of a social phenomenon and shed light on this unexplored problem, it was hence decided to pursue a qualitative study to supplement the doctrinal research.[32]

1.4.1. Documentary and comparative analysis

In order to obtain a comprehensive understanding of how and to what extent phishing is regulated within different dimensions, a wide range of documentary materials, including, policy documents, legislation, case law and secondary literatures including academic papers, national and international newspapers, and Internet resources, were gathered and reviewed.

The Council of Europe Convention on Cybercrimes has provided a fundamental guide for both European and non-European countries in altering or formulating their national laws on cybercrime. Taiwan also used the Convention as a precedent in the large-scale legal amendment of the Criminal Code in 2003 which added a new chapter on the offences against computer use. The first data protection law of Taiwan was passed in 1995 largely built upon the OECD Guidelines (*Organization for Economic Cooperation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*). In addition, the enactment of the Personal Information Protection Act in 2010 incorporated several data protection principles set out by the EU Directive (*Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free*

[32] Creswell, John W (2013), *Research design: Qualitative, quantitative, and mixed methods approaches* (2 edn.: Sage). Silverman, David (2001), *Interpreting qualitative data: methods for analyzing talk, text and interaction* (London: Sage).

Movement of such Data) and adopted the APEC (Asia-Pacific Economic Cooperation) Privacy Principles for a greater harmonization with international standards of personal data privacy. Through conducting a comparative analysis, this research examines correlations among regulations between different interfaces – global, regional and Taiwan – especially in the aspect of the legal protection of personal data and criminal law.

1.4.2. Qualitative study in Taiwan

Background

As indicated above, the thesis is primarily based on existing documents and secondary resources, and the field work is only supplementary. Given this, combined with the limited time and resources available to the researcher, it was decided to conduct a small-scale field work, with the participation of eight interviewees in total. Nevertheless, each interviewee was representative of a very small cohort of stakeholders involved in anti-phishing work and was able to provide valuable qualitative information. Further research is intended to build on this valuable study by involving a larger cohort as well as to focus on the interaction between the various stakeholders. This field work was conducted between April and May 2009 and between September and October 2011.

Selection of sample

The primary objective in selecting the participants was to ensure that expertise in multiple perspectives about the regulation of phishing was well represented. Thus the participants were chosen from different fields to include legal, administrative and technological experts. For the purpose of anonymity, this research does not provide detailed information about the participants but only briefly describes each one’s background and explains the reason why they were chosen.

Three legal experts were selected; one is the principal lawmaker for the cybercrime laws of Taiwan enacted in 2003 and the other two are police officers from specialized investigation units dealing with Internet crime. The main reason of this selection was to learn about the legal regulation of phishing cases, including the making and application of legislation and the practical operation of the investigation and prosecution work. It is noteworthy that the lawmaker expert was also a prosecutor and now is executive of an online merchant. A variety of information could be learnt from this expert, including legislation application, prosecution of phishers, and the anti-phishing policy and measures that an online merchant usually takes. Two experts from different information security industries also provided their knowledge about the development and effectiveness of anti-phishing technology. These two industries were chosen because they are major companies for information security services and products in terms of market share that have been in existence for over ten years.

In order to acquire an understanding of how and to what extent an ISP engages in anti-phishing work, one participant was selected from the information security department of the leading ISP of Taiwan. The other two participants of the administrative area were chosen from the National Communications Commission of Taiwan (NCC) and the Taiwan Network Information Center (TWNIC). NCC is responsible for regulating the development of the communication and information industry and acts as the administrative supervisory authority of ISPs in Taiwan. TWNIC is a non-profit organization that oversees domain name registration and IP address allocation in Taiwan. In 2009, TWNIC was commissioned to administer the operation of TWCERT/CC (Taiwan Computer Emergency Response Team / Coordination Center)[33] between 2009 and 2012, which included the construction of TAPWG (Taiwan Anti-Phishing Working Group)

[33] TWCERT/CC was founded in September 1998 to coordinate the responses to computer security incidents and unity the system and network related resources to help website operators to detect potential vulnerabilities and improve the security of their websites. See: http://www.cert.org.tw/eng/index.html.

and APNOW (Anti-Phishing Notification Window). This selection aimed to learn about their involvement in the current anti-phishing work and the measures they have employed to control and manage the threat of phishing.

Data collection method

The phenomenon of phishing involves various perspectives of regulation which in fact go far beyond the researcher's knowledge background. In order to explore this phenomenon from multiple angles and gain insights into the experiences and opinions of those engaged in the regulatory work of phishing in different fields, the method of in-depth interviews was preferred.

Face-to-face semi-structured interviews were employed in this study, where the participants were asked open-ended questions by using an interview schedule questionnaire as a guide. To have a well understanding of the nature of the participants' work involved, I made a careful study of the organization for which each participant works beforehand. This study included the scale and power of the organizations and the responsibilities and obligations of these organizations concerning cybercrime and phishing. A separate check-list of questions was hence designed individually for each participant in accordance with their working background. The use of open-ended questions allowed the participants to answer more freely and widely in their own terms and as Denscombe notes, the information gathered is "more likely to reflect the full richness and complexity of the views held by the respondent."[34]

Having obtained the written consent of the participants, each interview was recorded on a voice file. These interviews lasted for an average of 90 minutes and were mostly conducted at the participants'

[34] Denscombe, Martyn (2010), *The Good Research Guide: For Small-Scale Social Research Projects: For small-scale social research projects* (4 edn.: McGraw-Hill International).

office or preferred location.

Key themes of the interview questionnaires

Within the overall variations in the questions, there were the following key themes:

Background information

Each interview began by asking the interviewees briefly to describe the background of their work, including their work content, their position and how long they have been in that position.

Involvement in anti-phishing work

The questions asked in what ways and to what extent the interviewees were engaged in the regulation of phishing. These questions sought to establish the practical experience of each interviewee of dealing with phishing and how they examine the effectiveness of their work in regulating phishing.

Cooperation or connection with the other stakeholders, both national and international

The questions explored how the institutions interviewed cooperate with other countries, organizations, or even their customers to combat phishing and how they follow up with law enforcement to track the phishers. These sought to establish the practices employed to build up connections between different regulatory bodies at both the national and international level on the issue of phishing.

Evaluation of the current anti-phishing work and suggestions for future work

The questions asked each interviewee about their view on the overall anti-phishing work that has been undertaken in Taiwan as well as their suggestions for the improvements of future work.

Data analysis

Having transcribed verbatim the audio recordings of the interviews, the next step was to analyse the interview data. A grounded theory approach was employed to seek connections within the data and develop a concept. The first stage was to explore the data, which involved reading and re-reading the transcripts to become thoroughly familiar with the data. This helps the researcher to stay closer to the data and thereby reduce the possibility of misinterpretations arising.[35]

The subsequent stage was the coding of the data. This was carried out manually. The code was systematically used to link items of data to the key themes related to the analysis. Colour coding was also used to give each category a colour indicating the relevant responses in the transcript. After the interview data had been coded and categorised, a follow-up analysis was then conducted to seek emerging patterns and connections between the codes and categories and so develop concepts from the data.

Ethical considerations

To ensure that all of the interviewees were fully aware of the purpose of this study and their rights regarding confidentiality and anonymity, each one was asked to provide their informed consent on a voluntary basis by signing a written Consent Form, which indicated the purpose of study, the main objective of the interview, the recording method, and the protection of data use and identity of the interviewees, before they participated in the study. All of the data collected from the interviewees could only be used for the specific purpose of the academic analysis. In addition, as the interviews involved issues of a potentially sensitive nature concerning the personal experiences and opinions

[35] Radnor, Hilary (2001), *Researching your professional practice* (Buckingham: Open).

of the participants in respect to phishing practices, the identity of the participants was kept confidential and the data were quoted anonymously.

Accordingly, to preserve their anonymity, the participants were referred to as follows: Interviewee A (criminal investigator A), Interviewee B (criminal investigator B), Interviewee C (the expert who was prosecutor and participated the lawmaking of the cybercrime law of Taiwan, Chief Information Security Officer (CISO) of an online merchant, and is now Chief Executive Officer (CEO) of an online merchant), Interviewee D (the expert from the ISP), Interviewee E (the expert from the TWNIC), Interviewee F (the expert from security software industry), Interviewee G (the expert from the NCC), and Interviewee H (the expert from anti-spam industry).

1.5. Thesis Structure

This chapter sets out the research questions and the research methodology, examines research related to this subject, and highlights the main contribution of this research.

Before the discussion of regulatory issue of phishing, first we need to know what phishing is, why it should be regulated, and why phishing can succeed. In that way we can have a better understanding of the nature and elements of phishing and a clear picture of the regulations which are demanded for deterring a successful phishing attack. Chapter 2 provides a fundamental understanding of phishing, including the damage that phishing may cause, the various techniques that have been prevalently employed in performing phishing, and more importantly, the key factors that enhance the success of phishing attacks combined with a brief overview of the corresponding measures.

Chapter 3 then examines the particularly difficult position of Taiwan in pursuing effective regulation of phishing which underlines the fact that Taiwan has been exposed to extremely high risk of phishing attacks and also phishing hosts. Chapter 3 provides a more detailed explanation of the reasons why Taiwan was chosen as a case study by highlighting the significance of Taiwan's experience in regulating phishing to obtain a better understanding of the difficulties, both general and specific and the direction for future improvement.

The examination of the legal regulation of phishing in Taiwan begins with the exploration of the Taiwanese legislation related to phishing, with a primary focus on the Criminal Code and the Personal Information Protection Act. Chapter 4 examines the extent to which the Criminal Code is able to deal with phishing by looking into the applicability of the current provisions to the conduct of phishing including the reforms introduced by legislation in 1997 and 2003. This chapter investigates the various legal arguments about the application of the Code to phishing and indicates the negative influence that these might have produced upon the regulation of phishing. This chapter also investigates the difficulty in prosecuting phishing attackers and particularly examines the dilemma of Taiwan in seeking mutual legal assistance and engaging in international cooperation between law enforcement agencies.

While effective law enforcement is difficult to achieve, phishing demands a broad thinking of legal regulation which goes beyond criminal law. Chapter 5 aims to underline the relationship between information privacy and phishing and contributes toward an analysis of the role of personal information protection laws in the regulation of phishing in multiple dimensions. This chapter looks into the legal frameworks that have been developed for protection of personal information on three levels, including global, Asia-Pacific region, and Taiwan national level, and examines the harmonization and interaction between three regulatory interfaces. This chapter particularly focuses on the examination of the capability of the Taiwanese personal information protection laws of adequately dealing with phishing.

Weak law enforcement has been the major deterrent to effective legal regulation of phishing. What challenges that phishing has actually posed to legal enforcement work and what legal responses have been made, both nationally and internationally, to address phishing and enhance cross-border law enforcement are the questions that Chapter 6 examines. The chapter particularly examines the national laws in different domains on criminalizing phishing and the international laws, including both hard and soft law, which have been developed to promote harmonization of legislation and cooperation in legal enforcement against phishing or identity-related cybercrimes.

Legal regulation, as a corrective measure to constrain phishing attacks, is only made possible if it can successfully increase the risk experienced by phishing perpetrators of being convicted. This is a tough task to achieve without mutual legal assistance and effective law enforcement cooperation. The restricted regulatory power of legal regulation suggests a demand for a broader form of regulation beyond law which covers all the multi-dimensional phishing countermeasures including law, technology, education and institutional network. Chapter 7 therefore looks at the other forms of regulation, including technology, education, and institutional network, especially in relation to notice-and-takedown strategies, and investigates their respective function, strengths as well as weaknesses. As there is no silver bullet to phishing, it is suggested that multi-dimensional regulatory schemes may be the only answer to phishing. This suggestion is reinforced by the examination of the development of Taiwan's anti-phishing work and the associated empirical study described above.

The concluding chapter revisits the research questions set out in this chapter and provides suggestions for the future development and research.

CHAPTER 2 NATURE OF PHISHING

Synopsis

This chapter draws a picture of phishing by looking at its context, structures and the attack techniques used in different types of phishing along with an examination of the cost phishing has caused and may incur to individuals, businesses and the societies. This chapter also investigates the key factors that enhance the success of phishing attacks and provides an overview of the measures that have been developed in academia, industry and government at national and international levels to respond to each factor in order to curb phishing activities.

2.1. Introduction

To study the regulatory issues of phishing, the fundamental step is to understand the object we attempt to regulate: phishing. This includes an examination of the following questions: what is phishing, what damages may phishing cause to us, how phishing attacks are usually organized and performed, and the most important one is, why phishing attacks can succeed. This chapter provides a general understanding of phishing and particularly looks into the key factors favorable for phishing attacks combined with a brief review of the related work and measures that have been developed in different respects to respond to phishing.

2.2. What is phishing

Phishing is a malicious attack by employing both social engineering and technical subterfuge which targets the acquisition of confidential information, ranging from financial or personally sensitive information to intellectual property or trade secrets, or even military information, from an individual, group or organization, usually in an attempt to profit from stolen information or exploit solicited data as a stepping stone for subsequent criminal purposes. The term 'phishing' is a variation of the word 'fishing', which was coined in the mid 1990's to describe the form of attacks launched by the hackers who managed to steal America Online (AOL) accounts by duping the AOL users into providing their passwords through a spoofed email or AOL's Instant Message. This word, as explained by Myers, arises from the fact that users, or phish, are lured by imitative communication to a hook that collects their confidential information.[36]

Over the last decade, phishing has become the most common and effective way to acquire personal information to aid in identity theft or other fraudulent purpose.[37] Phishers can easily move money from another person's bank account as long as they obtain that person's online banking credentials. They can also use stolen information, for example usernames or passwords used to logon to Internet service platforms such as eBay and Yahoo! Bid, to masquerade as the genuine account holders to sell nonexistent goods and thereby defraud buyers of their money.

[36] Jakobsson and Myers (2007), op. cit.

[37] Anderson, Keith B, Durbin, Erik, and Salinger, Michael A (2008), 'Identity theft', *The Journal of Economic Perspectives*, 171-92;Brody, Richard G, Mulig, Elizabeth, and Kimball, Valerie (2007), 'Phishing, pharming and identity theft', *Academy of Accounting & Financial Studies Journal,* 11 (3);Eisenstein, Eric M (2008), 'Identity theft: an exploratory study with implications for marketers', *Journal of Business Research,* 61 (11), 1160-72;Mercuri, Rebecca T (2006), 'Scoping identity theft', *Communications of the ACM,* 49 (5), 17-21;Wall, David (2007), *Cybercrime: The transformation of crime in the information age* (4: Polity).

APWG (Anti-Phishing Working Group), a global association that brings together industry, law enforcement, and government working on reduction and prevention of phishing scams and other cybercrimes through development of data resources, data standards and response systems for private and public sectors, in their quarterly phishing activity trends report indicated that financial and payment services continued to be the top two of the most targeted industries in the second half of 2009, accounting for 39 and 33 percent respectively.[38] Similarly, the statistics compiled by Symantec over 2009 revealed that the sector of financial brands was ranked the top sector for being spoofed in phishing attacks, accounting for 74 percent of the total, followed by the sector of ISP.[39] ISP account can be attractive targets because a great number of people are used to using the same authentication information for manifold accounts. This information may be further exploited to provide access to victims' other accounts, such as online banking. It can also be used as a key to open the door to the free web-hosting space included in these accounts to put up deceptive sites to launch further phishing attacks.

The fact that the brands associated with the financial sector are at the highest risk of being spoofed may suggest a fact that most phishing attacks are motivated by financial gain, as the data obtained from the websites providing financial or payment services, for example credit card details or online banking login information, are more likely to yield financial profit in direct way. Although a majority of phishing activities are driven by financial gain, the target of phishing is obtainment of sensitive information which may not necessarily bring financial or property gain. Therefore the essence of phishing is misconduct against information security, rather than property. This distinction of a legal nature between phishing and other crimes that directly target a gain of property or profit

[38] APWG (2010a), 'Phishing Activity Trends Report: 4th Quarter 2009'. <http://docs.apwg.org/reports/apwg_report_Q4_2009.pdf>, accessed August 20 2014.

[39] Symantec (2010), 'Symantec Global Internet Security Threat Report –Trend for 2009', XV. <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf>, accessed August 20 2014.

should be clearly recognized in order to close the gaps between the existing laws and the effective regulation of phishing.[40]

2.3. The cost of phishing

The costs of crime can be disaggregated as losses, resources costs and externalities.[41] Resources costs are the expenditures in anticipation of and in response to the crime, and externalities refer to side effects from the commitment of the crime which are usually not reflected in market prices. Myers indicated that three types of cost should be taken into account when determining the phishing cost: direct, indirect, and opportunity costs.[42] According to Myers, the cost of phishing includes not only the value money or goods that are directly stolen through phishing but also those costs indirectly incurred to deal with or redress phishing attacks and the loss of potential customers for online commercial merchants as a result of users' refusal or mistrust of online services. In addition to the above costs, Anderson et al. suggested that defense cost which comprise the cost of security products, services and training as well as the effort put on detection, tracking, and law enforcement work should also be included in the cost of phishing.[43]

The Association for Payment Clearing Services (APACS) claimed that losses from phishing scams in the UK almost doubled in 2005 to £23.2 million, from £12.2 million in 2004.[44] Gartner found 3.6 million adults lost USD $3.2 billion to phishing attacks in the United States in the 12 months

[40] The individual legal nature of phishing and the difference between phishing and other identity-related crimes will be further explored in Chapter 6.

[41] Levi and Burrows (2008), op. cit.

[42] Myers (2006), op. cit.

[43] Anderson et al. (2013), op. cit.

[44] 'UK phishing fraud losses double', *Finextra*, 07 March 2006, http://www.finextra.com/news/fullstory.aspx?newsitemid=15013.

ending in August 2007.[45] RSA, in its online fraud report released in January 2014, estimated that the global loss to phishing attacks was over USD $5.9 billion in 2013.[46] However, as there is currently an absence of data from banks and other institutions that suffer damage, estimates on the damage caused by phishing may vary widely due to different methods used and assumptions of hidden costs such as damage to branding and loss that occur from distrust of online commercial services made by the organizations compiling and reporting statistics.[47] In addition, many companies may not report phishing losses because of fear of a loss of confidence from their consumers and investors.[48]

Phishing has posed increasing threat not only to Internet users but also to the corporations which provide online financial services such as online banking. More than monetary loss users may lose their confidence in the security of the online banking system and banks suffer damage to their reputation.[49] Litan reported that more than 42 percent of surveyed consumers stated that their concerns about online attacks such as phishing adversely affect their online shopping behaviours and more than 28 percent said online attacks have influenced their online banking activities.[50] The increase of phishing scams also poses severe threats to legitimate e-mail communications.[51]

[45] 'Gartner survey shows phishing attacks escalated in 2007; more than 3 billion lost to these attacks', Gartner, 17 December 2007, http://www.gartner.com/newsroom/id/565125.
[46] EMC (2014), *RSA Monthly Online Fraud Report – January 2014*, http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf.
[47] Herley and Florencio (2009), op. cit;Hong (2012), op. cit;Layton, Robert and Watters, Paul (2009), 'Determining provenance in phishing websites using automated conceptual analysis', *eCrime Researchers Summit, 2009* (IEEE), 1-7.
[48] Nykodym, Nick, et al. (2010), 'Cybercrime and Business: How to not Get Caught by the Online Phisherman', *J. Int'l Com. L. & Tech.,* 5, 252.
[49] Featherman, Mauricio S, Miyazaki, Anthony D, and Sprott, David E (2010), 'Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility', *Journal of Services Marketing,* 24 (3), 219-29;Furnell, Steven M (2004), 'Getting caught in the phishing net', *Network Security,* 2004 (5), 14-18.
[50] Litan, Avivah (2005), 'Increased phishing and online attacks cause dip in consumer confidence', *Gartner Study (June 2005)*.
[51] Ceesay (2008), op. cit;Wang, Jingguo, et al. (2009), 'Visual e-mail authentication and identification services: An investigation of the effects on e-mail use', *Decision Support Systems,* 48 (1), 92-102.

2.4. Phishing attack techniques

Emigh conducted a detailed analysis of the information flow in phishing attacks and the technology adopted by phishers at each step in the flow.[52] Bose and Leung also conducted a study of the channels and techniques that are widely employed by phishers.[53] In general, the performance of phishing attacks is achieved through two channels: phishing emails and malware.[54] A phishing attack consists of different elements and involves several steps. To provide a better understanding of phishing, this section examines the common techniques used in different types of phishing attacks.

2.4.1. Email-based attack

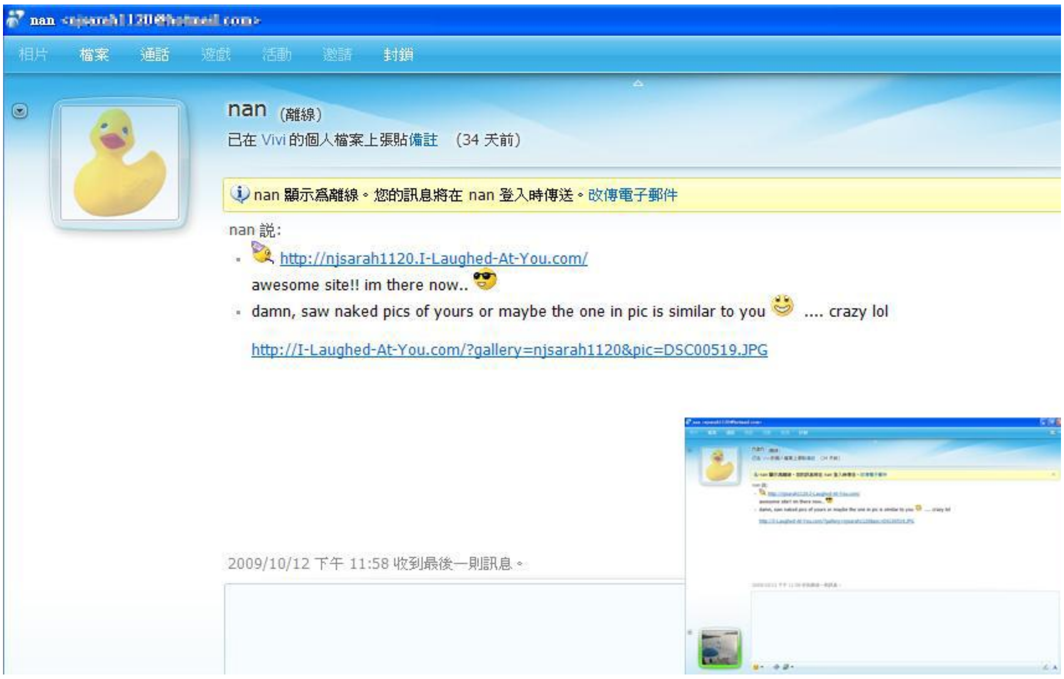
A typical social-engineering phishing attack is performed by sending an email[55] containing a web link which directs the unsuspecting recipients to a plausible website to tempt them to respond to the request by inputting their identifying information or other personally sensitive information. A phishing message may come from a non-acquaintance or pretend to be sent from a friend, a trustworthy organization. It may appear in the format of an MSN message (figure 2.1), a security reminder (figure 2.2), an advertising email (figure 2.3) or a greeting email.

[52] Emigh (2005), op. cit.

[53] Bose and Leung (2007), op. cit.

[54] 'Malware' is an abbreviation for 'malicious software', which refers to software programmes designed to damage or do other injurious actions on a computer system. Viruses, worms, Trojan horses, and spyware are common examples of malware.

[55] Phishing is primarily carried out through the use of email, but it can be done by using text messages via mobile phones, which is known as 'smishing'. A mobile user can also be targeted by 'vishing' which uses automated phone calls to entice the user to input personal information. It was indicated that smishing and vishing attacks have increased in the past several years and they frequently target customers of local banks. Moscaritolo, Angela (2010), 'FBI warns of SMS and phone-based phishing scams', *SC MAGAZINE*. <http://www.scmagazine.com/fbi-warns-of-sms-and-phone-based-phishing-scams/article/191565/>, accessed November 12 2014.



nan <njsarah1120@hotmail.com>

nan (離線)

已在 Vivi 的個人檔案上張貼備註 （34 天前）

nan 顯示為離線。您的訊息將在 nan 登入時傳送。改傳電子郵件

nan 說:

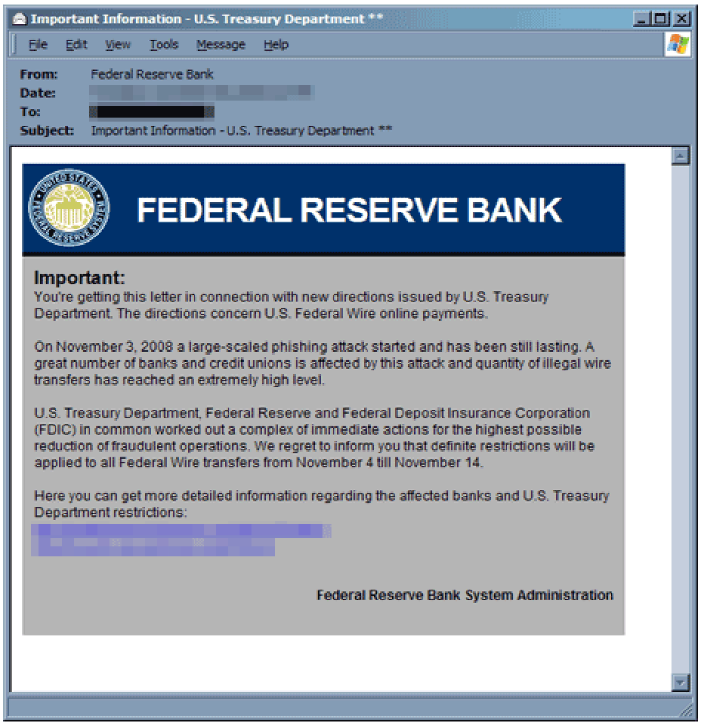
- http://njsarah1120.I-Laughed-At-You.com/
  awesome site!! im there now..
- damn, saw naked pics of yours or maybe the one in pic is similar to you .... crazy lol

  http://I-Laughed-At-You.com/?gallery=njsarah1120&pic=DSC00519.JPG

2009/10/12 下午 11:58 收到最後一則訊息。

Figure 2.1: Sample MSN Phishing Message[56]

[56] This MSN message was received on 12th October 2009 from a friend of the author.



From: Federal Reserve Bank
Date: [redacted]
To: [redacted]
Subject: Important Information - U.S. Treasury Department **

Important:
You're getting this letter in connection with new directions issued by U.S. Treasury Department. The directions concern U.S. Federal Wire online payments.

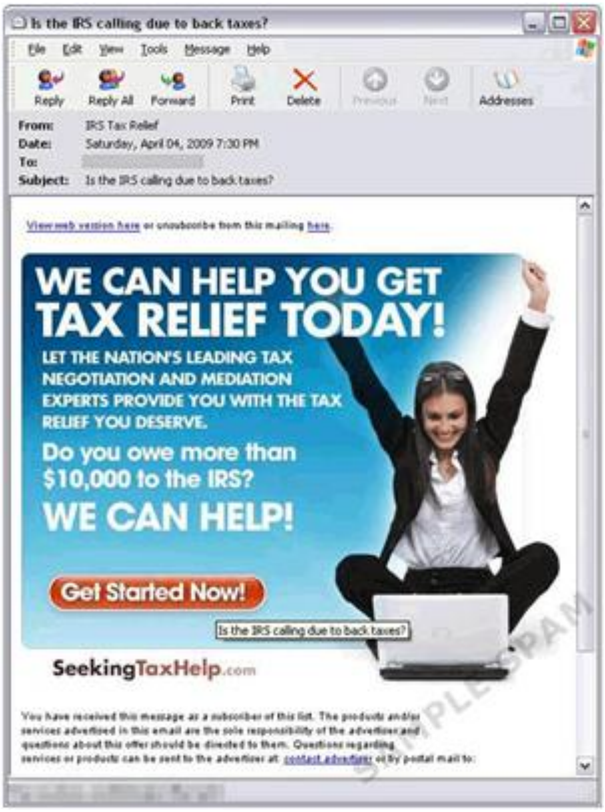
On November 3, 2008 a large-scaled phishing attack started and has been still lasting. A great number of banks and credit unions is affected by this attack and quantity of illegal wire transfers has reached an extremely high level.

U.S. Treasury Department, Federal Reserve and Federal Deposit Insurance Corporation (FDIC) in common worked out a complex of immediate actions for the highest possible reduction of fraudulent operations. We regret to inform you that definite restrictions will be applied to all Federal Wire transfers from November 4 till November 14.

Here you can get more detailed information regarding the affected banks and U.S. Treasury Department restrictions:
[redacted]

Federal Reserve Bank System Administration

Figure 2.2: Sample Spammed Security Reminder Email (Source: BLOG.TRENDMICRO.COM)


Is the IRS calling due to back taxes?
File
Edit
View
Tools
Message
Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses
WE CAN HELP YOU GET TAX RELIEF TODAY!
LET THE NATION'S LEADING TAX NEGOTIATION AND MEDIATION EXPERTS PROVIDE YOU WITH THE TAX RELIEF YOU DESERVE.
Do you owe more than $10,000 to the IRS?
WE CAN HELP!
Get Started Now!
Is the IRS calling due to back taxes?
SeekingTaxHelp.com
SAMPLE SPAM

From: IRS Tax Relief
Date: Saturday, April 04, 2009 7:30 PM
To: [redacted]
Subject: Is the IRS calling due to back taxes?

View web version here or unsubscribe from this mailing here.

You have received this message as a subscriber of this list. The products and/or services advertised in this email are the sole responsibility of the advertiser and questions about this offer should be directed to them. Questions regarding services or products can be sent to the advertiser at: contact advertiser or by postal mail to:

Figure 2.3: Sample Spammed Advertising Email (Source: BLOG.TRENDMICRO.COM)

An email-based phishing attack consists of two elements: a plausible email and a counterfeit web page, and it usually involves at least the following four steps.

Collecting email addresses

As the first step to launching an email-based phishing attack, it is a prerequisite to acquire the email addresses as many recipients as possible. In practice, email addresses can be massively collected in multiple ways. A great number of email addresses can be easily obtained via scanning websites, news groups, chat rooms or billboards that are open to the public by running particular software programs. Additionally, breaching computer security and hacking into the customer archives of mail servers is another way to gain myriads of customers’ email addresses through these mail servers.

Email generator software is designed for building email lists for marketing or advertising campaigns, but it can also be used by spammers to generate and search millions of email addresses directly from well-known mail servers. In addition, Dictionary Attack and Directory Harvest Attack (DHA) are also the methods that have been prevalently adopted in obtaining bulk email addresses. Dictionary Attack is a technique for alphabetically generating emails addresses in the hope that some addresses will prove correct. This attack is used to acquire email addresses by trying successively to guess all the words in a circumstantial list derived from a dictionary, a bible, etc.

Combined with Dictionary Attack, spammers have developed another attack technique called Directory Harvest Attack (DHA), which aims to collect a list of valid email addresses by sending thousands of generated email addresses to test the validity of individual email addresses according to the response of the targeted SMTP[57] server. The success of a DHA attack relies on the recipient of the email server, whereby an error message will be sent back if this email address is invalid or nonexistent.[58]

Composing scam emails

A phishing email is usually written in HTML[59] format, mimicking an email specifically used by a specific brand or entity; for example, a bank, credit card company, charity organization, online shopping company, etc. In order to make the email more plausible to convince the recipients, a spoof phishing email often uses the logo of a particular brand and copies the particular layout of the colour and graphics, even the character model, from the legitimate emails. A phishing email may be disguised under a variety of faces; for example a promotion email, a security reminder email or an account renewal email, which usually contains a web link that leads the recipients to a faux web page.

Irani et al.[60] conducted a study of phishing in a corpus of more than 380,000 phishing messages over 15 months. According to their analysis, a phishing email is usually composed of two major elements: the mail body (content) and the mail headers. The content is the main body of a phishing

[57] SMTP (Simple Mail Transfer Protocol) refers to an Internet standard for email transmission across IP networks.

[58] Bencsáth, Boldizsár and Vajda, István (2007), 'Efficient Directory Harvest Attacks and Countermeasures', *IJ Network Security,* 5 (3), 264-73.

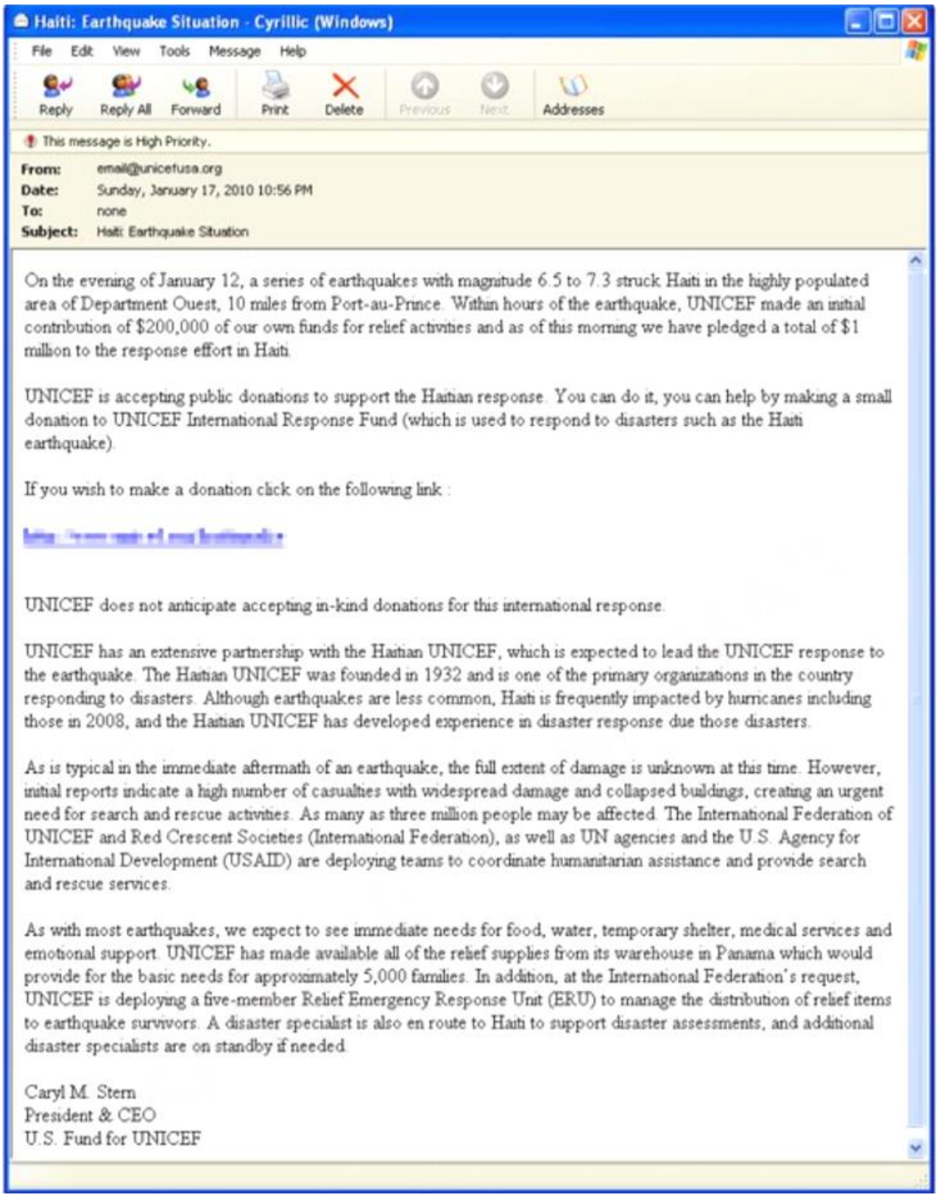
[59] HTML (Hyperlink Markup Language) is a standardized system for tagging text files to achieve font, color, graphic and hyperlink effects on World Wide Web pages.

[60] Irani et al. (2008), op. cit.

message used by phishers to trick the intended recipients which is usually designed to confuse, worry, upset, or excite recipients in order to prompt them to react immediately. It can be further split into two parts: a) *Cover* – the content which is produced to look like the message from the legitimate source and b) *Sting* – the part of the content that tempts recipients to take a particular action which is likely to cause pain to them as a result of a loss of personal credentials. The sting is commonly performed by requesting recipients to provide their confidential information through directly replying to the email or via a clickable URL that directs recipients to a bogus website.

The headers are the part of the message which is added by the mail clients, mail relays and spam-filters or virus-scanners which can be used to indicate the path of the message and how to unpack it. Mail clients add headers such as “To:”, “From:”, “Subject:” and some headers specified by the clients; for example, X-MSMail-Priority, X-Mailer, and X-MimeOLE.

Figure 2.4 shows a phishing email that impersonated the UNICEF International Response Fund to call for goods and donations to assist the victims of the Haiti earthquake. The cover of this email describes the work of UNICEF and purports relief fund raising for the victims of this large-scale accident to make recipients believe that this is a legitimate email sent from UNICEF. The sting can be found in Figure 2.4, where the phishing messages asks recipients to make a donation by following the link enclosed. The phisher adds “email@unicefusa.org” and “Haiti Earthquake Situation” to the headers and marks this email as High Priority.



This message is High Priority.

From: email@unicefusa.org
Date: Sunday, January 17, 2010 10:56 PM
To: none
Subject: Haiti: Earthquake Situation

On the evening of January 12, a series of earthquakes with magnitude 6.5 to 7.3 struck Haiti in the highly populated area of Department Ouest, 10 miles from Port-au-Prince. Within hours of the earthquake, UNICEF made an initial contribution of $200,000 of our own funds for relief activities and as of this morning we have pledged a total of $1 million to the response effort in Haiti.

UNICEF is accepting public donations to support the Haitian response. You can do it, you can help by making a small donation to UNICEF International Response Fund (which is used to respond to disasters such as the Haiti earthquake).

If you wish to make a donation click on the following link :

[illegible]

UNICEF does not anticipate accepting in-kind donations for this international response.

UNICEF has an extensive partnership with the Haitian UNICEF, which is expected to lead the UNICEF response to the earthquake. The Haitian UNICEF was founded in 1932 and is one of the primary organizations in the country responding to disasters. Although earthquakes are less common, Haiti is frequently impacted by hurricanes including those in 2008, and the Haitian UNICEF has developed experience in disaster response due those disasters.

As is typical in the immediate aftermath of an earthquake, the full extent of damage is unknown at this time. However, initial reports indicate a high number of casualties with widespread damage and collapsed buildings, creating an urgent need for search and rescue activities. As many as three million people may be affected. The International Federation of UNICEF and Red Crescent Societies (International Federation), as well as UN agencies and the U.S. Agency for International Development (USAID) are deploying teams to coordinate humanitarian assistance and provide search and rescue services.

As with most earthquakes, we expect to see immediate needs for food, water, temporary shelter, medical services and emotional support. UNICEF has made available all of the relief supplies from its warehouse in Panama which would provide for the basic needs for approximately 5,000 families. In addition, at the International Federation's request, UNICEF is deploying a five-member Relief Emergency Response Unit (ERU) to manage the distribution of relief items to earthquake survivors. A disaster specialist is also en route to Haiti to support disaster assessments, and additional disaster specialists are on standby if needed.

Caryl M. Stern
President & CEO
U.S. Fund for UNICEF

Figure 2.4: Sample Spammed Message (Source: BLOG.TRENDMICRO.COM)

Sending phishing emails

Phishing emails typically are massively forwarded and the recipients of the above emails are not specified to a particular group of people, which thereby increases the probability of success by quantity. While high volume of phishing email originating from a single host is likely to be intercepted by anti-spam devices, fewer messages coming from a larger number of compromised host are more likely to evade detection. Botnets hence become a very useful vehicle for phishers as they provide a distributed platform for sending phishing emails.

Botnets are widely used for a variety of cyber-attacks, such as Distributed Denial of Service (DDoS) attacks, malware dissemination, click fraud, stealing information, key-logging, mass spam distribution and phishing.[61] A bot is an automated software program that performs certain commands when it receives an input. Bots in reality are legitimate programs but have increasingly exploited for malicious purposes, which are mostly known as IRC (Internet Relay Chat) bots.[62] A botnet, which is also known as zombie network, is a collection of bot-loaded computers called *bot client* that allow the controller called *bot master* to control them remotely without the users' knowledge.[63] A single command may be either sent from a bot master to a bot client directly or transmitted by a command and control server (C&C server) to a bot client.

MessageLabs, an email security service provider, pointed out that over 83.2% of all spam worldwide were sent via botnets and one in 280.4 emails comprised a phishing attack in June 2009.[64] According to MessageLabs, Cutwail botnet, which was believed to be the largest botnet

[61] Bacher, Paul, et al. 'Know your enemy: Tracking botnets', <http://www.honeynet.org/papers/bots>, accessed 10 June 2014;Feily, Maryam, Shahrestani, Alireza, and Ramadass, Sureswaran (2009), 'A survey of botnet and botnet detection', in Rainer Falk, et al. (eds.), *The Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'09)* (Athens/Glyfada, Greece: IEEE), 268-73;Ianelli, Nicholas and Hackworth, Aaron (2005), 'Botnets as a vehicle for online crime', *CERT Coordination Center,* 1, 28;Milletary (2005), op. cit.

[62] The first IRC bot can be traced back to 1989, which was designed for the use of online chatting at the University of Oulu in Finland. Nevertheless, it has been abused by hackers for launching various malicious attacks. An IRC bot is formed when a computer virus or worm installs a backdoor program, such as a Trojan horse, that creates back doors of the infected PCs to offer hackers access. A hacker may search for compromised PCs with open ports and then install the bot program onto their hard drives once they have been located.

[63] Abu Rajab, Moheeb, et al. (2006), 'A multifaceted approach to understanding the botnet phenomenon', in Jussara Almeida, Virgilio Almeida, and Paul Barford (eds.), *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement* (Rio de Janeiro, Brazil: ACM), 41-52;Saha, Basudev and Gairola, Ashish (2005), 'Botnet: an overview', *CERT-In White Paper, CIWP-2005-05,* 240.

[64] MessageLabs (2009), 'Cutwail's bounce-back; instant messages can lead to instant malware'.

with a number of active bots between 1.5 and 2 million, pumped out 74 billion spam message per day.

Although sending emails to non-specific individuals, groups or organizations to mislead the recipients to bogus websites is still a common phishing phenomenon, it has become less effective due to the growing public awareness of phishing and the increasing sophistication of spam filtering. Therefore, the attack techniques of phishing have been constantly updated and developed. An apparent changing trend is an increase of spear-phishing campaigns.[65] Spear phishing is a targeted phishing attack that specializes in a particular group of people, company or entity rather than non-specific objects. While phishing messages typically appear to come from a well-known company or website with a broad membership base, the source of emails used in spear phishing is likely to be someone you trust; for example, your friend, colleague, or someone in a position of authority. The recipients are at higher risk of falling for a spear phishing attempt because of the highly credible email that has been specifically crafted for the recipients and the familiarity with the sender.[66] Statistics show that spear phishing response is 19%, compared to only 3-5% for the return to standard phishing emails.[67]

Constructing a bogus website

Duplication –

[65] Hong (2012), op. cit.

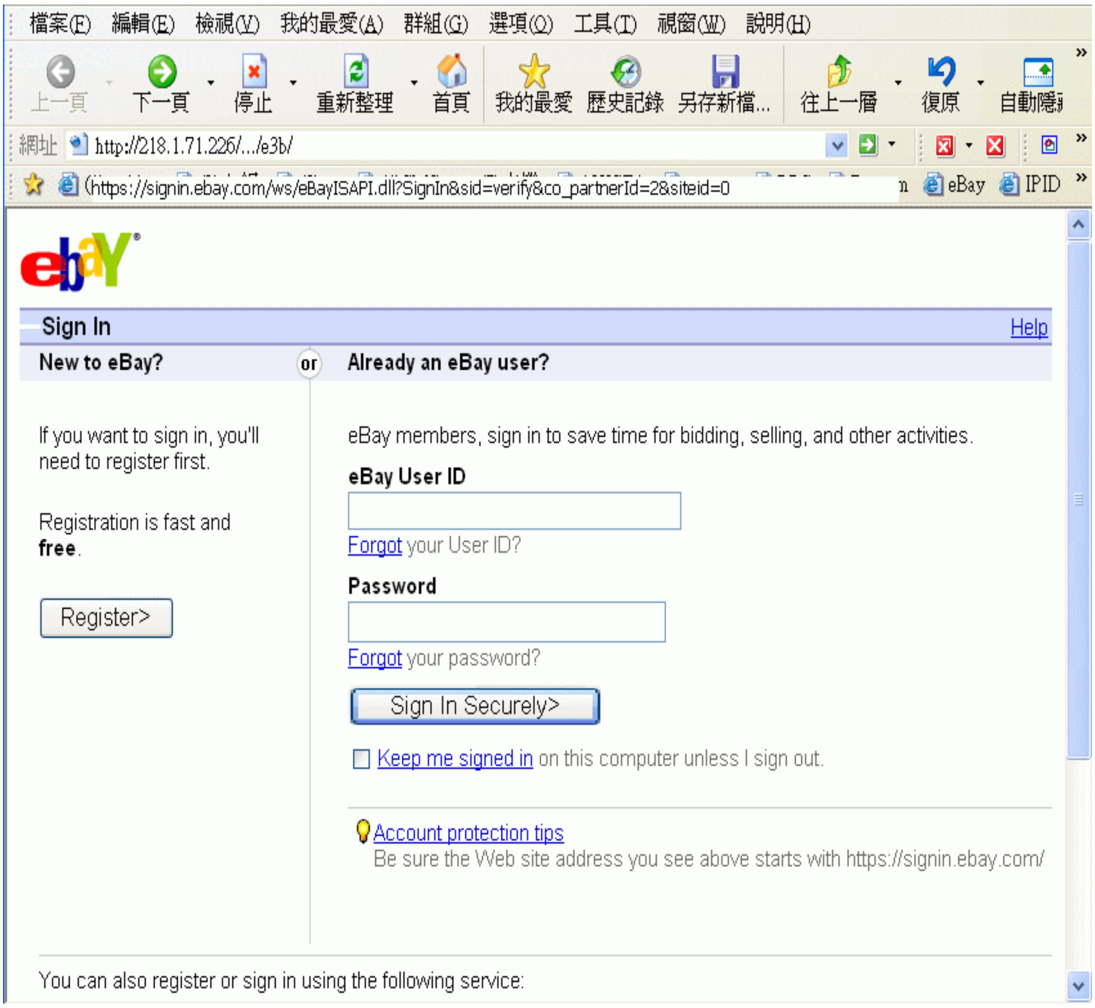
[66] Parmar (2012), op. cit.

[67] SearchITChannel (2006), 'Ready for some spear phishing', *TechTarget*. <http://searchitchannel.techtarget.com/feature/Ready-for-some-spear-phishing>, accessed September 17 2014.

A fraudulent website usually imitates the look of the legitimate site that it intends to copy, including the logo, graphics, fonts, layouts, and other related elements. In order to confuse users, phishers may register a similar looking URL to a genuine URL. For example, phishers may alter a legitimate URL by deleting or adding a single letter or replacing a letter or number with an analogical ones, such as l and 1 (one), O and 0 (zero), n and h, or v and w. Taking the instance of paypa“l”.com, it may be changed into paypa“1” (one).com to mix the spurious URL with the legitimate URL to spoof users.

In fact, it is not very difficult to detect the similar-looking URL if more attention is paid to the spelling of the words. However, users will be very likely to be misled if the URL of the phishing website looks exactly the same as the genuine one. An authentic-looking browser window can be created by using JavaScript[68] technique to disguise the real URL of the phishing website in the browser address bar to deceive users into thinking that they are at the correct website. Figure 2.5 is a sample of a phishing site that mimics the eBay login page. The URL that appeared in the browser address bar was the actual URL of a phishing site whereas the URL shown underneath the bar was created by JavaScript with the same-looking URL as the genuine one in order to hide the real address of the spoof site.

[68] JavaScript is a scripting language and functional programming language which is primarily implemented as part of a web browser in order to provide enhanced user interfaces and dynamic websites.



http://218.1.71.226/.../e3b/

(https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

Sign In

New to eBay?

If you want to sign in, you'll need to register first.

Registration is fast and **free**.

Already an eBay user?

eBay members, sign in to save time for bidding, selling, and other activities.

eBay User ID

Forgot your User ID?

Password

Forgot your password?

□ Keep me signed in on this computer unless I sign out.

Account protection tips
Be sure the Web site address you see above starts with https://signin.ebay.com/

You can also register or sign in using the following service:

Figure 2.5: Sample Phishing Website (Source: .WWW.NEO.COM.TW)

Botnets –

Botnets are often used by phishers to protect phishing websites from closure and protect themselves from being tracing back directly. *Rock Phish*, which first appeared in late 2004, has been a well-known and active group of phishers primarily focusing on European and U.S. financial institutions. This group has developed a variety of new attack techniques and purchased volumes of domain names to create unique URLs for its phishing messages to get past the blacklist-based filters. Rock-phish gangs operate by using botnets and causing them to serve as proxies that relay requests and responses to and from the hidden mothership, namely, the server which holds large number of counterfeit websites and stolen information. It was estimated that Rock Phish is responsible for between one-third and one-half of all phishing messages that are sent out on any given day.[69]

Fast-flux technology which is operated on botnets allowing a continual change of website IP addresses every few minutes has been widely employed in phishing attacks over the past few years.[70] A fast-flux network works by resolving a domain name to different sets of IP addresses over a short period and returning rapidly changing IP addresses. A browser connecting to the same phishing website every three minutes would actually be connecting to a different compromised computer.[71] The ever-changing list of IP addresses extends the lifetime of phishing websites,[72] making it nearly impossible to entirely locate all of the hosting machines and take them offline.

Lists of bot-infected computers is valuable and they can be rented out, sold or traded.[73] Phishing has become one of major financial sources for botnet owners, bringing an average income of millions of dollars to botnets owners per year. Phishers do not need to create their own fast-flux network, they can simply pay USD $1000 to $2000 to botnet owners per month for fast-flux hosting services.[74] According to Kaspersky Lab, Rock Phish cooperated with a botnet operator, Asprox, to upgrade their infrastructure for fast-flux compatibility in 2008.

Pay-Per-Click Ads –

[69] Mcmillan (2006), op. cit.

[70] Nazario and Holz (2008), op. cit.

[71] Bacher et al. (2005), op. cit;Holz et al. (2008), op. cit.

[72] Moore and Clayton (2009), op. cit.

[73] Wall (2007), op. cit.

[74] Namestnikov, Yuri (2009), 'The economics of botnets', *Analysis on Viruslist. com, Kaspersky Lab*.

Patience is always important for anglers when waiting for fish to take the bait, and likewise the phishers must wait for the recipients to link to the bogus website after sending out the lures, i.e. phishing emails or messages. Another change is that phishing attacks have been more active in tempting users to visit spoof websites by purchasing Pay-Per-Click (PPC) ads on top of search engines such as Google and Yahoo.

PPC ads are the ads shown on the right-hand side of a search result page when users type a keyword into search engines. PPC is one of the fastest ways to boost web traffic to a website, as relatively more people are used to relying on search engines to search websites and find the information that they need.[75] Promoting phishing websites through PPC ads not only greatly increases the click traffic to the fake websites but also significantly raises the risks that users will be deceived.

2.4.2. Malware-based attack

In addition to email-based attacks, phishing can be carried out through a technical subterfuge scheme by infecting users' PCs with malware or exploiting the browser vulnerability of websites.

Infecting PCs with malware

A technical-subterfuge phishing plants malware, in particular Trojan horses, onto Internet user's PCs to scan the stored information or intercept their activities or keystrokes and thereby obtain

[75] Juels, Ari, Stamm, Sid, and Jakobsson, Markus (2007), 'Combating click fraud via premium clicks', *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium* (Boston, MA. USA: USENIX Association), 1-10;Kshetri, Nir (2010), 'The Economics of Click Fraud', *IEEE Security & Privacy,* 8 (3), 45-53.

credit card credentials, passwords or other sensitive personal information directly. A Trojan horse or Trojan is a type of malware that has been widely used in phishing attacks. It is named after the wooden horse that infiltrated Troy, which is actually a piece of harmful software that masquerades as benign files used to trick users into loading or executing them on their system. As Trojans do not reproduce by infecting other files nor do they self-replicate, Trojans have to spread through user interaction such as opening a malicious email attachment or downloading and running a file from the websites that are embedded with malware. Users unwillingly download Trojans either by clicking on links which contains malicious code or even simply by visiting malicious injection URLs.

A Trojan can make several attacks on the infected host after it has been activated, ranging from irritating the users or damaging the host, such as deleting files, stealing data, or activating and spreading other malware. Trojans are also well known for their use in creating back doors of compromised hosts. By installing malware onto users' PCs, it may turn the compromised machines into members of botnet for subsequent criminal use.

In addition to opening PCs' Internet ports and exposing the ports to bot installation, Trojans can be used to steal data from infected PCs through key-logging interception or access to stored information. A variety of information, such as banking data, passwords or other sensitive information, will be automatically output to another computer controlled by the phishers for receiving data when victims input it on their PCs. Phishers may even directly access the data stored in a Trojan-infected PC if they can gain substantial control over it.

Milletary provided some examples of Trojans that are prevalent in phishing attacks.[76] Bancos, originally identified in July 2003, is a representative of phishing malwares that monitors Internet Explorer for specific bank URLs and attempts to capture account information. Bancos can overlay certain banking websites with a counterfeit one to trick users into disclosing their information. Bankash is the first known piece of malware that targets AntiSpyware.[77] It attempts to disable Microsoft anti-spyware program and steal online banking login information of targeted banks by using a keylogger or displaying a fake login page.

Exploiting the browser vulnerability of websites

A typical phishing attack is heavily based on a huge number of fake email messages claiming to be sent from trusted resources. However, the increasing sophistication of spam filtering driven by ISPs has made it more difficult to ensure that spoof emails reach the targeted objects successfully. Removing the email component, phishing techniques thus have been enhanced to abuse the vulnerabilities in web browsers that provide phishers with the ability to obfuscate URLs or install malware on users' machines. Exploitation of web browser vulnerabilities could allow attackers to create a pop-up window that overlays the address bar to hide the illegitimate URL of a phishing website or to change or replace content within the browser window containing the legitimate websites.[78]

A good example of exploitation of web browser vulnerabilities is 'in-session attack', which is carried out by making use of web-based fake alerts to convince the end users to provide their login

[76] Milletary (2005), op. cit.

[77] Broersma, Matthew 'Trojan Targets Microsoft's AntiSpyware Beta', <http://www.eweek.com/c/a/Security/Trojan-Targets-Microsofts-AntiSpyware-Beta/>, accessed 15 June 2014.

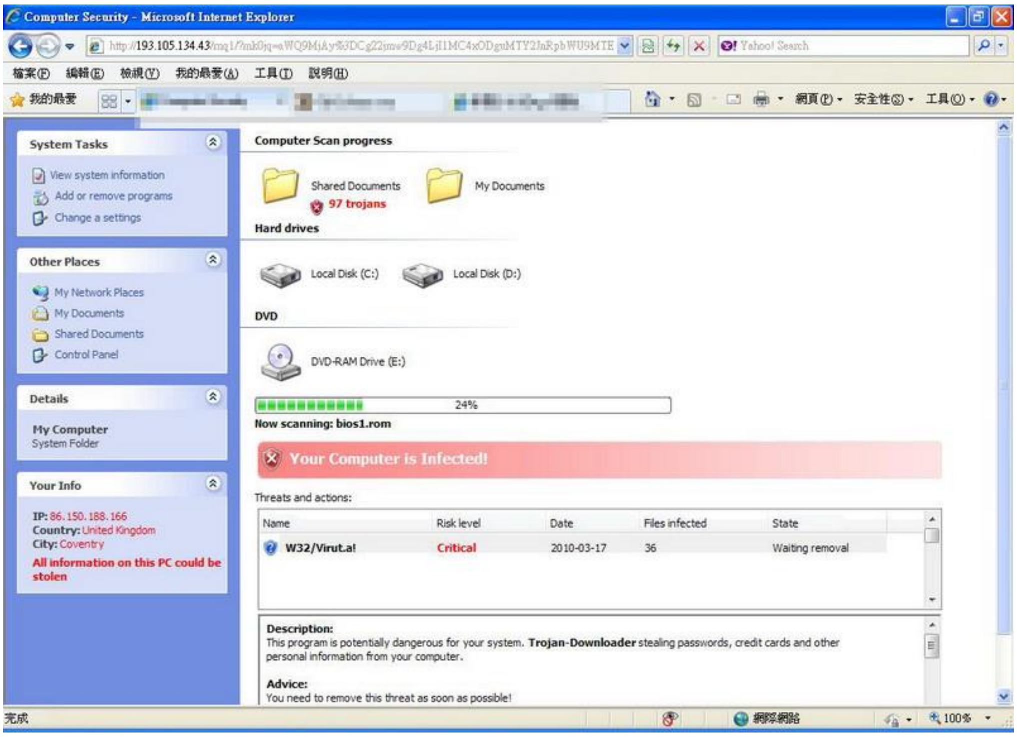
[78] Milletary (2005), op. cit.

information. In 2008, Trusteer found a JavaScript flaw in all leading browsers, such as Internet Explorer, Firefox, Safari, and Chrome, which allows a website to trace the footprint and check whether a user is currently logged onto another website.[79] Once a user is identified as being logged onto a website with malicious code injection, the said code would present a web-based pop-up window pretending to be from the website. It may ask users to complete a customer survey or ask users to retype their usernames or passwords by claiming that "Your login session has expired. Please sign in again" and thereby capture users' login credentials.[80]

A website with malicious code injection may also generate a fake security warning pop-up that cautions users that their computer has been infected by Trojan (see figure 2.6) and strongly prompt them to install the antimalware software it provides (see figure 2.7). However, there are in fact no Trojans infections but users will soon be the next victims of Trojans if they decide to click to install a Trojan that is masquerading as antimalware software.

[79] Trusteer (2008), 'In session phishing attacks', *Trusteer Research Paper*.

[80] Vijayalekshmi and Rabara (2010), op. cit.



Computer Scan progress

Shared Documents 97 trojans

Hard drives

DVD

Now scanning: bios1.rom

Your Computer is Infected!

IP: 86.150.188.166
Country: United Kingdom
City: Coventry
All information on this PC could be stolen

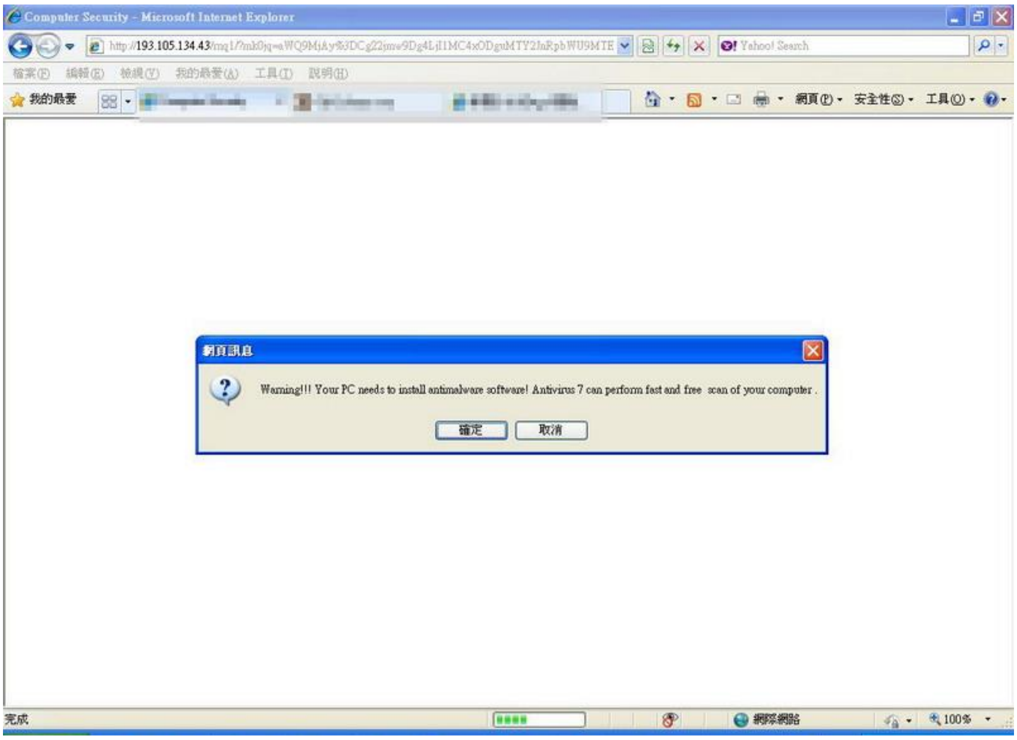
Threats and actions:

Name	Risk level	Date	Files infected	State
W32/Virut.a!	Critical	2010-03-17	36	Waiting removal

Description:
This program is potentially dangerous for your system. **Trojan-Downloader** stealing passwords, credit cards and other personal information from your computer.

Advice:
You need to remove this threat as soon as possible!

Figure 2.6: Fake spoofed infection warning pop-up (1)


Computer Security - Microsoft Internet Explorer
http://193.105.134.43/mq1/?mk0jq=aWQ9MjAy%3DCg22jmw9Dg4LjI1MC4xODguMTY2JnRpbWU9MTE
Yahoo! Search
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
網頁(P) 安全性(S) 工具(O)
網頁訊息
確定
取消
完成
網際網路
100%

Warning!!! Your PC needs to install antimalware software! Antivirus 7 can perform fast and free scan of your computer .

Figure 2.7: Fake spoofed infection warning pop-up (2)

2.4.3. Pharming

Pharming is an updated form of online fraud based upon phishing. Similarly, phishing and pharming rely on counterfeit websites in the same attempt to steal confidential information. A phishing attack is reliant on users clicking on an enticing link in fraudulent emails; however, through DNS cache[81] poisoning, a pharming attack re-directs victims to a fictitious website even if they type the right web address into their web browser.[82]

DNS cache poisoning is an attack on the Internet naming system by which pharmers direct users to a series of bogus websites by changing the routes from the domain names to the IP addresses and thereby dupe unsuspecting victims into divulging their confidential information. One of the first known pharming attack happened in early 2005. The domain name for a large New York ISP, Panix, was hijacked to point to a website in Australia. Pharming attacks not only threaten the personal information security of users but also causes adverse impact on the hijacked website, as the legitimate website can no longer be reached once the traffic flow has been re-directed and the original address has been moved to a new address.

The techniques used in DNS-based attacks have been constantly updated and sophisticated. Stamm et al. examined an attack termed *Drive-by Pharming* where attackers create a web page, which simply when viewed by the victim, changes the DNS setting on the victims' home broadband router.

[81] DNS servers are responsible for transferring letter-based website names, for example (www.google.com) into machine-understandable digits (125.13.213.1) to take users to the website of their choice. A DNS cache is a component that temporarily stores data about website names and their corresponding IP addresses so that future requests for data can be recalled quickly.

[82] Grebb (2005), op. cit.

The attackers can direct the victims' Internet traffic to the attackers' own websites by which acquire victims' confidential information.[83] Karlof et al. also described a new type of DNS attack -*Dynamic Pharming*. It works by sending victims a web document containing malicious JavaScript code which then exploits DNS vulnerability in browsers to hijack a legitimate session after authentication has taken place. A dynamic pharming can be used for a variety of malicious purposes; for example eavesdrop on sensitive content, forge transaction or sniff passwords.[84]

2.4.4. Tabnapping

Tabnapping, a new type of phishing techniques, was discovered and named by Aza Raskin in early 2010.[85] It works by replacing the contents and label of an open-but-not--active tab with a page designed to capture users' login information after they visit a hostile or compromised website.[86] Very commonly, Internet users work with multiple tabs. For example, a user might open a tab to Gmail, a news site, and an infected site. The infected site morphs into a fake Gmail login page when the user browsers the news site. The user may be unaware of this, or may assume that the initial login session has been timed out and retype login information when he returns to the tab of the duplicate Gmail login.[87]

2.5. The keys to successful phishing attacks and the corresponding

[83] Stamm, Ramzan, and Jakobsson (2007), op. cit.
[84] Karlof et al. (2007), op. cit.
[85] Aza Raskin worked as head of user experience at Mozilla Labs and lead designer for Firefox. Raskin's original tabnapping disclosure, see http://www.azarask.in/blog/post/a-new-type-of-phishing-attack.
[86] Claburn (2010), op. cit.
[87] TrendMicro 'Tabnapping: new phishing attack works through imposter browser tabs', (updated July 2010) <http://www.trendmicro.com/ftp/documentation/general/TRENDMICRO_JUL10/trendsetter_july10_tabnap.html>, accessed 16 June 2014.

measures[88]

Having obtained a picture of the components and tactics of phishing, we now need to understand the factors that assist in the performance of phishing attacks. Why phishing attackers can successfully hide themselves and dupe unsuspecting users into divulging their confidential information? What can we do to prevent a successful phishing attack from happening? This section aims to investigate the key factors leading to the success of phishing and the current corresponding measures proposed against them.

2.5.1. Transnational nature

The overwhelming majority of phishing attacks are operated from one country to another by taking advantage of the borderless nature of cyberspace. The transnational nature of phishing enables phishers to obscure their identity and location and to abuse inconsistent legal protection among different countries to impede investigation and prosecution, which poses a severe challenge to policing strategies.[89]

The role of laws against phishing usually involves the discussions of three dimensions: criminalization of phishing, harmonization of legal standards, and international cooperation of legal enforcement. Criminalization of phishing is a prerequisite to make phishing perpetrators liable for

[88] This section only provides a brief review of different types of scholarly work developed as a solution to respond to phishing attacks. This will be discussed in great detail in latter chapters.

[89] Broadhurst, Roderic (2006), 'Developments in the global law enforcement of cyber-crime', *Policing: An International Journal of Police Strategies & Management,* 29 (3), 408-33;Lovet, Guillaume (2009), 'Fighting Cybercrime: Technical, juridical and ethical challenges', *Virus Bulletin Conference* (Geneva, Switzerland), 63-76;Wall, David (2003), *Crime and the Internet* (Routledge).

their conducts. Several studies were generated to examine the phishing laws in various countries such as USA,[90] UK,[91] South Africa[92] Saudi Arabia,[93] India,[94] and Malaysia.[95] Instead of introducing a new provision specific to phishing, many countries incorporate phishing under their existing cybercrime laws or common laws in relation to spam, impersonation, theft or fraud. However, as phishing involves both social-engineering and technical-subterfuge schemes and usually involves overlaps of the elements of multiple offences, some studies argued that the existing legal framework is adequate to fully accommodate the conduct of phishing.[96]

Another major concern raised about legal solutions is the effectiveness of cross-border legal enforcement.[97] It is not possible to restrain the attempt of phishing attackers from legal perspective if they do not feel the risk of being caught and punished. The difference between legal provisions relating to phishing across jurisdictions nevertheless creates ‘safe havens’ for phishing attackers, and the anonymity characteristic of cyberspace enables phishers to flee easily from the track. Whether laws can curb phishing activities largely depends on successful prosecution of perpetrators, which can only be made by promoting the consistency and compatibility of the phishing laws between jurisdictions through the development of a set of common standards to be enforced and creation of expedient multilateral platform to facilitate international cooperation among legal systems.[98]

[90] Lynch (2005), op. cit;Mcnealy (2008), op. cit.

[91] Bainbridge (2007), op. cit;Mcgowan (2006), op. cit.

[92] Granova and Eloff (2005), op. cit.

[93] Almerdas (2014), op. cit.

[94] Nappinai (2009), op. cit.

[95] Dinna et al. (2007), op. cit.

[96] Dinna et al. (2007), op. cit;Granova and Eloff (2005), op. cit;Nappinai (2009), op. cit.

[97] Broadhurst (2006), op. cit;Cheng, Fa-Chang (2011), 'The Law Enforcement in Cyberspace Criminal: Focusing on the Experience between Taiwan and the United States', *2011 Third International Conference on Multimedia Information Networking and Security (MINES)* (Shanghai, China: IEEE), 577-80;Dinna et al. (2007), op. cit;Stevenson, Robert Louis B (2005), 'Plugging the" Phishing" Hole: Legislation Versus Technology', *Duke L. & Tech. Rev.,* 2005, 6-26;Sullins (2006), op. cit.

[98] Menon, Sundaresh and Siew, Teo Guan (2012), 'Key challenges in tackling economic and cyber crimes: Creating a multilateral platform for international co-operation', *Journal of Money Laundering Control,* 15 (3), 243-56;Sullins

Over the past decade, considerable progress has been made to develop a transnational legal instrument to respond to the threat of cybercrimes. The well-known examples include the United Nations Convention against Transnational Organized Crime and the Council of Europe Convention on Cybercrime. While these two international treaties provide a fundamental basis for the harmonization of the legal standards to deal with cybercrime, whether they can effectively regulate phishing remains a question.[99] In order to tackle the rise of cybercrime, significant efforts have also been made by several international organizations to coordinate actions between governments against cybercrime, for example the United Nations, OECD, G8 and APEC. The establishment of a 24/7 network is especially important to facilitate cybercrime investigation by speeding up communication through a single point of contact and authorizing the contact point to carry out certain investigation right away.

2.5.2. High availability of technical resources

The easy availability of phishing kits is also an important factor that enables flourishing phishing attacks.[100] The technical resources needed for launching phishing attacks such as pre-generated HTML pages for popular banks and online commerce entities, scripts for processing user input, email and proxy server lists, and even hosting services for phishing websites can be easily bought[101] or downloaded free of charge[102] through various sources. Some even provide "bulletproof" web

(2006), op. cit.

[99] Schjolberg, Stein and Ghernaouti-Helie, Solange (2011), 'A global treaty on cybersecurity and cybercrime', *Cybercrime Law*.

[100] Bose and Leung (2007), op. cit;Brody, Mulig, and Kimball (2007), op. cit;Messagelabs (2009), op. cit;Milletary (2005), op. cit.

[101] Dunn, John E. (2007), 'Do-it-Yorself Phishing Kit Found Online', *PCWorld*. <http://www.pcworld.com/article/128524/article.html>, accessed September 8 2014.

[102] Sophos (2004), 'Do-it-yourself phishing kits found on the internet, reveals Sophos', *Sophos*. <http://www.sophos.com/en-us/press-office/press-releases/2004/08/sa_diyphishing.aspx>, accessed September 19

hosting services which guarantee to keep phishers' websites up under any circumstance.[103] The low technical requirement for committing phishing makes phishing viable for a larger population, including non-technical criminals.

A number of countries have recognized the problem of producing, possessing, or transferring both data and programs that may assist in committing a computer offence and have therefore embedded provisions that criminalize these conducts. For example, Taiwan Criminal Code makes it a crime to produce computer programs for the commitment of the offences against computer use provided under chapter 36 of the Code which came into force in June 2003 (Art. 362). The UK Frauds Act 2006 makes it an offence to possess, make, adapt, supply or offer to supply an article knowing that it is designed or adapted for use or in connection with fraud (section 6 and 7). Section 8 makes it clear that 'article' includes 'any program or data held in electronic form'.

2.5.3. Increasing sophistication of attack techniques

Phishing attack techniques are constantly updated and reformed from time to time to produce better outcome and to circumvent detection. Even the savviest users could be fooled by sophisticated phishing attacks. A variety of technical solutions have hence been proposed to serve as the first line of defense to prevent phishing emails from reaching users, identifying phishing attacks and block fake websites in the first place. Generally speaking, the anti-phishing technical countermeasures can be divided into the following four categories.

2014.

[103] Roberts, Paul (2004), 'More Scam Artists Go Phishing', *PCWorld*. <http://www.pcworld.com/article/116330/article.html>, accessed September 17 2014.

Detecting phishing emails

Whether an email is phishing can be distinguished by identifying phishing email features or authenticating its sender. There are several research studies of content-based phishing classification using machine learning techniques.[104] Machine learning is where an algorithm (classifier) tries to classify an email to phishing or legitimate by learning certain features in the email. A well-known example is *PILFER*, a classifer proposed by Fette et al.,[105] which identifies phishing by incorporating 10 different specific features that are directly applicable to phishing emails, for example, nonmatching URLS, HTML emails, number of links, domains and dots.

A convincing phishing email has to make the intended recipients believe that the source of the communication is an entity that they trust. The spoofing of email senders has thus become an essential tactic used by phishers. The three predominant approaches to email sender authentication are Sender Policy Framework (SPF), Sender ID Framework (SIDF) and DomainKeys Identified Mail (DKIM).[106] Gorling found that despite that SPF is designed for easy adoption and consistently implemented in several popular anti-spam solutions, the adoption-ratio of SPF as an anti-phishing mechanism is very low.[107] Several methods have also been proposed to enhance email authentication, for example, the use of digitally signed mails[108] or a particular identity-based digital signature[109] to better guarantee authorship.

[104] Abu-Nimeh et al. (2007), op. cit;Basnet, Mukkamala, and Sung (2008), op. cit;Bergholz et al. (2010), op. cit;Ceesay (2008), op. cit;Chandrasekaran, Narayanan, and Upadhyaya (2006), op. cit;Fette, Sadeh, and Tomasic (2007), op. cit;Islam and Abawajy (2013), op. cit.

[105] Fette, Sadeh, and Tomasic (2007), op. cit.

[106] Herzberg (2009b), op. cit;Lininger and Vines (2005), op. cit.

[107] Görling, Stefan (2007), 'An overview of the Sender Policy Framework (SPF) as an anti-phishing mechanism', *Internet Research,* 17 (2), 169-79.

[108] Garfinkel et al. (2005), op. cit.

[109] Adida, Hohenberger, and Rivest (2005), op. cit.

Security management of password

Nowadays, it is a very common phenomenon that users have multiple password protected accounts over the Internet; for example, Internet banking account, email account or other accounts for accessing online services. Many users are used to utilizing the same password for manifold accounts due to the difficulty of remembering and managing several different and unrelated sets of password, which effectively provides phishing attackers an effortless access to a victim's various accounts once the password is stolen by phishers. A variety of methods have been proposed to protect users' passwords against phishing, including improving both the convenience and security logins,[110] strengthening authentication schemes,[111] preventing users from submitting sensitive information to a spoofed website by suggesting an alternative safe path[112] or issuing warning,[113] and preventing phishers from stealing such information.[114] Nevertheless, studies have shown that users are accustomed to ignore security indicators.[115] In addition, it was suggested that the usability

[110] Dhamija, Rachna and Tygar, J Doug (2005), 'The battle against phishing: Dynamic security skins', *Proceedings of the 2005 symposium on Usable privacy and security (SOUPS)* (Pittsburgh, PA, USA: ACM), 77-88;Feng, Qingxiang, et al. (2011), 'New Anti-phishing Method with Two Types of Passwords in OpenID System', in Junzo Watada, et al. (eds.), *2011 Fifth International Conference on Genetic and Evolutionary Computing (ICGEC 2011)* (Kinmen, Taiwan; Xiamen, China: IEEE), 69-72;Gouda, Mohamed G, et al. (2007), 'SPP: An anti-phishing single password protocol', *Computer Networks,* 51 (13), 3715-26;Halderman, J Alex, Waters, Brent, and Felten, Edward W (2005), 'A convenient method for securely managing passwords', *Proceedings of the 14th international conference on World Wide Web* (ACM), 471-79;Yee, Ka-Ping and Sitaker, Kragen (2006), 'Passpet: convenient password management and phishing protection', *Proceedings of the second symposium on Usable privacy and security (SOUPS '06)* (Pittsburgh, PA, USA: ACM), 32-43.

[111] Dhamija, Rachna and Perrig, Adrian (2000), 'Deja vu: A user study using images for authentication', *Proceedings of the 9th conference on USENIX Security Symposium* (9: USENIX Association Berkeley), 45-58;Ross, Blake, et al. (2005), 'Stronger Password Authentication Using Browser Extensions', *Proceedings of the 14th conference on USENIX Security Symposium* (14: USENIX Association Berkeley, CA, USA), 17-32.

[112] Wu, Min, Miller, Robert C, and Little, Greg (2006a), 'Web wallet: preventing phishing attacks by revealing user intentions', *Proceedings of the second symposium on Usable privacy and security (SOUPS '06)* (Pittsburgh, PA, USA: ACM), 102-13.

[113] Chou et al. (2004), op. cit;Kirda and Kruegel (2005), op. cit;--- (2006), 'Protecting users against phishing attacks', *The Computer Journal,* 49 (5), 554-61.

[114] Bin, Sun, Qiaoyan, Wen, and Xiaoying, Liang (2010), 'A DNS based anti-phishing approach', *2010 Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC)* (2; Wuhan, Hubei, China: IEEE), 262-65.

[115] Stebila, Douglas (2010), 'Reinforcing bad behaviour: the misuse of security indicators on popular websites', *Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction* (Brisbane, Australia: ACM), 248-51.

problem of anti-phishing tools affect not only the performance of these tools but also the willingness of general users to employ them.[116]

Blocking phishing websites

Whether or not users can be kept away from spoofed websites is crucial to determine the success of phishing attacks, as the users are immediately exposed to attacks carried by the phishing websites once they access to these websites. A number of researches have been conducted to detect phishing at the website level, which fall into three main categories: blacklisting and whitelisting, heuristic-based approach, and website authentication.

Blacklist approaches detect phishing websites by checking their URLs against a blacklist of known phishing URLs. Blacklists can be generated in various ways, including automatic categorization using the rules based on phishing patterns, manual verification by administrators or crowd sourcing by users. The best-known anti-phishing blacklists are operated by Google and Microsoft which integrated a list of phishing URLs into browsers.[117] Another popular blacklist is operated by PhishTank,[118] where anyone can submit suspected phishes and verify other users' submissions. Once a number of people required vote a submission is a phish, it is added to the blacklist. However, it always takes time for phish detected to appear on blacklists. A time delay of updating, in the meanwhile, produces advantages to the phishers. Sheng et al. conducted two tests on eight anti-phishing toolbars by using 191 fresh phish that were less than 30 minutes old. The authors

[116] Li, Linfeng and Helenius, Marko (2007), 'Usability evaluation of anti-phishing toolbars', *Journal in Computer Virology,* 3 (2), 163-84.

[117] Google op. cit;Microsoft op. cit;Mozilla 'Mozilla Firefox built-in phishing and malware protection', <https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work>, accessed August 15 2014.

[118] PhishTank, http://www.phishtank.com/.

found blacklists were ineffective at hour zero and could only identify 47% -83% of phish even after 12 hours.[119] To change the reactive nature of blacklists, researchers proposed alternative predictive blacklisting to detect phishing proactively based on known-bad domains[120], features of known phishing sites[121] or URLs,[122] or relevance ranking scheme borrowed from the link-analysis community.[123]

In contrast, the whitelist approach detects phishing by maintaining a trust list on different bases such as analysis of users' online behaviors[124] or URL validation.[125] For example, *PhishingGuard*, an anti-phishing solution introduced by Kang and Lee, maintains lists containing mapping of trusted domains and corresponding IP addresses to prevent access to phishing sites and warns for access to suspicious phishing sites by the URL similarity check

[119] Sheng, Steve, et al. (2009b), 'An empirical analysis of phishing blacklists', *CEAS 2009: Sixth Conference on Email and Anti-Spam* (Mountain View, California, USA).

[120] Felegyhazi, Mark, Kreibich, Christian, and Paxson, Vern (2010), 'On the potential of proactive domain blacklisting', *Proceedings of the Third USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET '10)* (San Jose, CA, USA).

[121] Prakash, Pawan, et al. (2010), 'Phishnet: predictive blacklisting to detect phishing attacks', *2010 Proceedings IEEE INFOCOM* (San Diego, California, USA: IEEE), 1-5.

[122] Ma, Justin, et al. (2009), 'Beyond blacklists: learning to detect malicious web sites from suspicious URLs', *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining* (Paris, France: ACM), 1245-54.

[123] Zhang, Jian, Porras, Phillip A, and Ullrich, Johannes (2008), 'Highly Predictive Blacklisting', in Paul Van Oorschot (ed.), *17th USENIX Security Symposium* (San Jose, CA), 107-22.

[124] Cao, Ye, Han, Weili, and Le, Yueran (2008), 'Anti-phishing based on automated individual white-list', in Elisa Bertino and Kenji Takahashi (eds.), *Proceedings of the 4th ACM workshop on Digital identity management* (Alexandria, VA, USA: ACM), 51-60;Dong, Xun, Clark, John A, and Jacob, Jeremy L (2010), 'Defending the weakest link: phishing websites detection by analysing user behaviours', *Telecommunication Systems,* 45 (2-3), 215-26.

[125] Kang, JungMin and Lee, DoHoon (2007), 'Advanced white list approach for preventing access to phishing sites', in Yun Ji Na, et al. (eds.), *The 2007 International Conference on Convergence Information Technology (ICCIT 2007)* (Gyeongju, Korea: IEEE), 491-96;Ronda, Troy, Saroiu, Stefan, and Wolman, Alec (2008), 'Itrustpage: a user-assisted anti-phishing tool', *ACM SIGOPS Operating Systems Review - EuroSys '08* (42; Glasgow, UK: ACM), 261-72;Sengar, PK and Kumar, Vijay (2010), 'Client-side defense against phishing with pagesafe', *International Journal of Computer Applications,* 4 (4), 6-10.

Heuristic-based anti-phishing technique is to estimate whether a given page has certain phishing heuristics characteristics. Most of heuristic-based researches look into URL features[126] or/and website content,[127] including textual and visual content such as words, titles, or images in the website, to identify phish. For example, Ludl et al. discovered a list of 18 properties of a phishing site, two of which are derived from the page's URL and the remaining features are extracted from the HTML source of a page, including number of forms, input fields, number of links, etc. Although nearly all the anti-phishing techniques claimed to have reached very high positive rates (correctly identifying a phishing site) while producing low false positive rate (incorrectly labeling a legitimate site as phish), Zhang et al. pointed out that the result of testing is significantly influenced by the source of phishing URLs and the freshness of the URLs tested.[128]

Another method proposed to detect a phishing website is to verify the identity of a legitimate site and prove it is a genuine site before users through image-based authentication using visual cryptography.[129] The use of visual cryptography is to decompose one secret image captcha[130] into

[126] Alsalman (2012), op. cit;Garera et al. (2007), op. cit;Hsu, Wang, and Pu (2011), op. cit.

[127] Chen et al. (2009), op. cit;Chen, Dick, and Miller (2010), op. cit;Liu et al. (2006), op. cit;Ludl et al. (2007), op. cit;Medvet, Kirda, and Kruegel (2008), op. cit;Nirmal, Ewards, and Geetha (2010), op. cit;Pan and Ding (2006), op. cit;Wenyin et al. (2005), op. cit;Xiang and Hong (2009), op. cit;Zhang, Hong, and Cranor (2007a), op. cit;Zhang et al. (2011), op. cit.

[128] Zhang et al. (2007b), op. cit.

[129] James, Divya and Philip, Mintu (2012), 'A Novel Anti phishing framework based on visual cryptography', *2012 International Conference on Power, Signals, Controls and Computation (EPSCICON)* (Thrissur, Kerala, India: IEEE), 1-5;Naor, Moni and Shamir, Adi (1995), 'Visual cryptography', in Alfredo De Santis (ed.), *Advances in Cryptology EUROCRYPT'94 - Workshop on the Theory and Application of Cryptographic Techniques)* (Perugia, Italy: Springer), 1-12;Yenurkar, Mr Bhushan and Zade, Mr Shrikant (2014), 'An anti-phishing framework with new validation scheme using visual cryptography ', *International Journal of Computer Science and Mobile Computing (IJCSMC),* 3 (2), 739-44.

[130] A CAPTCHA (short for Completely Automated Public Turing Test to Tell Computers and Humans Apart) is a program that protects websites against bots by telling whether its user is a human or computer through generating tests that humans can pass but current computer programs cannot. This terms was coined in 2000 by Luis von Ahn et al. of Carnegie Mellon University. It is prevalently used to prevent bots from taking part in online polls, registering for free email accounts, entering a web site, and sending email worms and spams. The most common type of CAPTCHA was invented by Lillibridge et al. in 2001 which requires type the letters of a distorted image, sometimes with an obscured sequence of letters or digits that appears on the screen. Lillibridge, Mark D, et al. (2001), 'Method for selectively restricting access to computer systems', (Google Patents);Von Ahn, Luis, et al. (2003b), 'Captcha: Telling humans and computers apart automatically', *Proceedings of Eurocrypt*;Von Ahn, Luis, et al. (2003a), 'CAPTCHA: Using hard AI problems for security', in Eli Biham (ed.), *Advances in Cryptology - EUROCRYPT 2003 (International Conference on the Theory and Applications of Cryptographic Techniques)* (Warsaw, Poland: Springer), 294-311.

two shares, one resides with user and the other resides with server, such that the original image can be revealed only when both are simultaneously available. During authentication a genuine server forwards its share and the user forwards his share. Once the original image captcha is revealed to the user it can prove the website is genuine.

BogusBiter, a client-side tool developed by Yue and Wang[131] to counter phishing in a different way from the aforementioned proposals which primarily focuses on helping users identify phishing sites or prevents them from giving away credentials. Instead of preventing users from biting the bait, BogusBiter feeds large number of bogus credentials into a suspected phishing site once a login page web page is classified as a phishing page. The real credential is concealed among bogus credentials. It also enables a legitimate website to identify stolen credentials as long as the phishers visit the legitimate site to verify the victim's credential.

While a number of technical solutions have been proposed and developed to defend against phishing, recent usability studies have demonstrated an alarming result which put in question the effectiveness of both server-side security indicators such as SSL certificate or URL and client-side toolbars and warnings to help users avoid phishing attacks.[132] Browser security indicators are frequently ignored or inappropriately interpreted by users. Most users are not clear about what to look for in phishing messages[133] and what they are expected to do to respond to warnings.[134] The result of the above studies suggests two facts: first, maintain security is seen by most users as a

[131] Yue, Chuan and Wang, Haining (2010), 'BogusBiter: A transparent protection against phishing attacks', *ACM Transactions on Internet Technology (TOIT),* 10 (2), 6.

[132] Aburrous et al. (2010), op. cit;Dhamija, Tygar, and Hearst (2006), op. cit;Downs, Holbrook, and Cranor (2006), op. cit;Egelman, Cranor, and Hong (2008), op. cit;Herzberg (2009a), op. cit;Schechter et al. (2007), op. cit;Wu, Miller, and Garfinkel (2006b), op. cit;Zhang et al. (2007b), op. cit.

[133] Furnell, Steven (2007), 'Phishing: can we spot the signs?', *Computer Fraud & Security,* 2007 (3), 10-15.

[134] Furnell, Steven M (2009), 'The irreversible march of technology', *Information Security Technical Report,* 14 (4), 176-80.

secondary goal;[135] and second, technology alone is not adequate to address phishing, as its effectiveness is largely dependent upon whether users have a baseline level of security awareness[136] and understand what they are supposed to respond and why.

2.5.4. Exploitation of users' weakness

Phishing is a typical form of social engineering attack which means sending an email seemingly from a reputable financial, trustworthy entity or a friend that requests account information, suggests a problem, recommends something that might interest you or capitalizes on world events.[137] Social engineering attacks are attacks made by misappropriating human interaction or social skills to manipulate people into performing actions or divulging confidential information.[138] Social engineers often attempt to persuade potential victims with appeals to strong emotions such as excitement or fear to create a feeling of trust and commitment.[139]

The success of phishing attacks crucially relies on whether phishing emails favorably dupe the recipients into clicking on the link enclosed which will lead them to a catch site or into opening a benign-looking file that will infect their computers. This may be achieved by abusing two aspects of human nature: trust in acquaintances and a fear of crisis. Comparing an email that comes from a

[135] Kumaraguru et al. (2010), op. cit;Wu, Miller, and Garfinkel (2006b), op. cit.

[136] Bakhshi, Papadaki, and Furnell (2009), op. cit;Furnell (2007), op. cit.

[137] Irani, Danesh, et al. (2011), 'Reverse social engineering attacks in online social networks', in Thorsten Holz and Herbert Bos (eds.), *Detection of intrusions and malware, and vulnerability assessment* (6739: Springer), 55-74;Workman (2008), op. cit.

[138] Mitnick, Kevin D and Simon, William L (2001), *The art of deception: Controlling the human element of security* (John Wiley & Sons).

[139] Gao, W and Kim, J (2007), 'Robbing the cradle is like taking candy from a baby', *Proceedings of the Annual Conference of the Security Policy Institute (GCSPI)* (4; Amsterdam, The Netherlands), 23-37.

stranger, most people tend to trust the same email sent from a friend or somebody they know and they are more likely to respond to the request by following the link or executing the attachment.

In addition to taking advantage of human trust in acquaintances, abusing the fear of a crisis in human nature is frequently used to influence the recipients. Phishing attackers often send emails, the subjects of which appear significantly to concern the interests of the recipients; for example 'Immediate security update of online banking' or 'Important verification of email account.' By inspiring the general sense of crisis, this sort of email is more likely to attract the attention of the potential victims and has more chance of tempting them to follow the advice indicated in the email.

There is no single solution to eliminate social engineering attacks, as it largely deals with the human factor. The problem of phishing is that it targets the weakest link in the security chain, namely, human.[140] Workman conducted a study grounded in social psychology theory to investigate the reasons why people may or may not fall victims.[141] He found that people feel obligated to reciprocate favors such as receiving free software or gift certificates by giving away confidential information; for example, company email addresses or employee identification numbers. A savvy phisher is proficient at manipulating the weakness of human to interfere with potential victim's ability to analyze carefully the content of the message.

[140] Aburrous et al. (2010), op. cit;Butler, Rika (2007), 'A framework of anti-phishing measures aimed at protecting the online consumer's identity', *Electronic Library, The,* 25 (5), 517-33;Macewan (2013), op. cit;Thomson, K and Van Niekerk, Johan (2012), 'Combating information security apathy by encouraging prosocial organisational behaviour', *Information Management & Computer Security,* 20 (1), 39-46.

[141] Workman (2008), op. cit.

In addition to interference of emotion, phishing attacks succeed by exploiting a user's inability to distinguish phishing emails or websites from legitimate ones. Bakhishi et al.[142] conducted an email-based experiment in which 152 staff members were sent a message asking them to visit an external web site and install a claimed software. The result showed that 23 percent of recipients were fooled by the simulated attack even though the message was designed to convey signs of a deception and the external website was intentionally badly designed in order to alert users. Several research studies have been conducted to investigate the factors such as gender or age that could impact user's susceptibility to phishing.[143] Sheng et al.[144] suggested that women are more susceptible than men to phishing, whereas Kumaraguru et al.[145] found no distinct difference between males and females in the tendency to fall for phishing. However, both studies concluded that the participants in the 18 – 25 age group are more susceptible to phishing than other age groups.

Enabling users to engage in secure online behaviours is another important countermeasure against phishing which is frequently done by education and training.[146] Researchers[147] proposed a game-based education framework to encourage user avoidance behavior by enhancing their avoidance motivation which was determined by five elements: perceived susceptibility, perceived severity, safeguard effectiveness, safeguard cost, and self-efficacy.[148]

[142] Bakhshi, Papadaki, and Furnell (2009), op. cit.

[143] Ademaj and Schuck (2009), op. cit;Kumaraguru et al. (2008), op. cit;Martin (2009), op. cit;Sheng et al. (2010), op. cit.

[144] Sheng et al. (2010), op. cit.

[145] Kumaraguru et al. (2008), op. cit.

[146] Ademaj and Schuck (2009), op. cit;Arachchilage, Nalin Asanka Gamagedara and Love, Steve (2013), 'A game design framework for avoiding phishing attacks', *Computers in Human Behavior,* 29 (3), 706-14;Davinson and Sillence (2010), op. cit;Jerram et al. (2012), op. cit;Liang, Huigang and Xue, Yajiong (2010), 'Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective', *Journal of the Association for Information Systems,* 11 (7);Von Solms (2013), op. cit.

[147] Arachchilage and Love (2013), op. cit.

[148] Comesongsri, Veti (2010), 'Motivation for the avoidance of phishing threat', (The University of Memphis);Liang and Xue (2010), op. cit.

Several researchers have proposed user education or training programs, which are mostly designed in the format of game, to help users to better recognize phishing and improve their resistance to phishing attacks.[149] Game-based education provides a natural and interactive environment for learning by doing. *PhishGuru*, a well-known embedded training system developed by Kumaraguru et al.,[150] teaches users to avoid falling for phishing by delivering a training message at the teachable moment, i.e. when the user clicks on the URL in a simulated phishing email. Another example is *Anti-Phishing Phil*, an online game grounded in learning science principles that enhance users' ability to avoid phishing by teaching them how to use cues in URLs to identify fraudulent websites.[151]

While the results of both lab and real-world experiment indicated that the above education tools are effective to help users to better recognize phishing, some researchers raised questions about the effect of education measures. An evaluation of the effects of Anti-Phishing Phil found that the training appears not to have produced a broad effect on promoting secure behaviour beyond the specific points it trained on.[152] Researchers[153] also argued that phishing tests can do very little help to enhance users' ability to spot phishing. Another problem is that the constant and long-term cost of education and training without immediate benefit can be an important factor may negatively influence the incentive of the businesses to engage in education scheme.[154]

[149] Kumaraguru et al. (2008), op. cit;Kumaraguru (2009), op. cit;Kumaraguru et al. (2009), op. cit;Kumaraguru et al. (2010), op. cit;Robila and Ragucci (2006), op. cit;Sheng et al. (2007), op. cit;Sheng et al. (2010), op. cit;Von Solms (2013), op. cit;Yang et al. (2012), op. cit.

[150] Kumaraguru et al. (2008), op. cit;Kumaraguru (2009), op. cit;Kumaraguru et al. (2009), op. cit;Kumaraguru et al. (2010), op. cit.

[151] Kumaraguru et al. (2010), op. cit;Sheng et al. (2007), op. cit.

[152] Davinson and Sillence (2010), op. cit.

[153] Anandpara et al. (2007), op. cit.

[154] Purkait (2012), op. cit.

2.5.5. The transient nature of phishing websites

To avoid detection and trace, the lifetime of a phishing website is usually very short, existing for only few days or even few hours. APWG’s statistics revealed an average time online for phishing sites was 3.1 days.[155] Phishing sites often appear and disappear in a very short time and move from one host to another at extremely high speed through the use of free web space or compromised machines or by utilizing fast-flux network. In fact, a phishing site does not need to stay alive for a long time to be effective. A research article indicated that 80 percent of stolen credentials are gathered and become usable by phishers within the first 5 hours and that, by 10 hours, more than 90 percent of the data that a phishing site is able to collect has already been harvested.[156] Whether a phishing site could be blocked and taken down within 5 to 10 hours hence becomes crucial to suppressing phishing attacks.

One of the key countermeasures to phishing is the prompt removal of the spoofed websites. The strategy of ‘notice-and-takedown’, which describes the scheme for the removal of undesirable content from the Internet, has been prevalently employed by banks and organizations that are impersonated to deal with counterfeit websites. A majority of banks outsource specialist companies, which we call ‘takedown companies’, to take phishing websites down by either removing the web pages from the hosting machine or requiring a registrar to suspend a domain name from the DNS (domain name system) when the domain name in question has been registered especially for phishing use or in some complex cases where page request are relayed by ever-changing bot-infected machines.

[155] APWG (2008a), 'Phishing Activity Trends: report for the month of January 2008'. <http://docs.apwg.org/reports/apwg_report_jan_2008.pdf>, accessed September 15 2014.

[156] Klein, Amit (2010), 'The Golden Hour of Phishing Attacks', *Trusteer* <http://www.trusteer.com/blog/golden-hour-phishing-attacks>, accessed September 10 2014.

To evade being traced, most phishing attackers tend to use free web hosting services or host the site on compromised machines rather than on their own machines.[157] In this case, it is necessary to contact the free web-hosting providers or the system administrator (sysadmin) who looks after the machine to ask them to remove the spoofed site. A research[158] indicated that whether the brand owners are aware of the existence of phishing sites is a key that decides how quickly these sites are removed.

However, the use of fast-flux technique can significantly extend the lifetime of phishing sites[159] which has become a huge challenge to the effectiveness of takedown strategies because the ever-changing list of IP addresses resolved from a domain makes it almost impossible to locate all the hosting machines and shut them down.[160] Rock-phish sites have also largely increased difficulty of takedown procedure as they can quickly and automatically switch to another bot-infected machine. To have the domain registrars to suspend the domain name in question is the only way to remove fast-flux phishing and rock-phish sites which is nevertheless not that easy and sometimes rather time-consuming.[161]

[157] McGrath, D Kevin and Gupta, Minaxi (2008), 'Behind Phishing: An Examination of Phisher Modi Operandi', *LEET,* 8, 4;Moore and Clayton (2009), op. cit.

[158] Moore and Clayton (2009), op. cit.

[159] Moore and Clayton (2007), op. cit.

[160] McGrath, D Kevin, Kalafut, Andrew, and Gupta, Minaxi (2009), 'Phishing infrastructure fluxes all the way', *IEEE Security & Privacy,* 7 (5), 0021-28;Moore and Clayton (2007), op. cit;Moore and Clayton (2009), op. cit.

[161] For example, the Austrian domain registrar nic.at initially refused to remove rock-phish domains and asked the reporter, Spamhaus – an email-blacklist operator, to prove that these domains had been registered by non-existent persons. Warrner, Gary (2007), 'Report on the criminal 'Rock Phish' domains registered at Nic.at', *SPAMHAUS*. <http://www.spamhaus.org/organization/statement/7/>, accessed September 15 2014.

Take-down strategy of phishing sites was described as a cat and mouse game,[162] as we are currently unable to prevent the creation of phishing sites but can only chase them and shut them down. Even though, taking down a phishing site as soon as it is detected is requisite to reduce the potential damage and victims that phishing site may cause. The effectiveness of a takedown regime can be improved by prompting the reaction of the actors responsible for takedown, i.e. domain registrars, ISPs and system administrators, to removal requests and enhancing the cooperation between the stakeholders involved by sharing their information about phishing URLs with each other.[163]

This chapter has assessed the reasons why phishing attacks succeed and overviewed the work that has been developed on the countermeasures against phishing in diverse fields. Every countermeasure has its strengths and weaknesses, which proves that there is no silver bullet to phishing and a combined approach incorporating strategies from multiple interfaces may be the answer to phishing.[164] However, while significant volume of research studies have been conducted on developing technological tools to prevent users from phishing attacks, very little research-based literature, apart from the debates that focus on liability rules and legal reforms, could be found that explores the legal force to address the problem of phishing.[165] This may suggest two possibilities: one is that technology has been prevalently recognized as a powerful anti-phishing tool which is worthy of more development; and the other is that the relation between laws and phishing is not properly understood or the function of legal force in regulating phishing is not recognized.

2.6. Conclusion

[162] Varghese (2008), op. cit.

[163] Moore and Clayton (2008), op. cit.

[164] Lynch (2005), op. cit;Mcnealy (2008), op. cit;Sullins (2006), op. cit;Wilson and Argles (2011), op. cit.

[165] Savirimuthu, Joseph (2008), 'Identity theft and the gullible computer user: what Sun Tzu in the art of war might teach', *J. Int'l Com. L. & Tech.,* 3, 120.

Phishing, a term that first appeared in the 1990s, has posed increasing threats to information security and caused tremendous damage on a global scale. Phishing targets the obtainment of confidential information which may yield financial gain both directly and indirectly but is not always true. The damage that phishing is likely to cause includes the direct monetary loss, the cost used to redress phishing and also the loss of customers and the damage to reputation and credit. It is difficult to regulate phishing because it usually takes advantage of the borderless nature of cyberspace, easy availability of phishing resources, and ephemeral nature of phishing websites. Also, a phisher is proficient at exploiting vulnerability of technology and weakness in humans. Considerable effort has been made for the development of anti-phishing strategies to prevent phishing attacks in different respects. However, having examined the existing research on phishing countermeasures, this chapter found a gap of the anti-phishing research between legal and other fields. The current research is dominated by technical solutions whereas comparatively little work has been conducted on studying the role of laws. In addition, the current legal debates over phishing have mostly focused on legal reforms and liability rules of criminal law which is actually not easy to be enforced because of the nature of phishing and is particularly difficult for Taiwan to implement due to its disadvantaged political status. The next chapter explores the special experience of Taiwan as a case study.

CHAPTER 3 THE PROBLEM OF PHISHING ENCOUNTERED IN TAIWAN

Synopsis

This chapter continues the account of phishing in the previous chapter by considering it in the specific context of Taiwan and indicates the specific significance of using Taiwan as a case study. This includes general factors such as the nature and prevalence of phishing attacks and the problems of regulation as well as special factors resulting from Taiwan's international relationships.

3.1. Introduction

Taiwan has a well-developed information technology infrastructure and plays an important role in the cyber world; however, it has been a major target of phishing attacks as well as one of the top hosting country of phishing websites. The severity of phishing threat has inspired a strong demand for regulation of phishing, but yet, Taiwan has been in a particular dilemma of developing effective regulation due to a complex of factors.

This chapter underlines the particular problems facing in Taiwan in combating phishing to highlight the contribution that Taiwan's experience can make to the research development of phishing. It examines the reasons why Taiwan is so vulnerable to phishing attacks and looks into the specific difficulties of Taiwan in effectively regulating phishing.

3.2. Overview of the phishing problem in Taiwan

Cyberspace provides phishers a borderless platform to launch attacks across countries. In order to evade trace and prosecution, very seldom will an attacker host the phishing site that targets the users all in the same country where he resides. In most cases, an attacker in country A may target the users in country B through a spoofed website hosted in country C. An attacker in country A may also target the native users by utilizing a network of bot-infected machines located in country C or in more than one other countries. Phishing is a global problem, and it is almost impossible for any country to be isolated from the issue of phishing. A country, especially with mature online environment and considerable scale of online commerce but insufficient protection of information security is at the highest risk of becoming not only the main target but also the hotbed of phishing attacks. The situation can be more complicated if some motivations other than financial profit are involved, for example, political factors. This is exactly the case of Taiwan.

Taiwan has been one of the main targets of phishing attacks as well as one of the top countries for phishing hosting. In spite of sever threats posed by phishing, Taiwan appears to be still struggling with effective regulation of phishing. The issue of phishing did not receive proper attention from either researchers or government in Taiwan until recently. In addition, Taiwan has always been experiencing particular difficulty of taking part of international conventions or agreements and engaging in international cooperation due to complicated political factors. This thesis recognizes that Taiwan has been at high risk of phishing attacks and has a desire for effective regulation, but yet, it faces severe challenges in terms of developing a viable regulatory regime. Taiwan's experience is able to provide a valuable insight into the general and specific difficulties that practically reside in managing phishing, which are worth considering for future development of a regulatory framework of phishing as well as other similar cybercrimes. This is the main factor leading to the selection of Taiwan as a case study. Taiwan is my home country, which also makes it earlier to me to obtain a good understanding of the situation and access the resources necessary for this research.

3.3. Taiwan is one of the principal targets and hosts of phishing attacks

Over a decade, Symantec has been researching information security threats and has regularly released reports providing analysis of the data about emerging trends and landscape of global threat activity. It has published a series of monthly phishing report of the metrics and trends observed in phishing activity between May 2009 and March 2010. The statistics given in Symantec's reports showed that Taiwan was the second highest globally ranked country for malicious activities per Internet user during the second half of 2006.[166] For the specific measurement of malicious activities, the above report showed that Taiwan was the top country for phishing hosts and the second highest number of bot-infected computers with the Asia-Pacific/Japan region (hereinafter, APJ region). Symantec, in its phishing monthly reports, also found that Taiwan was on the list of top five countries in the world where the phishing sites were hosted[167] and Taipei, the capital city of Taiwan, was the top city of hosting phishing sites followed by Jacksonville and Houston.[168]

The above statistics demonstrate that phishing has caused a severe threat to Taiwan, and this can be

[166] Symantec (2007), 'Symantec Internet Security Threat Report –Trend for July-December 2006', XI. <http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf>, accessed August 30 2014.

[167] --- (2009a), 'The State of Phishing: A Monthly of Report – May 2009'. <http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_report_05-2009.en-us.pdf>, accessed August 30 2014.

[168] --- (2009c), 'The State of Phishing: A Monthly of Report – August 2009'. <http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_report_08-2009.en-us.pdf>, accessed August 31 2014.

imputed to the following causes.

3.3.1. Mature environment of Internet usage and connectivity

Taiwan is a highly computerized country with a high density of Internet users and large numbers of Internet hosts. The data gathered by the Taiwan Network Information Center (TWNIC)[169] revealed that the number of Internet users in Taiwan had reached 16,217,009, accounting of over 70% of the total population by the end of March 2010.[170] The figures from *CIA World Factbook*[171] generated in 2012 showed that Taiwan has 6,272,000 Internet hosts, giving it a ranking of the third highest in the APJ region, after Japan and China.[172]

Taiwan has a high level of Internet usage and connectivity, along with high-speed Internet infrastructure. Nevertheless, the Internet is a ‘double-edged sword’. While the mature online environment may substantially expedite information circulation and boost the development of the online economy in Taiwan, it also provides cyber attackers with larger capacities, faster speeds, constantly connected systems and more stable connections which inevitably make Taiwan vulnerable to a variety of malicious attacks, including phishing.

3.3.2. Insufficient management of web server security

[169] TWNIC is a neutral and non-profit organization established at the end of 1999 and supervised by the Ministry of Transportation and Communication that manages domain name registration and IP address allocation in Taiwan.

[170] Taiwan Network Information Center (2010), 'Wireless Internet Usage in Taiwan – A summary Report of the January Survey of 2010'. <http://www.twnic.net.tw/download/200307/1001c.pdf>, accessed August 27 2014.

[171] *CIA World Factbook* is a reference resource produced by the U.S. Central Intelligence Agency (CIA) with information on the history, people, government, economy, geography, communications, transportation, military, and transnational issues for the countries of the world.

[172] Central Intelligence Agency (2012), 'The World Factbook'. <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2184rank.html>, accessed September 1 2014.

According to a technical expert from Symantec,[173] insufficient management of web server security, especially regarding web servers that have been set up by small and medium-sized businesses, students or heavy Internet users, is another important cause responsible for the large number of phishing hosts in Taiwan. Phishing attackers usually compromise targeted websites by exploiting web browser vulnerabilities through an in-session attack to generate a phishing pop-up without changing the original content of the compromised website. As the content and functions run by the base website generally are uninfluenced, the performance of this kind of phishing attack is hence not easy to detect promptly with a shortage of resources and manpower for managing web server security.

In fact, it is a universal phenomenon that small and medium-sized businesses (SMBs) are more vulnerable to various malicious attacks, including phishing. In September 2011, Symantec conducted a research survey of 1,900 SMBs around the globe to gain an understanding of their familiarity with threats and their actions to protect themselves.[174] The findings revealed that while the SMBs are familiar with security threats such as DDoS attacks, targeted attacks, and keystroke logging, they do not consider themselves in danger as targets of cyber-attacks simply because they are a small company. Since the SMBs did not feel at risk, many of them failed to take actions to protect themselves. 61 percent did not use anti-virus on all desktops and 47 percent did not use security on mail severs.

However, Symantec's data had proved that the assumption of the SMBs is wrong. Since the beginning of 2010, 40 percent of all targeted attacks have been directed at small businesses whereas

[173] ZDNet (2007), 'Taipei has beceome the principal setting location of phishing web sites within the Asia-Pacific region', (ZDNet).

[174] Symantec (2011), 'SMB Threat Awareness Poll – Global Results'. <http://www.symantec.com/content/en/us/about/media/pdfs/symc-smb-threat-awareness-poll.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Nov_worldwide_SMBflashpoll/>, accessed August 29 2014.

only 28 percent at large enterprises. The possible reasons can be that cybercriminals recognize that targeting large enterprises carries a greater risk of detection and SMBs, just like ‘low hanging fruit’, become an easy target to cybercriminals due to a lack of alertness and weak security management.[175]

3.3.3. High volume of bot-infected computers

Botnets have been described as ‘Swiss Army knives of the underground economy’ because they are capable to assist in a great variety of malicious attacks, including phishing.[176] A botnet is a very useful tool to phishers to either deliver phishing messages or host and protect phishing websites from disclosure. Taiwan is on the list of top countries hosting phishing websites in the world; however, it does not necessarily suggest that these phishing attacks really originate in Taiwan. People from other countries may launch phishing attacks on other countries through a scapegoat – bot-infected machines in Taiwan. A well-known example is ‘Operation Aurora’, where Chinese hackers launched large scale sophisticated cyber-attacks against dozens of commercial companies in the United States from mid-September to December 2009 by utilizing compromised computers located in Taiwan.[177]

Number of bot-infected computers can serve as a meaningful indicator of the extent of phishing hosts. An increase of number of bot-infected computers, in general, results in a corresponding rise of phishing hosts. Lee Hsiang-Chen, the director of the National Police Administration’s Internet Crime Investigations unit, indicated in an interview conducted in 2007 that over a third of

[175] Macewan (2013), op. cit.

[176] Wilson, Clay (2008), 'Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress', *CRS Report for Congress*. <http://fas.org/sgp/crs/terror/RL32114.pdf>, accessed September 20 2014.

[177] http://en.wikipedia.org/wiki/Operation_Aurora.

computers in Taiwan have been installed with bot programs.[178] Symantec also found Taipei was the top city for bot infections in the APJ region in 2008.[179] Why is Taiwan so vulnerable to botnets? In addition to the high speed of Taiwan's Internet infrastructure and a lack of security and management by operators,[180] it was indicated that insufficient users' awareness about computer security is another main cause that contributes to the botnets problem in Taiwan.[181] When users discover that their computer is infected, they usually choose to reinstall the operating system of the computer. However, reinstallation will only protect the computer from botnet manipulation for a short time. The computer is still at high risk of being re-infected if the users don't have adequate knowledge and sense of computer security.

3.3.4. Intense malicious cyber-attacks from China

China has been one of the top active originating countries for many cyber-attacks, and Taiwan, unsurprisingly, has been one of the most preferred targets for China's attackers. While the phishing hosts in Taiwan primarily targeted European countries and America, most phishing attacks on Taiwan were reportedly originated from China.[182] The possible reasons for this phenomenon can be the commonality of language and culture and the political tension between these two countries.

The performance of social engineering attacks predominately depends on whether an attacker can successfully manipulate the action of potential victims with appeals to strong emotions. This can be much easier if the attackers share the same or similar language and culture as the victims. Taiwan

[178] Hsueh, Yi-Jing (2007), 'Averagely ten times hacker attackers daily', *Business Next*, 72.

[179] Symantec (2009b), 'Symantec APJ Internet Security Threat Report – Trend for 2008', XIV. <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_apj_internet_security_threat_report_04-2009.en-us.pdf>, accessed August 29 2014.

[180] Chao, Y (2010), 'Google attacks used addresses based in Taiwan', *Taipei Times,* 16 January 2010;Su, Wen-Bin (2009), 'Taipei becomes the headquarters of bots in the Asia and Pacific Region', *iThome*. <http://www.ithome.com.tw/itadm/article.php?c=54571>, accessed September 20 2014.

[181] Su (2009), op. cit.

[182] Zdnet (2007), op. cit.

users are more likely to respond to a phishing message written in Mandarin which appears to be aware of the hot topics happening in Taiwan society rather than an English-written email. The commonalities of language and cultural background largely increases the possibilities of deception of Taiwan users,[183] which in turn intensifies the phishing attempt of China's attackers against Taiwan.

The political tension between Taiwan and China is another eventful factor responsible for the considerable number of phishing attacks against Taiwan. PRC (People's Republic of China) led by the Communist Party has long claimed territorial sovereignty over Taiwan because the island is ruled by the exiled ROC (Republic of China) government led by the Kuomintang (KMT, Chinese Nationalist Party) which was defeated in 1949 during China's civil war. Both the ROC and the PRC agree to a 'one-China' policy but have disagreement about the form that a 'one-China' policy should take. The PRC considers itself the legitimate ruling power for all of China whereas the ROC refuses to acknowledge the governing status of the PRC. To maintain territorial integrity, the government in Beijing never gives up the use of force to keep Taiwan from declaring independence where necessary.

The antagonistic relationship between Taiwan and China has boosted the growth of malicious cyber-attacks between them.[184] Tsai De-Sheng, the acting director of the National Security Bureau of Taiwan claimed that over 3,100 attacks were launched by a Chinese cyber army against Taiwan government systems with an attempt to steal sensitive information during 2008.[185] This did not include attacks against the private sector. In addition, Taiwan's political activities, for example,

[183] Chang, Yao-Chung (2012), *Cybercrime in the Greater China region: regulatory responses and crime prevention across the Taiwan Strait* (Edward Elgar Publishing);Chao (2010), op. cit.

[184] Mazanec, Brian M (2009), 'The art of (cyber) war', *Journal of International Security Affairs,* 16, 81-90.

[185] Xu, Shao Xuan (2009), 'Over 3,100 cyber attacks towards Taiwanese government system were originated by Chinese cyber army', *Liberty Times,* 24 March 2009.

legislative or presidential elections, have been usually accompanied with an increase of attacks originated by China in order to influence the campaigns.[186] In August 2011, Taiwan's Democratic Progressive Party (DPP), which has long advocated Taiwan becoming its own nation against the wishes of both the PRC and Kuomintang, alleged that the Chinese government is behind a series of phishing attacks that target information about the party's election activities.[187] According to the DPP's statement, the attackers sent the DPP staffers emails which appeared to be from the employees of the other party but contained a virus in the attached files that can be used to monitor the compromised computers. The above statement also indicated that some of the attacks had been traced to China's Xinhua Agency, which is a state-run press group.

The peculiar political situation of Taiwan not only exposes Taiwan to fierce cyber-attacks triggered by China but also puts other countries involved, especially the USA, at a very high risk of being attacked. *The Mutual Defense Treaty between the USA and the ROC*, which was signed in December 1954 and came to an end in January 1980, assisted the ROC in maintaining its legitimacy as the sole government of all of China and secured Taiwan from invasion by the PRC until 1970s. In 1971, the ROC walked out of the United Nations shortly before it recognized the government in Beijing as the legitimate holder of China's seat in the United Nations. In 1979, the U.S. Congress passed the *Taiwan Relations Act* to maintain commercial, cultural and other relations in unofficial form with Taiwan after the establishment of diplomatic relations with the PRC and the breaking of relations between the United States and Taiwan. The Act requires the United States to "provide Taiwan arms of a defensive character"; and to "maintain the capacity of the United States to resist

[186] Symantec (2008), 'Symantec APJ Internet Security Threat Report – Trend for July-December 07', XIII. <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_apj_internet_security_threat_report_xiii_04-2008.en-us.pdf>, accessed August 31 2014.

[187] Kan, Michael (2011), 'Taiwan political party accuses China of hacking', *PCWorld*. <http://www.pcworld.com/article/237591/taiwan_political_party_accusses_china_of_hacking.html>, accessed September 7 2014.

any resort to force or other forms of coercion that would jeopardize the security, or the social or economic system of the people on Taiwan."[188]

The United States intentionally stands in an ambiguous position towards security issues in the Taiwan Strait, which is known as '*strategic ambiguity*' – a dual deterrence policy designed to dissuade Taiwan from a unilateral declaration of independence, and to dissuade the PRC from unilaterally unifying Taiwan with the PRC by other than peaceful means, including by boycotts or embargoes.[189] China expressed strong opposition to the U.S. Taiwan Relations Act and regarded it as an open violation against China's sovereignty.[190] To deter U.S. involvement in a future conflict over Taiwan, China has been continually investing in military force such as new missile technologies[191] and increasingly developing advanced capacity in cyberspace. It has been suggested that China attempts to achieve military effects and influence the outcome of conventional armed conflicts via cyber-warfare.[192] By using the threat of cyber-warfare, China seeks to deter an actor from behaving in a manner that is in opposition to Chinese strategic interests, for example, ultimate reunification with Taiwan.

3.4. Poverty of anti-phishing research development besides technology

Although nearly two decades have passed by since the emergence of phishing in the mid of 1990s, Taiwan appears to show very little interest in the development of anti-phishing solutions except for technical tools. Very little Taiwanese scholarly literature could be found that is closely related to

[188] The full text of the Taiwan Relations Act, http://www.ait.org.tw/en/taiwan-relations-act.html.

[189] Benson, Brett V and Niou, Emerson MS (2000), 'Comprehending strategic ambiguity: US policy toward Taiwan security', *Taiwan Security Research*.

[190] Embassy of the People's Republic of China in the United States of America, 'China opposes US congress' resolution on Taiwan (19/07/04), http://www.china-embassy.org/eng/xw/t143465.htm.

[191] Kueter, Jeff (2009), 'The missile defense mission', *Journal of International Security Affairs,* 16, 33-40.

[192] Mazanec (2009), op. cit.

phishing countermeasures prior to 2008. A proposal for an email authentication protocol was brought forward by Chang et al.[193] in 2007 to spot phishing emails by verifying an authentication message which is contained in each email and can only be signed by the sender himself. In the same year, Fang[194] introduced a new type of visual cryptography, named *visual cryptography in reversible style*. Although the author did not particularly address the connection between his work and phishing, the technique of visual cryptography has been prevalently employed to identify the genuineness of a website which can in turn be used to detect a bogus website.

There is significant progress in Taiwanese scholarly work on phishing solutions since 2008, which is nevertheless dominated by the studies over technical countermeasures. A heuristic-based approach was taken by some researchers to develop tools to detect phishing websites by identifying the features extracted from the web pages.[195] A URL classification method was also proposed to differentiate phishing sites and benign ones by examining lexical features of URLs which usually include domain name, path, filename, and some arguments[196] or using both lexical and descriptive features of URLs to combine the filtering results.[197] Several studies introduced a mutual authentication mechanism between users and severs as an anti-phishing solution which can be achieved by different keys, including a data-embedded image uploaded by users[198] or users' biometric information.[199] One-time-password (OTP) protocol was employed by some researchers

[193] Chang and Chang (2007), op. cit.

[194] Fang (2007), op. cit.

[195] Chen et al. (2009), op. cit;Huang et al. (2010), op. cit.

[196] Hsu, Wang, and Pu (2011), op. cit;Pao, Hsing-Kuo, Chou, Yan-Lin, and Lee, Yuh-Jye (2012), 'Malicious URL Detection Based on Kolmogorov Complexity Estimation', *Proceedings of the The 2012 IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technology - Volume 01* (1: IEEE Computer Society), 380-87.

[197] Lin et al. (2013), op. cit.

[198] Lin and Chiang (2009), op. cit.

[199] Lee et al. (2011), op. cit.

to ensure independence between each login and thereby thwart phishing attacks by rendering the stolen passwords invalid.[200]

Instead of distinguishing phishing patterns in web pages, Lee et al. focused on the access contexts in which users will fall prey to phishing by exploring users' web browsing behaviors.[201] The authors extracted discriminatory features of each clicked URL in a user's access sequence to capture contextual information for phishing detection and demonstrated that their method had achieved very high accuracy for predicting the phishing threats of users' next accesses through large-scale experiments. Tseng et al. worked on the frame model of phishing attack knowledge and page scenario which be utilized to build up an anti-phishing attack model for detection of phishing attacker behaviors.[202] The model developed by Tseng et al. can also be used to automatically improve the contents of anti-phishing education game by extending the original phishing pages and model new pages.[203] To transform the continuously increasing anti-phishing knowledge to learning materials and to make the materials more readable and easy for students to learn, Yang et al. classified anti-phishing knowledge into different levels of learning and proposed an anti-phishing

[200] Lin, Chun-Li and Cheng, Ming-Her (2008), 'The one-time Password Authentication Protocol of against Phishing Attack', *2008 Management and Application of Information Communication Technologies Conference* (Kaohsiung, Taiwan: Shu Te Univeristy), 216-25;Sun, Hung-Min, Chen, Yao-Hsin, and Lin, Yue-Hsun (2012), 'oPass: A user authentication protocol resistant to password stealing and password reuse attacks', *Information Forensics and Security, IEEE Transactions on,* 7 (2), 651-63.

[201] Lee, Lung-Hao, et al. (2012), 'Context-aware web security threat prevention', in Ting Yu, George Danezis, and Virgil Gligor (eds.), *Proceedings of the 2012 ACM conference on Computer and communications security* (Raleigh, North Carolina, USA: ACM), 992-94;Lee, Lung-Hao, et al. (2013), 'User-Centric Phishing Threat Detection', *In Poster Session of the 34th IEEE Symposium on Security and Privacy* (San Francisco, California, USA);Lee, Lung-Hao, et al. (2014), 'Users' behavioral prediction for phishing detection', in Chin-Wan Chung, et al. (eds.), *Proceedings of the companion publication of the 23rd international conference on World wide web companion* (Seoul, Korea: International World Wide Web Conferences Steering Committee), 337-38.

[202] Tseng, Shian-Shyong, et al. (2013), 'Building a Frame-Based Anti-Phishing Model based on Phishing Ontology', *The 7th International Conference on Advanced Information Technology* (Chaoyang University of Technology, Taichung, Taiwan).

[203] Tseng, Shian-Shyong, et al. (2011), 'Automatic content generation for anti-phishing education game', *2011 International Conference on Electrical and Control Engineering (ICECE)* (Yichang, China: IEEE), 6390-94.

education game that will provide students with game missions according to their different learning achievements.[204]

Although significant progress has been made in developing anti-phishing solutions in Taiwan over the past five years, it is an imbalanced development which apparently only focuses on the discussion of technology with very little attention on the countermeasures that can be developed in other dimensions. There is a distinct shortage of scholarly literature on the legal regulation of phishing in Taiwan, with only an article written by Professor Hsueh, Chih-Jen in 2013.[205] This article explored whether or not there is a need to make a sui generis phishing law by examining the application of the current criminal laws to phishing. The author suggested that it is not absolutely necessary to add a phishing-tailored law for two reasons. One is that the conduct of phishing is fully covered by the current laws. Interestingly, the other reason is that lawmaking is far less effective in deterring phishing attacks than enhancement of preventative measures, users' information security awareness, and criminal investigation capability.

However, Hsueh's work only looked into the criminal liability of phishing and its focus was on the Taiwan Criminal Code. While, the Criminal Code of Taiwan is considered in Chapter 4, the objective of this thesis is to consider wider aspects of national and international legal regulation in its context. In addition to the Criminal Code, the practice of phishing usually contains several steps (see Chapter 2, section 2.4.) which may involve violation against trademark or copyright laws. More importantly, phishing is a direct infringement of the right to information privacy in its attempt to acquire confidential information through deception or malware infection. Phishing attacks can be

[204] Yang et al. (2012), op. cit.

[205] Hsueh (2013), op. cit. Professor Hsueh, Chih-Jen was an assistant professor of the law department of National Cheng Kung University at the time when this article was published. He now is an assistant professor of the law department of National Taiwan University. More discussion of Hsueh's work, see Chapter 4, section 4.4.2.3.

blocked and its damage can be decreased by strengthening the legal requirement for data holders in terms of information management and protection. To phishing, law should not only be a corrective measure providing civil remedy or criminal penalty, it can also act as a preventative measure by enhancing information security. Chapter 5 examines the influence upon the right to information privacy caused by phishing and explores the contribution of the Taiwan Personal Information Protection Act to the regulation of phishing. Moreover, the legal regulation of phishing is unlikely to be achieved within a single country only as phishing is free of geographical boundaries. It is always important to look at the laws in other domains to seek harmonization of legal standards and cooperation of legal enforcement with other countries. Chapter 6 studies the legislative responses to phishing at both the national and international levels and looks into the international legal approaches that have been taken with regard to coordinating the actions against phishing.

3.5. Slow and insufficient progress in anti-phishing work

During the period between 1990 and 2003, Taiwan undertook a series of legal amendments to the Criminal Code which brought the Criminal Code into a new era by putting in an individual chapter specially designed for the regulation of computer crimes. The new chapter – chapter 36 'Offences against Computer Use', which came into force in June 2003, makes it an offence that a person access to another person's computer or obtain, delete, or alter another's person's electromagnetic records without authorization (Art. 358 and 359). It also criminalizes unauthorized interference with computers (Art. 360) and production of computer programs for the commitment of the offences laid down in this chapter (Art. 362).

The purpose of the above enactment was to protect the security of computer use, the domination of electromagnetic records and computer efficiency. However, while the new legislation have made a significant contribution to addressing hacker problem to certain extent, it appears to have provided rather limited help to deal with phishing largely due to inappropriate interpretation of the laws and failure of prosecuting phishers. The Chapter 4 of this thesis provides an outline of the legislative background and investigates the problems with the practical application of the new legislation to the case of phishing.

In addition, Taiwan enacted the Personal Information Protection Act in May 2010 which involved a large-scale amendment to the previous law, the Computer-Processed Personal Data Protection Law. The Act provides that a private data controller should take necessary technical and organizational measures to prevent personal data from being stolen (Art. 27.1) and makes data controllers liable for illegal collection, processing and usage of personal information due to their non-compliance with the requirements provided by the Act (Art. 28 and 29). While the Act is generally regarded as a milestone in the development of Taiwan's information protection laws, this thesis discusses whether the Act is capable of providing substantial protection for personal information against illegal access. There is always a gap between ideal and reality. The gap mainly comes from a lack of independent privacy protection authority empowered to supervise data controllers and oversee their compliance with the data protection provisions and the concession of the executive power of Taiwan to the interests of data controllers when facing a conflict between personal information protection and business interests. This thesis draws on the key problems observed from the Act which result in insufficient protection of personal data in Chapter 5.

The Taiwan government did not pay proper attention to anti-phishing work until recently. Given the necessity of integrated effort of computer security teams across different sectors in responding to arising security incidents, the TWCERT/CC called on government agencies, ISPs, academic units, computer security industries and business corporations collectively to build up a joint defensive alliance, named the Taiwan information Security Strategic Alliance (hereinafter, the Alliance) which was formally established on 23 September 2010. Prior to the establishment of the Alliance, the Alliance members reached a consensus that anti-phishing work should be placed in their prioritized tasks. Accordingly, TWCERT/CC introduced the Taiwan Anti-Phishing Working Group (TAPWG) in July 2010 and activated a phishing reporting system known as the Anti-Phishing Notification Window (APNOW) in October in the same year.

The APNOW provides an internal and external platform for reporting suspected phishing attacks and streamlines the processing procedures of phishing reports by passing the report to the corresponding CERTs, including CERTs of commercial, academic and governmental network, or to the ISPs directly after it receives a report to suspected phishing emails or phishing sites. The establishment of the TAPWG and the APNOW set a landmark in Taiwan’s development of anti-phishing work and reflected Taiwan’s ambitions to combat phishing through collective effort and an institutional network. The APNOW is supposed to be helpful to tackle phishing by quickly coordinating the action between different teams to remove the phishing sites hosted in Taiwan or other countries; however, this thesis demonstrates the defects of the APNOW and its limited function in regulating phishing by providing an exploration of the structure, processing procedures, practical operation and effectiveness of this mechanism in Chapter 7. Furthermore, by means of in-depth interviews with the experts from different stakeholders, this thesis examines the effectiveness of Taiwan’s anti-phishing work by providing an insight of the work engaged by the relevant stakeholders and the key factors that have handicapped their performance in the regulatory network of phishing.

3.6. Obstacles to engaging in international cooperation

The political tension between Taiwan and China has not only made Taiwan a primary target of phishing attacks originated in China but also drawn Taiwan into international affairs complexities. As indicated by Wang, if the mainland fails to reunify with Taiwan, the revival of the Chinese nation would not be meaningful to many Chinese people, who do not wish the sovereignty of China, which includes the region of Taiwan, to be altered.[206] China considers Taiwan only a local government under Beijing's command but one that will be permitted to enjoy a high degree of autonomy, like Hong Kong and Macao. This is known as '*one country, two systems*' model.[207] To serve the national goal, China has been taking a hardened posture on the Taiwan issue in making and implementing its international policies in order to deter Taiwan form moving towards de jure independence.[208]

Since the day the ROC walked out of the United Nations in 1971, Taiwan has struggled to regain the international recognition it had once enjoyed. While the attempt to obtain official international status still remains difficult in the short run due to the overwhelming power of China, focusing on membership in international organizations has become an alternative way for Taiwan to seek a space in international society.[209] However, pressure from China continues to impede Taiwan's attempts to participate in international arena by blocking Taiwan's attendance in international conferences or denying Taiwan's membership or/and observer status to join the international

[206] Wang, Jisi (2004a), 'China's Changing Role in Asia', *The Rise of China and a Changing East Asian Order, Tokyo, Japan: Japan Center for International Exchange*.

[207] Wang, Te-Yu and Liu, I-Chou (2004), 'Contending identities in Taiwan: Implications for cross-strait relations', *Asian Survey,* 44 (4), 568-90.

[208] Lee, Che-Fu (1997), 'China's Perception of the Taiwan Issue', *New Eng. L. Rev.,* 32, 695.

[209] Zaid, Mark S (1997), 'Taiwan: It Looks like It, It Acts like It, but Is It a State-The Ability to Achieve a Dream through Membership in International Organization', *New Eng. L. Rev.,* 32, 805.

organizations, for example, World Health Organization (WHO), International Monetary Fund (IMF) and the United Nations.[210]

Asia-Pacific Economic Cooperation (APEC) has been the major political battleground between Taiwan and China since Taiwan joined APEC in 1991 under the name ‘Chinese Taipei’. Although APEC is the most important intergovernmental organization where Taiwan is accepted as a full member, Taiwan is not allowed to participate in negotiation processes involving political issues as an equal member and the president or high level of government officials of Taiwan such as foreign minister or department directors are excluded from APEC Ministerial Meeting because of Chinese opposition on political grounds.[211]

The political force from China has been a major hindrance to Taiwan to equally participating in intergovernmental activities and fully engaging in international cooperation that requires statehood. Because of its disadvantaged international status, Taiwan has not only been excluded from most international organizations but also been prevented to become a signatory for most international conventions. As treaties are concluded based on nation-to-nation relationship, the countries which recognize China are unable to enter into binding agreements with Taiwan.[212] The obstacle to pursuing bilateral or multilateral cooperation with most countries in the world further aggravates the difficulty of Taiwan in combating phishing. The situation becomes even more complicated when the primary threat of phishing attacks and the obstacle to Taiwan’s regulation of phishing come

[210] FormosaFoundation 'Taiwan's participation in international organizations', [Ambassador Program Issues 2013], <http://www.formosafoundation.org/ambassador-program/documents/issues/TW-International-Participation.pdf>, accessed 15 July 2014.

[211] Wu, Ling-Jun (2001), 'The current role and future adjusment of Taiwan in APEC', *NPF Research Report* (National Policy Foundation);Yang, Phillip Y. M. (1997), 'Taiwan's approaches to APEC: economic cooperation, political significance, and international participation', *International Conference on Canada-Taiwan Relations in the 1990s* (National ChengChi Univeristy, Taipei, Taiwan).

[212] Chang (2012), op. cit.

from the same source, namely, China. As phishing frequently has a transnational dimension, an anti-phishing solution which can only be practiced within the border is a mere armchair strategy. How to avoid the political hindrance and expand Taiwan's international participation in anti-phishing campaign at international level is a very important lesson that needs to be learnt.

3.7. Conclusion

Cyberspace is free of territorial borders. An overwhelming majority of phishing attacks are operated from one country to another. This makes every country in the world a potential object of phishing as long as it has connection to the Internet. Taiwan has been suffering severe threats posed by growing phishing attacks, as it is not only a major target but also one of the top countries hosting phishing websites. This may be blamed on the fact that Taiwan has high levels of Internet usage and Internet connectivity but in the meantime it has weak management of web security and considerable volume of bot-infected computers. Another factor that significantly elevates the risk of phishing to Taiwan is the vigorous malicious attacks from China, which are largely assisted by the commonality of language and cultures and encouraged by political motives. While Taiwan desires effective regulation of phishing, it has experienced a variety of difficulties in achieving this. The research development of phishing countermeasures of Taiwan is slow and uneven and only concentrates on the technical solutions with little respect for measures in other areas. The movement of the anti-phishing work in Taiwan has been lagging and its performance is unsatisfactory. Most importantly, phishing is often committed beyond borders and needs to be addressed by an international approach which usually involves harmonization of legal standards and international legal cooperation. Nevertheless, Taiwan has been suffering crucial political obstacles to engaging in international conventions or agreements and legal enforcement cooperation. Taiwan provides a good illustration of both the general and particular difficulties in regulating phishing and the efforts that should be endeavored for the development of an effective regulatory framework against phishing.

The next chapter begins the examination of the legal regulation of phishing in Taiwan by first exploring Taiwan’s legislation relating to phishing and focusing especially on the capability of the Criminal Code.

CHAPTER 4 TAIWAN’S PHISHING LEGISLATION

Synopsis

This chapter examines the extent to which Taiwanese laws are able to deal with phishing, with a particular focus on the Criminal Code. A phishing attack is very often a transnational phenomenon and usually involves violation against protection of different legal interests. The chapter first looks at the issue of jurisdiction followed by an overview of the legislation related to phishing, including the civil law, trademark law, copyright law, and personal information protection law.

The chapter concentrates on the examination of the Criminal Code and particularly two major legal amendments to the Criminal Code, the 1997 Act and 2003 Act, focusing especially on the difficulties in applying the relevant provisions to phishing and highlights the challenges posed by phishing to law enforcement work.

4.1. Introduction

Law has been a typical regulator that usually serves as an essential tool to control certain behaviours by setting rules and punishing the violators in either the real or virtual world. To make phishing attackers accountable for their conduct, the most fundamental step is to ensure that phishing is a legally impermissible behaviour. Phishing has raised a variety of legal issues but has appeared to inspire not much legal scholarship in phishing regulation. Chapter 2 reviewed the corresponding measures that have been developed to prevent or disrupt phishing attacks and found that there was a dearth of legal scholarship in comparison with other research areas, in particular technological research. A study of the role of laws in the regulation of phishing is hence necessary to fill the gap existing in the current anti-phishing research.

Chapter 3 demonstrated that Taiwan has been one of the major targets as well as the main sources of phishing attacks, which makes it pressing to pursue a practicable regulation of phishing. However, Taiwan has been struggling with establishing and enforcing effective regulation of phishing due to a variety of reasons, comprising both the general factors that have been discussed in Chapter 2 (section 2.5) and Taiwan-specific factors that have been examined in Chapter 3. A study of Taiwan's experience in regulating phishing can provide a clear understanding of the reasons which make an effective regulation of phishing so difficult and the problems to be addressed to better deal with phishing. Although the focus of this research is especially on Taiwan's legal regulation of phishing which is dealt with in this chapter and Chapter 5, the global nature of phishing makes it necessary to also look into the regulation in other domains and international regulation, which will be examined in Chapter 5 and 6.

Phishing, for its attempt to target unauthorized acquisition of a variety of personally sensitive and confidential information via Internet networking, constitutes an offence against computer and information security and also a direct infringement of personal information privacy. The focus of the examination of Taiwan's legal regulation will therefore be the Criminal Code, with deals with the laws relating to cybercrime and the Personal Information Protection Act. This chapter examines Taiwan's legislation relating to phishing, primarily focusing on the Criminal Code and the two reforms, the 1997 and 2003 Act. The chapter also addresses the Personal Information Protection Act (the PIP Act), but only briefly, with a focus on the comparison between the PIP Act and its previous law. The following chapter will provide a detailed examination of the relationship between phishing and information privacy and an exploration of the work that personal information protection laws can do in combating phishing, both nationally and internationally.

Phishing is frequently a transnational phenomenon which usually involves multiple jurisdictions. This chapter commences by looking into the issue of which jurisdiction may be involved in a phishing case. This is followed by an overview of the laws involved in dealing with phishing combined with an analysis of their relevance to phishing. Taiwan undertook two major legal amendments to the Criminal Code between 1990 and 2003, which brought the Criminal Code into a new era in responding to the emergence of new offences consequent on the dramatic growth of information technologies. This chapter primarily concentrates on the extent to which the Criminal Code is able to deal with phishing by investigating the applicability of the 1997 and 2003 Act to the conduct of phishing. There are several studies that examined the issue of cybercrime in Taiwan,[213] most of which focused on an analysis of the demographic characteristics of cyber criminals and the characteristics of computer crimes happening in Taiwan. As I have mentioned in Chapter 3,[214] only one piece of work could be found that specifically examined the applicability of Taiwanese Criminal Code to the conduct of phishing.[215] While Hsueh concluded that phishing can be flawlessly covered by the existing laws of Taiwan, this chapter leads to a different conclusion.

This chapter looks into the arguments, both academically and practically, over the elements of the provisions in relation to phishing and explores the negative influence that might have produced upon the regulation of phishing. This chapter also addresses the difficulty in arresting and prosecuting phishing attackers and examines the challenges to Taiwan's criminal law enforcement.

[213] Chang (2012), op. cit;Jen, Wen-Yuan, Chang, Wei-ping, and Chou, Shih-chieh (2006), 'Cybercrime in Taiwan–an analysis of suspect records', in Hsinchun Chen, et al. (eds.), *Intelligence and Security Informatics* (Springer), 38-48;Liao, You-lu and Tsai, Cynthia (2006), 'Analysis of computer crime characteristics in Taiwan', in Hsinchun Chen, et al. (eds.), *Intelligence and Security Informatics* (Springer), 49-57;Lu, Chi-Chao, et al. (2006), 'Cybercrime & cybercriminals: An overview of the Taiwan experience', *Journal of Computers,* 1 (6), 11-18;Wang, Jau-Hwang, et al. (2006), 'Technology-based Financial Frauds in Taiwan: Issues and Approaches', *IEEE International Conference on Systems, Man and Cybernetics, 2006* (6; Taipei, Taiwan: IEEE), 1120-24.

[214] See Chapter 3, section 3.4.

[215] Hsueh (2013), op. cit.

4.2. Jurisdiction

"*In the networked world, no island is an island*."[216] Cyberspace is borderless, that a crime can be committed without the limitation of a geographical boundary as long as criminals have access to the Internet.[217] Cybercrime is often operated from one country to another in a remote way, and the states of domicile or residence of the perpetrator and the victim are usually different. Also, the place where a cybercrime is committed tends not to be where the results are felt.

Traditional jurisdiction, including the jurisdiction to prescribe, adjudicate, and enforce, has been primarily based upon the concept of territory.[218] The transnational and immaterial character of cybercrimes has posed a challenge to the current initiatives based on geographical boundaries and deciding their jurisdiction has become a controversial issue. This section examines the issue of which jurisdiction may be involved in a phishing case under the laws of Taiwan.

4.2.1. Legislation

The Criminal Code, in principle, applies to an offence committed within the territory of Taiwan (Art. 3).[219] According to Taiwan's Criminal Procedure Code, a court of the place where an offence has

[216] McConnel (2000), 'Cybercrime…and punishment? Archaic Laws Threaten Global Information'. <http://www.witsa.org/papers/McConnell-cybercrime.pdf>, accessed September 21 2014.

[217] Svantesson, Dan Jerker B (2005), 'The characteristics making Internet communication challenge traditional models of regulation–What every international jurist should know about the Internet', *International Journal of Law and Information Technology,* 13 (1), 39-69.

[218] Koops, Egbert Jakob and Brenner, Susan W (2006), 'Cybercrime jurisdiction - an introducation', in Egbert Jakob Koops and Susan W Brenner (eds.), *Cybercrime and Jurisdiction; A Global Survey* (Hague: T.M.C. Asser Press), 3-4.

[219] The Criminal Code can also apply to the offence committed outside the territory under certain exceptional circumstances, including a. the offences enumerated in Art. 5 based on the universality principle and protective principle; b. the offences listed in Art. 6 committed by a public official; c. the offences committed by any national which are not specific in Art. 5 and 6 but are punishable by no less than 3 years of imprisonment and are punishable by the law of the place where the offence is committed (Art. 7); or d. the offences provided under Art. 7 committed by an alien against a national Taiwan (Art. 8). Universal jurisdiction allows any nation to claim criminal jurisdiction over an

been committed or where an accused is domiciled, resides, or is located shall claim jurisdiction over the case (Art. 5 I). The place where an offence has been committed shall include the places of both the conduct and result (Art. 4 of the Criminal Code).[220] However, how to recognize the place of commitment is always a problem in the case of cybercrime because of its transnational nature. In Taiwan's judicial practice, inconsistent opinions have arisen about the recognition of the place where a computer or Internet-related offence has been committed.

4.2.2. Inconsistent judicial interpretations

In a case where a man is accused of posting an advertisement for selling munitions and firearms via a website which was available to the general public, the Taipei District Court decided that the place where any person within that place could access that advertising information was the place in which the offence was committed.[221] According to the court's opinion, Taiwan shall have jurisdiction over crimes involving unlawful information in cyberspace as long as any person within the Taiwanese jurisdiction can have access to this information.

Under the provision of the Criminal Code, as aforementioned, both the place of conduct and the place of result are deemed the commitment place of an offence (Art. 4). Wang argued that the foregoing interpretations failed to indicate clearly whether the place where the munitions advertisement is accessed is the place of conduct or the place of result.[222] Most importantly, in this

offender for certain crimes, irrespective of the commitment place, nationality, country or residence of the alleged offender or victim. Protective jurisdiction provides a state to assert jurisdiction over a person whose conduct threatens the security of that particular state or the functional operation of its government even when this conduct has been committed abroad. Randall, Kenneth C (1987), 'Universal jurisdiction under international law', *Tex. L. Rev.,* 66, 785. Phishing is obviously not covered by universal or protective jurisdiction. In addition, the penalty for phishing is no more than 5 years of imprisonment (Art. 339, 359). To conclude, the Criminal Code cannot apply to phishing if it is committed abroad pursuant to the above provisions.

[220] *Sup. Ct., Criminal Division, 72 Tai-Shang No. 5894 (1983) (Taiwan)*

[221] *Taipei Dist. Ct., Criminal Division, 87 Yi No. 428 (1998) (Taiwan)*

[222] Wang, Ming-Yong (2004b), 'Criminal Jurisdiction over Computer Crimes', *The Online Symposium of the Academic Research and Practical Deliberation Conference 'Cyberspace: Information, Law and Society* (6), 25-34.

interpretation, the court excessively extended the recognition of the place of the offence commitment to widen Taiwan's jurisdiction over cybercrime. Cheng argued that this excessive extension of Internet jurisdiction was inappropriate as it could negatively influence the development of cyber activities.[223]

The above interpretation of the Taipei District Court was later narrowed by the Taiwan High Court in *89 Shang-Su No. 1175* in 2000.[224] The Taiwan High Court considered that the extreme interpretation of the place of offence commitment may make every corner of the world fall under Taiwan's jurisdiction, which could lead to improper intervention in other countries' jurisdictions and cause difficulties for Taiwan's courts in exercising its jurisdiction. In addition to the place where the perpetrator was domiciled and the place where the web page host was allocated, the Taiwan High Court decided that the jurisdiction over cybercrime should also take account of a. the place where the email host was located, b. the place where the host that was used to install the web page or transmit the data was located, or c. other specific places involved in different cases. This interpretation of the Taiwan High Court regarding criminal jurisdiction over cybercrime has been followed in subsequent cases.

4.2.3. The problem of jurisdiction over phishing cases

The application of the Criminal Code is primarily based on territorial jurisdiction (Art. 3), supplemented by universal (Art. 5), protective (Art. 5), and national jurisdiction (Art. 6-8). As the offences related to phishing are not the same at those specified in Art. 5 and 6, nor offences which are punishable by no less than three years of imprisonment (Art. 7 and 8), jurisdiction over a phishing case is hence based on the territoriality principle (Art. 3 and 4, and Art. 5 I of the Criminal

[223] Cheng, C. I. (2009), 'The Extension and Tension of Internet Jurisdiction', *Socioeconomic Law and Institution Review,* 43, 127-60.

[224] *Taiwan High Ct., Criminal Division, 89 Shang-Su No. 1175 (2000) (Taiwan)*

Procedure Code). Accordingly, a Taiwanese court shall claim jurisdiction over a phishing case where the offender is domiciled, resides, or located in Taiwan or where the offence takes place in Taiwan, with the place of commitment defined narrowly by the Taiwan High Court decision.

Phishing is a malicious activity that directly targets the acquisition of confidential information performed in electromagnetic format. The Criminal Code makes it an offence to obtain electromagnetic records from another person without authorisation (Art. 359). In one case,[225] a man was accused of the unauthorised obtainment of electromagnetic records by acquiring the property in the form of New Taiwan Dollars (NTD) 30,000 of Kao, a player of an online game, by inputting Kao's account name and password to log on to the game, and transferring the property to another account. The court followed the foregoing Taiwan High Court's opinion in *89 Shang-Su No. 1175* and considered the place where (i) the perpetrator accessed the online game web server and input the victim's login account name and password to acquire the electromagnetic records or (ii) the online game web server and host was located as the place where the offence had been committed.

Therefore, according to the Criminal Procedure Code (Art. 5 I) in conjunction with the above judicial interpretation of the commitment place, Taiwan courts shall exercise jurisdiction over a phishing case in any of the following three circumstances:

a. The phishing perpetrator accesses the phishing website and obtains the victims' confidential information within the territory of Taiwan;
b. The phishing website is hosted in Taiwan; or
c. The perpetrator resides or stays in Taiwan.

In other words, the Taiwanese courts cannot claim jurisdiction over a phishing case if the offender

[225] *Taipei Dist. Ct., Criminal Division, 93 Yi No. 697 (2004) (Taiwan)*

accesses the phishing website and obtains information abroad and the offender, without respect to his/her nationality, as well as the phishing host is located in another country.

However, as we learnt from Chapter 3 (section 3.3.4), in most phishing attacks that target Taiwan's users, neither the attackers nor the phishing hosts are usually in Taiwan. As a result, an overwhelming majority of phishing cases may be dismissed by the Taiwan courts due to their lack of jurisdiction, even though these attacks are launched by a Taiwan national who resides abroad and may have caused enormous losses to a great number of Taiwan users.

In addition, Art. 4 of the Criminal Code explicitly defines the offence commitment place as the place of conduct and damage. A court of the place where a phishing attack causes damage shall also take jurisdiction over this case. However, the above interpretation made by Taipei District Court in *93 Yi No. 697* only recognized the place of conduct as the offence commitment place with no mention about the place of damage, which caused an evident loophole in the protection of the litigation rights of the phishing victims in Taiwan.

Too broad recognition of the place of offence commitment in a cybercrime case may cause inappropriate interventions in other countries' jurisdictions; nevertheless, too restrictive recognition of the offence commitment place, especially in a cross-border cybercrime case, may lead to the inadequate protection of the victims of the crimes. The borderless nature of cyberspace enables phishers to perform attacks freely without geographical restriction, with the vast majority of phishing being committed across more than one country. Phishing attackers, phishing hosts, and victims may be located under two or even three different jurisdictions. In my opinion, in addition to the court of the place where the phishers and host are located, the court of the place where the damage from the phishing occurs should also have jurisdiction over a phishing case in order to conform to the legal requirement of Art. 4 of the Criminal Code and also better protect the litigation rights of the phishing victims.

4.3. Relevant Legislation to Phishing Activity

Phishing is a malicious cyber-attack which targets unauthorized acquisition of personal sensitive information or financial credentials often through the use of a counterfeit email or/and a bogus website. To better convince the recipients and to deceive them into divulging their financial or personal confidential information, a phishing attacker mostly forges a phishing message and/or a phishing website by imitating the genuine message or website and copying the trademark which may have been registered by the legitimated business or organization. Therefore, phishing not only constitutes an offence against criminal law but also involves violation against legal protection of civil rights, trademark, copyright and personal information. This section considers the civil law, trademark law, copyright law, and personal information protection law and identifies how they are related to phishing. The examination of the criminal law is in section 4.4.

4.3.1. Civil law

The full enjoyment of privacy concerning personal information is an important element in personality development. Phishing, which targets unauthorized acquisition of personal sensitive information or financial credentials, apparently constitutes an infringement of the right to personal information privacy. Under the tort law laid down in the Civil Code (Art. 184), the injured party may claim for the damage caused by the phishing attack.

Under the provision of the Application Laws for Foreign-related Civil Law (hereinafter, International Private Law) of Taiwan, claims grounded on tort shall principally be governed by the law of the State in which the tort was committed, without difference (Art. 25.1). However, to provide more flexible choices of law for claims grounded on tort committed by disseminative means, such as the "press, radio, television, computer Internet or other media methods", a new article was added to the International Private Law in May 2010 which provides three choices of laws at the option of the injured party (Art. 28).[226] In the case of claims founded on tort by phishing, the above provision shall be applied to solve the problem of a conflict of laws.

4.3.2. Copyright Act

It is very commonly noted on a web page that all rights have been reserved. Any breach of copyright is strictly prohibited once someone obtains the copyright of the whole contents of the web page, including the words, pictures or web page layout. The creation of a phishing web page, for example, a bank website or a login page of an email account or other online service, by mimicking the authentic websites is deemed as a "reproduction of work" (Art. 3.1(1) and (5)) [227] which causes a violation against the copyright of the rightful owner.

A person who infringes copyright shall compensate for damages caused by infringement and shall remove or prevent the infringement according to the claim made by the copyright owner (Art. 84, 88). A counterfeit phishing website is usually openly displayed and made freely accessible by unsuspecting visitors to achieve the fraudulent purpose. Besides civil liability, a person who distributes the copy or with the intention to distribute by publicly displaying it is punishable by imprisonment of up to three years and may be additionally fined NTD 70,000-750,000 (Art. 91-1.2).

[226] The three choices of laws include: a. the law of the State in which the tort was committed or the law of the State of domicile of the tortfeasor if the place of commitment cannot be identified; b. the law of the State in which the injuries or the infringement have occurred if the tortfeasor should have foreseen that the injuries would occur in that State; and c. the law of the State of the injured party if the act caused an infringement of personality rights (Art. 28 I).

[227] "To reproduce", according to the Copyright Act (Art. 3.1(5)), means to "reproduce directly, indirectly, permanently, or temporarily a work by means of printing, reprography, sound recording, video recording, photography, and written notes, or otherwise." "Work" means a creation within a "literary, scientific, artistic, or other intellectual domain" (Art. 3.1(1)).

An important amendment was made in May 2009 to the Copyright Act in respect of the liability of Internet service providers for the breach of copyright by users through accessing their services. Prior to May 2009, Internet service providers (ISPs) faced a high risk of being sued jointly with a person who has violated copyright by posting infringing materials or engaging in similar activities through using its service by a copyright holder. The great accountability of ISPs for the online infringement of copyright was criticised for having had a detrimental influence upon Internet industrial development, as ISPs in fact are almost unlikely to review all of the content posted via their service and detect every breach of copyright facilitated by it use.[228]

The Copyright Act Amendment Bill, which was enacted in May 2009 and was based largely upon the ISPs' liability limitation regime set out in section 512 of the 1998 U.S. Digital Millennium Copyright Act (DMCA), provided a clear definition of ISP (Art. 3.1(19))[229] and established safe harbour provisions (Art. 90-4-90-8, 90-10) that ISPs may avail themselves in order to limit liability for online copyright infringement by their users. A notice/take down mechanism has been established for caching, information storage, and search service providers can now claim the protection of a safe harbour (Art. 90-6-90-8). ISPs, except for connection service providers, have been required to respond expeditiously to any notification by a copyright holder of infringement by users of the service provided by removing or disabling access to the alleged contents or related information.

Accordingly, information storage providers should remove or disable access to an imitative phishing web page at the request of the copyright holder promptly in order to avoid liability for damage caused by the infringement of the copyright. Internet connection service providers (ICPs)

[228] See the statement on the draft amendment to the Copyright Act.

[229] ISP means those who provide the following services: connection service provider, caching service provider, information storage service provider, and search service provider (Art. 3.1(19)).

are not obligated to do so, because it is difficult for them to assess the content of a website due to the nature of their work.[230] Although it can actually limit the potential damage caused by phishing attacks if ICPs can disable access to phishing websites as soon as they are informed of them, the protection of general Internet users from fraud crimes committed through counterfeit websites, after all, is not the focus of this Act. The priority of the Copyright Act is the protection of the rightful owners of the copyright.

4.3.3. Trademark Act

Knowingly using a trademark which is identical with or similar to another person's registered trademark without the consent of the trademark right holder, and hence damaging the reputation of the trademark or confusing consumers about goods or services is seen as an infringement of the trademark right (Art. 70.2). Unauthorised use of a trademark registered by any enterprise or organisation to fake a web page or email and so tricking individuals to obtain their confidential information violates the protection of trademark rights under the above act and the trademark right holder may claim compensation for damages and request excluding infringement (Art. 69.1 and 69.3).

4.3.4. Personal Information Protection Act

Personal information is not only the main target of phishing attacks but also provides valuable materials for phishers to craft a highly convincing phishing message for a specific target that is very likely to lead to serious data breach incidents involving enormous financial damage and loss of personal data. The protection of personal information against illegal collection is a fundamental component of phishing regulation and should be guaranteed by laws.

[230] See Art. 90-5, the Amendment Explanatory Memoranda of the Copyright Act 2009.

However, very little scholarship could be found that investigates the regulatory relationship between the personal information protection laws and phishing, both nationally and internationally. As we saw in Chapter 2 and 3, current international and Taiwan legal debates over phishing mostly concentrate on criminal rules and reforms,[231] and the challenge to law enforcement.[232] Criminal law is undoubtedly important to the regulation of phishing by deterring phishing attempts through imposing the threat of punishment. Yet, this thesis argues that the function of law in regulating phishing is more than a corrective measure. It can also prevent phishing by ensuring protection of personal information against illegal or unauthorised access or collection.

Taiwan passed it first personal information protection law, namely the Computer-Processed Personal Data Protection Law (the CPPDP Law), in 1995. In order to provide adequate legal protection for personal data to respond to the increasing sophistication of computer technology and also to better harmonize with international legal standards relating to information privacy, especially the APEC Privacy Principles, Taiwan initiated a large-scale amendment to the CPPDP Law and passed a new enactment of the Personal Information Protection Act (PIP Act) in 2010.[233]

This section first describes the shortcomings of the CPPDP Law concerning collection of personal information by individuals and then examines whether the PIP Act provides better protection or causes adverse effect on the protection of personal information against unauthorised collection.

[231] Almerdas (2014), op. cit;Bainbridge (2007), op. cit;Dinna et al. (2007), op. cit;Granova and Eloff (2005), op. cit;Hsueh (2013), op. cit;Lynch (2005), op. cit;Mcgowan (2006), op. cit;Mcnealy (2008), op. cit;Nappinai (2009), op. cit.

[232] Dinna et al. (2007), op. cit;Krebs, Brian (2004), 'Companies Forced to Fight Phishing', *The Washington Post*. <http://www.washingtonpost.com/wp-dyn/articles/A61916-2004Nov19.html>, accessed September 15 2014;Lynch (2005), op. cit;Stevenson (2005), op. cit;Sullins (2006), op. cit.

[233] The Executive Yuan put the PIP Act into practice in two stages. The Personal Information Protection Act, together with its enforcement rules, largely came into effect in October 2012, except for Art. 6 and 54 given the difficulty of implementation. The resistance of Taiwanese enterprises to two controversial provisions, Art. 6 (special categories of sensitive data) and Art. 54 (duty to notify data subjects of personal information indirectly collected without consent pre-amendment), eventually forced the Executive Yuan to suspend the implementation of the above two articles. The inappropriate influence of business power on the legal protection of personal information will be further explored in Chapter 5, section 5.3.3.1 and 5.4.5.

4.3.4.1. Pre-amendment: the Computer-Processed Personal Data Protection Law

Provisions:

The CPPDP Law was only valid for 'computer-processed data', excluding 'manually-processed information' (Art. 1). Under the CPPDP Law, the subjects liable for the breach of personal information protection included government agencies (Art. 3 (6)) and the enterprises, groups or individuals of the specific categories enumerated, but not covering all non-government agencies (Art. 3 (7)).[234]

A non-governmental agency shall not collect or process any personal data unless they are specified for a particular purpose and comply with any of the following (Art. 18):

> (1) Written consent of the principal;
>
> (2) An agreement or similar contractual relationship with the principal;
>
> (3) The information is already known to the public or
>
> (4) There is a need for academic study and no material adverse effect will be caused to the major interests of the principal; and
>
> (5) Other exceptional conditions empowered by this Law and other laws and regulations

A person who intended to make profit for himself by violating the provisions of Art. 18 resulting in

[234] The specific categories of enterprises, groups or individuals, including: credit search businesses and groups or individuals whose major line of business is to collect or process personal data by computer; hospital, schools and the telecommunication, financial, securities, insurance and mass communication industries; and other businesses, groups, or individuals designated by the Ministry of Justice in conjunction with the government authority in charge of such industry at the central government level (Art. 3 (7)).

injury to another shall be punished under the provision of Art. 33. In addition, Art. 34 provided punishment to a person who intended to make unlawful gains for himself or for a third party or intended to infringe upon the interests of another by illegally outputting a personal data file thus causing damage to another. “Outputting personal data” includes illegally sending personal data from non-governmental agency to the data receiver and/or directly obtaining data from the agency.[235]

Shortcomings:

The restriction laid down by the CPPDP Law on both the objects and subjects opened a loophole in the protection of non-computer-processed personal data and a breach of regulation of data collection by non-government agencies.

Another major defect of this Law is that it provided ample exceptional conditions along with inappropriate use of indeterminate legal concepts for the prohibitions of data collection. As the data subject is entitled to have inviolable autonomy over his personal information and refuse unnecessary intervention,[236] any obtainment, processing, or use of personal information without the consent of the data subject should be strictly prohibited. However, according to Art. 18, the data subject’s written consent was only one of the conditions for permitting the collection of personal data and can easily be excluded by other exceptional conditions.

More importantly, it did not constitute a crime to collect another person’s information if it was already known to the public or the collection was for research purposes, as long as there is no violation of the data subject’s “*major interests*” (Art. 18 (3) and (4)). “*Major interests*” – an

[235] Shiu, Wen-Yi (1991), *The Theory of Personal Data Protection Law* (Taipei: San-Min Book Co. Ltd).

[236] Chiou, W. T. (2009), 'Comments on the Constructional Problems of the Amendment Bill of the Computer-Processed Personal Data Protection Law – Based on the Ideologies of Information Autonomy and Information Privacy', *Yue-Dan Jurisprudence Magazine*, 168, 172-89.

indeterminate legal concept – was used as a criterion to decide the legality of a collection of personal information. An indeterminate legal concept is designed by the legislators deliberately to leave more flexible room for the administrative authorities to determine the content of the concept. However, in the case there is no specific independent authority that takes charge of the task of personal information protection, the use of indeterminate legal concepts very likely will lead to divergent interpretations on the same concept depending on different organizations which in turn may cause a loophole in the legal protection of personal information.[237]

A person who illegally collected or output personal information will be punished only when this collection or output was intended to make a profit for himself or making unlawful gains for himself or for a third party pursuant to the provisions under Art. 33 and 34. There was an apparent inconsistency in the elements between the above provisions and the similar provision of the Criminal Code (Art. 359), where a person who obtains personal information in electromagnetic format without authorization shall be found guilty no matter whether the perpetrator intends to gain profit for himself or for a third party. This has produced a conflict of legislation.

4.3.4.2. Post amendment: the Personal Information Protection Act

The enactment of the PIP Act set a landmark in the development of Taiwan's information protection laws, which incorporated the standards relating personal data protection set up in the international privacy frameworks, in particular the EU Directive and the APEC Privacy Principles.[238] While the PIP Act was intended to redress the defects of the DPPDP Law and to provide comprehensive protection of personal information, this research proves that the above attempt was ineffective.

[237] This will be further discussed in the following section, 4.3.4.2.

[238] More discussion about the EU Directive and the APEC Privacy Framework, see Chapter 5 (section 5.3.2.2). Chapter 5 will also provide an analysis of the influence of the above two instruments upon the development of Taiwan's legislation (section 5.3.3.2).

Key points of amendment relating to data collection

The PIP Act deleted the limitation on the objects to cover non-computer-processed information (Art. 1) and extended the scope of protection data to include passport number, medical records, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, and other information which may be used to identify a natural person in either a direct or indirect way (Art. 2 (1)). In addition, the PIP Act broke the business limitation to expand the non-government subjects to include natural persons, juridical persons or groups other than government agencies (Art. 2 (8)).

The PIP Act amended the provision of exceptional conditions to data collection prohibitions for non-government agency and moved it to Art. 19. According to this article, an individual is prohibited from collection of personal information unless the purpose of that collection can be specified and the collection complies with one of the following conditions (Art. 19.1):

(1) Where there is a legal authorization;

(2) Where there is a contract or quasi-contract between the data subject and the agency;

(3) Where the data subject has disclosed such information by himself or when the information has been publicized legally;

(4) Where it is necessary to the public interest for statistics or the purpose of academic research conducted by a research institution;

(5) Where written consent has been provided by the data subject;

(6) Where public interest is involved; and

(7) Where the personal information is obtained from publicly available resources.

Some constraints have been placed on the application of the exemption conditions founded on academic research purposes and publicly-available resources. The information disclosed by the collector on the basis of the public interest for statistics or academic research should not lead to the identification of certain people (Art. 19.1 (4)). The collector or processor should delete or stop processing or using personal information *ex officio* or upon the request of the data subject when he realizes that the use and processing of the information is limited by the data subject and the obvious worthiness of the protection of the data subject's major interests or when he has been notified by the data subject (Art. 19.1 (7), 19.2).

Deficiencies of the PIP Act in regulating phishing

The PIP Act was intended to strengthen the personal autonomy of information disclosure, search and correction. However, while the increase in the number of protection objects and liability subjects, to certain extent, was helpful in providing more comprehensive protection for personal data, this enactment made insufficient efforts to redress the defects observed in the previous law which may produce a reverse-effect on the legal protection of personal information against phishing.

In comparison with the CPPDP Law (Art. 18 (1)), disappointingly, the PIP Act still saw the written consent of the data subject as merely one of the conditions for the lawful collection and processing of personal information rather than an indispensable requirement (19.1 (5)). Liou argued that the principle of personal information autonomy can still be easily excluded and has been turned into a mere figurehead without proper fulfillment.[239] Moreover, this Act failed to resolve the problem regarding the use of the indeterminate legal concept that had existed in the previous legislation, but

[239] Liou, J. Y. (2010), 'Unsatisfying Progress of Legislation: Initial Comments on the Personal Information Protection Act.', *Yue-Dan Jurisprudence Magazine*, 183, 147-64.

instead created more vague concepts, which have further undermined the protection of personal information.

The PIP Act deleted the phrase “no material adverse effect will be caused to the major interests of the principal” in Art. 18 (3) and replaced it with Art. 19.1 (3) on the ground that there is no need to protect information that has been disclosed by the data subject himself and that it was difficult to recognize the contents of the “no material adverse effect” and “major interests of the principal”.[240] It was a relatively paradoxical amendment as it seemed to try to avoid the difficulty of determining certain vague legal concepts but actually adopted more other indeterminate legal concepts in its provisions. Examples include “*public interests*” (Art. 19.1 (4) and (6)), “*publicly available resources*” (19.1 (7)), and “*obvious worthiness of the protection of data subject’s major interests*” (19.1 (7)). As mentioned in section 4.3.4.1, the use of an indeterminate legal concept is sometimes unavoidable given the flexibility of administrative authorities in determining the content of the said concept. However, it is always a problem if there is an absence of a specific independent authority of personal information protection which can provide a uniform interpretation when inconsistent opinions have arisen.

Taiwan currently has no independent authority taking charge of personal information protection tasks which can deal with disputes over indeterminate legal concepts. It is predictable that the authorities responsible for the related subject sectors are very likely to either shirk the responsibility for dealing with the arguments arising over personal information incidents or always make favorable interpretations to themselves. A large employment of indeterminate legal concepts, in this case, is improper and potentially to lead to discordant interpretations of a single concept which is not only unhelpful to the protection for personal information but also significantly increases the risk

[240] See the Explanatory Memoranda of the Personal Information Protection Bill, Art. 19, available at: <http://lis.ly.gov.tw/lgcgi/lglaw?@5:1804289383:f:NO%3DE01829*%20OR%20NO%3DB01829$$10$$$NO-PD>, accessed September 27 2014

of loopholes of legal protection by abusing indeterminate concepts.[241]

Certain indeterminate legal concepts used in the Act seem to provide phishing attackers an exemption from liability for unauthorized collection of personal data. As mentioned in Chapter 2 (section 2.4.1), a large amount of email addresses as well as personal information can be easily acquired by searching or scanning websites, in particular social networking websites, news groups, chat rooms that may open to the public manually or automatically. However, the disclosure of personal information by someone does not mean consent of the data subjects to anyone to use the said information in various ways. It is particularly true if the personal data are revealed by a third party without the authorization or awareness of the data subjects. Nevertheless, phishing attackers are eligible for an exemption from liability and rationalize their collection and processing of personal information as long as they can prove the information has been obtained from "*publicly available sources*" (Art. 19.1 (7)).

Although the data subject can notify the collector and thereby limit the collection, processing and use of personal information (Art. 19.2), it cannot provide substantial protection for a data subject if he/she is unaware of the collection matter, which is very often true of the victims of phishing attacks. The Act apparently failed to provide substantial protection for data subjects against unlawful data collection but put them at greater risk of being phished.

To conclude, while the PIP Act claimed and attempted to strengthen protection of personal information and redress the problems that previously existed in the CPPDP Law, it actually showed inadequate respect for the personal information autonomy and created more problems and loopholes of legal protection of personal information against unauthorized collection. This section only briefly

[241] The following chapter will continue to explore other problems that a lack of specific authority may incur, see Chapter 5, section 5.4.4.

examines the effort of the PIP in terms of providing better protection for personal information. A more comprehensive analysis of the relationship between information privacy and phishing as well as the role of national and international personal information protection laws in the regulation of phishing will be provided in Chapter 5.

4.4. The Criminal Code

This section examines the extent to which the Criminal Code of Taiwan is able to deal with phishing. Criminal law is an essential element of legal regulation of phishing and is a major deterrent to phishing attempts by making phishing an offence and imposing the threat of punishment on phishing attackers. Criminalization of phishing is often the first step in legal approaches by many countries to respond to phishing, which is usually done by integrating phishing with the current criminal legislation,[242] upgrading the existing laws to criminalize phishing,[243] or adding a sui generis law for dealing with phishing.[244] As I have mentioned in Chapter 2 (section 2.5.1) and will discuss in Chapter 6 (section 6.2.1 and 6.3), many countries, for example, India, South Africa, Saudi Arabia and Malaysia, did not introduce new laws specifically for addressing phishing but covered phishing under their existing cybercrime laws or general laws relating to spam, impersonation, theft or fraud. This is also the case of Taiwan.

The rapid growth of information technologies has given rise to new forms of crimes which have posed severe challenges to both the national and international legal systems. To respond to the emergence of new offences, Taiwan undertook two major legal amendments to the Criminal Code between 1990 and 2003, which brought the Criminal Code into a new era. A study of the

[242] Almerdas (2014), op. cit;Dinna et al. (2007), op. cit;Granova and Eloff (2005), op. cit;Nappinai (2009), op. cit.
[243] Bainbridge (2007), op. cit;Mcgowan (2006), op. cit.
[244] Lynch (2005), op. cit;Mcnealy (2008), op. cit. Some states of the USA have enacted specific anti-phishing statutes, for example, California, New York, Louisiana, etc. However, the USA currently has no federal law that directly aims at prohibiting phishing conduct.

background and the key elements of these two legal amendements is considered valuable to provide a full picture of the process of how Taiwanese Criminal Code has moved from a traditional criminal law based on ideology of physical property to a new criminal law that deals with cybercrimes involving virtual property. More importantly, it helps us to obtain a better understanding about what the Criminal Code has addressed and what it had failed to address regarding the regulation of phishing. This section introduces the legislative background and key elements of the 1997 Act and the 2003 Act respectively and paticularly examines the extent to which these two enactments are capable of dealing with phishing.

4.4.1. The 1997 Act

The 1997 Act focused on crimes committed using computers and crimes which targeted electromagnetic records. The most important contribution of the 1997 Act to the regulation of cyber crimes was that it expanded the protection of property from tangible property to electromagnetic records. However, this amendment received a lot of critiscms for its lack of careful consideration of the compatibility of electromagnetic records and the elements of the crimes against property, in particular larceny.[245] In addition, the 1997 Act adopted the 1990 Bill which was drafted since 1974 with very few changes. Several researchers doubted this reckless adoption to satisfy the demands of current society for regulation of cybercrime.[246] The fierce debates over the 1997 Act resulted in more proposals for legal amendments to the Criminal Code which was then passed and enacted in 2003.

[245] Cheng, C. W. (2001), 'Analysis of Electromagnetic Records Larceny', *Criminal Law Magazine*, 45 (6), 112-38;Huang, R. J. (2000), *The Limit of Penalty* (Yuan Jhao Publisher);Lin, Sian-Tian (2006b), *The Specific Provisions of the Criminal Code* (5 edn., 1; Taipei: Angel Publisher);Tsai, H. F. (2003), 'The regulations of the Criminal Law of the unauthorised acquirement act of electromagnetic records', *The Jurisprudence Collected Papers of the Chung Cheng University,* 13, 1-196.

[246] Li, Mao-San (1998), *Authority, Subject, and Criminal Laws* (Taipei: Han-Lu Publisher);--- (2001), 'The virtual image and actual features of computer crimes in Taiwan', *Collection of Papers on Criminal Policies and Research of Crimes* (4: Ministry of Justice), 1-16;Liao, Y. L. and Li, S. C. (2003), *Computer Crime –Theory and Practice* (Taipei: Wu-Nan Book Co. Ltd);Liao, Y. L. and Jin, M. C. (2006), 'A comparatively study of two reenactment of Penal Code on computer crime', *Journal of Information, Technology and Society,* 2006 (2), 56-76.

This section provides an overview of the development of the 1997 Act and looks into its effect on regulating phishing.

4.4.1.1. The 1990 Bill

A Criminal Code amendment research committee was established in 1974 by the Ministry of Judicial Administration,[247] with the aim of proposing a comprehensive amendment to the Criminal Code of 1935. After fifteen years, the Ministry of Justice brought the amendment bill to the Executive Yuan Committee which was then submitted by the Legislative Yuan in 1990.[248] The 1990 Bill was drafted for the proper development of agriculture, industry and commerce and proposed a large-scale amendment to the Criminal Code in many respects such as national security, social order, and people's physical health and private property. Although this Bill put eight articles to the Criminal Code for punishing computer crime offences, this was only a subsidiary task and was not the main focus of the Bill.[249]

Instead of sui generis legislation, the 1990 Bill extended the application of existing laws[250] to cover new types 'information age' activities involving the infringement of electromagnetic records, illegal computer use and attacks on computers. The new Art. 220 III defined for the first time an

[247] The Ministry of Judicial Administration operating under the Judicial Yuan was the predecessor of the Ministry of Justice operating under the Executive Yuan before 1980. The administration of the Taiwan High court and all other courts under its jurisdiction was separated from the system of prosecution under the Ministry of Judicial Administration and placed under the Judicial Yuan as part of the judicial reform in 1980. The Ministry of Judicial Administration was renamed the Ministry of Justice and shifted from the Judicial Yuan to the Executive Yuan subsequently.

[248] On the history of conducting the amendment bill to the Criminal Code, see the 1st meeting record of the Legislative Yuan, session 86, *Legislative Yuan Bulletin*, vol.80, issue 25, 225-26.

[249] The tasks which were involved within the amendment aspect of properly developing agriculture, industry and commerce, supra, 239.

[250] The laws which had been updated in the 1990 Bill to deal with computer crimes included the laws of forging or altering instruments (Art. 220), larceny (Art. 320), infringement of secrets (Art. 316-318), fraud (Art. 339), and the destruction, abandonment, and damage of instruments (Art. 352).

electromagnetic record as "*any record which is produced by electronic, magnetic or any other means unrecognisable by natural perceptive functions and is used for data processing by computer*".[251] The Bill addressed the protection of electromagnetic records by granting the same legal status to them as an instrument and movable property under the provision of the offence of forging or altering instruments (Art. 220 II) and the offences against property interests, including larceny (Art. 323, 320), abrupt taking, robbery, piracy (Art. 334-1), criminal conversion (Art. 338), and fraud and breach of trust (Art. 343).[252]

In addition, Art. 339-2, which was based on Art. 246 of the Criminal Code of Japan,[253] made it an offence to obtain another person's property by inputting false data or giving an unauthorised command to a computer or related equipment to create a false acquisition, loss or alteration of electromagnetic records. In order to protect information integrity, the 1990 Bill also made it an offence to interfere with another person's processing operation of electromagnetic records which results in damage to the other person or the public (Art. 352 II).[254] This provision, which was based on section 156.20 of the New York State Law and section 303b of the German Criminal Code,[255] saw 'interference with the operation of electromagnetic records' as an illegal change to or demolition of electromagnetic records and therefore included in the offence of destruction, damage or alteration to the instrument (Art. 352).

However, the deliberation of the 1990 Bill was greatly delayed. The Bill involved a total of 220

[251] The definition of 'electromagnetic records' was slightly amended and moved to Art. 10 V in a later amendment in 2005. An 'Electromagnetic record' was re-defined as 'any record which is produced by electronic, magnetic, optic or any other similar means and is used for data processing of computer.'

[252] Under the 1990 Bill, the larceny law in respect of the protection objects (Art. 323) shall also apply to the offences of abrupt taking, robbery, piracy (Art. 334-1), criminal conversion (Art. 338), fraud and breach of trust (Art. 343), where appropriate. Accordingly, the 1990 Bill added electromagnetic records to the protected objects under the above provisions. Whether it is proper to apply the elements of the above provisions to the case of electromagnetic records will be explored further later.

[253] The 1990 Bill Explanatory Memoranda of Art. 339-2, see *Legislative Yuan Bill Document Related*, no. 246, the 8th meeting of the Legislative Yuan, session 85, 273.

[254] It will be further explored in the following section the appropriation of the legislation of Art. 352 II.

[255] The 1990 Bill Explanatory Memoranda of Art. 352 II, supra, 278-279.

articles, but the Legislative Yuan had only completed the examination of 27 articles from 1990 to July 1995. This situation remained unchanged until 1995 when the Taiwan government placed its administrative priority on developing Taiwan into an Asia-Pacific regional operation centre and then forced the Ministry of Justice to complete an amendment to the Criminal Code related to computer crimes in order to improve the legal environment and enhance legal protection of personal data from illegal collection and utilization.[256]

4.4.1.2. The enactment of the 1997 Act

In July 1995, the legislator Zhang, Jian-Guo proposed an individual amendment bill to the Criminal Code (hereinafter, the 1995 Bill) which was intended to facilitate Taiwan's Asia-Pacific Regional Operation Centre project and contained the eight articles with exactly the same content as the 1990 Bill in respect of computer crimes. The only change that the 1995 Bill had made was adding a new article, 339-2, to deal with the offence of fraudulently obtaining property from automatic pay machines and shifted the former Art. 339-2 to Art. 339-3 accordingly as a result of negotiations between the government and the opposition parties. The 1995 Bill eventually became law in September 1997.

The 1995 Bill included all the computer crime provisions of the 1990 Amendment Bill; however, these two Bills were constructed for completely different purposes. The 1995 Bill intended to

[256] The Taiwan 'Economy Prosperity Scheme', initiated in July 1993, had the goal of establishing Taiwan as an Asia-Pacific regional operation centre as a response to the dramatic growth of economic regionalism, particularly within the Asia-Pacific economic region. In January 1995, the Council for Economic Planning and Development of the Administrative Yuan officially presented a plan which set the establishment of a modern legal environment for the information society as one of the main tasks. Therefore, the Ministry of Justice was requested to complete an amendment to the Criminal Code related to computer crimes and to finish the legislation of the CPPDP Law with the least delay by December 1995. The background and blueprint of the development of the Asia-Pacific regional operation center, see http://park.org/Taiwan/Government/Theme/Asia_Pacific_Rigional/english/foreword/1.htm and http://park.org/Taiwan/Government/Theme/Asia_Pacific_Rigional/english/foreword/2.htm. The content of the Plan of Building Taiwan into an Asia-Pacific Regional Operation Centre, see http://theme.cepd.gov.tw/aproc/html/total(1).doc, accessed September 29 2014.

establish a legal environment for the information society in coordination with the government's economic policy of establishing Taiwan into an Asia-Pacific regional operation centre, while the 1990 Bill was drafted with the broader purpose of prompting development in respect of agriculture, industry, and business. Liao[257] described it as "unimaginable" that almost the same legislation could be adopted based on two completely different lawmaking motivations. The specific needs of Taiwan's information society were not sufficiently explored in the recycling of the computer related provisions of the 1990 Bill.

In addition, as I mentioned at the beginning of this section, the 1990 Bill started to be drafted in 1974, when computers were not prevalent in Taiwan at all. Even in 1983, there were only 1,065 computers in Taiwan.[258] The Internet, which can be traced back to 1968 in America, was first available in Taiwan through the Taiwan Academic Network for research purposes at the end of 1991. Li[259] argued that there existed no clear comprehension of either the conception of computer crimes or Internet construction prior to the 1990's. Surprisingly, the legislation drafted based on incomplete knowledge about computer crimes between the 1970's and 1980's was enacted in 1997 regardless of the changes brought about by the prevalence of computers and the Internet. The 1997 Act was criticised as being full of loopholes due to its foundation upon an "old-fashioned" understanding about computer crimes.[260]

Liao pointed out that the hasty passing of the 1997 Act was also influenced by two cases named the 'Munitions Godfather' case and the 'Anarchist Document' case, detected in August and September in the same year.[261] The 'Munitions Godfather' case involved a website named 'Munitions Godfather' posting an advertisement selling firearms which invited the public to access and place

[257] Liao and Jin (2006), op. cit.
[258] Li (1998), op. cit.
[259] Li (2001), op. cit.
[260] Li (2001), op. cit.
[261] Liao and Li (2003), op. cit;Liao and Jin (2006), op. cit.

orders. This case was considered to be the beginning of headline computer crime which significantly expedited the enactment of the 1995 Bill.

The ‘Anarchist Document’ case involved a university student who built a personal web page named ‘anarchist document’ on the university website. This could be viewed and accessed by the public and included instruction on making bombs and discussions about atomic bombs. In fact, the above two cases were not examples of typical computer crimes but only constituted the offence of openly inciting people to break the law (Art. 153 (1)). However, the method adopted to commit it was new to Taiwanese society. It brought a comparatively more serious threat to society as information could be largely and efficiently spread through the Internet.

4.4.1.3. The compatibility of the 1997 Act and phishing

Assuming that an electromagnetic record could be flawlessly adopted as the object protected by the laws of larceny and fraud, in the case of phishing carried out by deceiving users into giving away their financial or other sensitive information may constitute an offence of the fraud of electromagnetic records (Art. 339, 343). It may break the law of larceny (Art. 320, 323) if the phishing attacker obtains electromagnetic records directly from users’ computers or their related equipment by infecting their computers with malicious programmes. The difference lies in whether a phishing attacker adopts a fraudulent method to mislead his/her victims and make them believe that the imitative website is legitimate.

In addition, it might also constitute the offence of destruction, damage and alteration to an instrument (Art. 352 II) if an electromagnetic record is acquired accompanied by change or damage to an electromagnetic record.[262] A person may commit a crime against secret protection (Art. 318-1)

[262] Art. 352 II actually did not specify the interference conducts nor did it define the coverage of protected objects.

if he/she leaks another person's sensitive information or disseminates or transacts the information obtained by means of phishing.

However, the compatibility of electromagnetic records and the elements of the crimes against property has been strongly questioned by both researchers and judges, not because an electromagnetic record sometimes does not have business value but because an electromagnetic record is not capable of being stolen (Art. 320) or delivered (Art. 339) within Taiwan's legal context due to its duplicable nature.

In fact, the applicability of the larceny law to electromagnetic records has often been questioned in two respects: whether an electromagnetic record is a movable property protected in law and whether an electromagnetic record is capable of being stolen. The question whether an electromagnet record is a moveable property is less debated, as it has been widely recognised that a moveable property is not limited to physical property but also includes intellectual property. What has been argued is whether the value of a movable property, as defined by the Criminal Code, should be an objective and universal value or a subjective value that is applicable to a particular person or group.

An electromagnetic record, for example an account username or password which is often the target of phishing attacks and may be valuable to the record possessor or certain people, still cannot be objectively valued and is not deemed a universal object of monetary transaction. The property value was generally recognized by most researchers of Taiwan as including both business value (object value) and usufruct value (subject value) based on the function of property.[263] The business value of a movable property should not be seen as a necessary requirement to decide whether it is an

What did it mean by 'interference'? Did it mean deletion or alteration of data or did it also include enter or transmission of data? It was also unclear about the protected objects under this provision. Did Art. 352 II only protect computer data or cover the carrier and system used for that data? These were the questions that the legislators failed to answer.

[263] Han, J. M. and Wu, J. F. (2000), *The Specific Provisions of the Criminal Code* (1 edn.);Liang, H. C. (1994), *Research of Living Examples of the Criminal Code* (Taipei: Wu-Nan Book Co. Ltd.).

object which is worthy of legal protection. Accordingly, a meaningful picture or a letter which is priceless to a particular individual but may be valueless in a business transaction is also the object protected by larceny, as the legal interests protected by the laws against property offences contain both objective and subjective values. Therefore, there should be no question about violation of property legal interests, once acquiring an electromagnet record incurs a subjective disadvantage to the record possessor.

An electromagnetic record as a moveable property that is worthy of legal protection itself is not controversial; but the question is whether taking an electromagnetic record can satisfy the elements of larceny (Art. 320). The legal interest that the larceny law aims to protect is actually the possession of a moveable property.[264] It hence cannot be seen as an offence of larceny if obtaining a moveable property has not resulted in the loss of possession of the original possessor.[265] The element of larceny is only satisfied when a person destroys the original possession relationship and builds his new possession of that property. As an electromagnetic record is duplicable in nature, it is usually obtained through duplication which will not be accompanied by the destruction of the control of the original possessor. Researchers[266] argued that any analogy with the elements should be strictly prohibited based on the principle of legality,[267] and therefore the larceny law cannot apply to the case of unauthorized acquisition of electromagnetic records as long as its elements cannot be satisfied.

Although there were differences in judicial opinion,[268] the Taiwanese judicial interpretations

[264] Lin (2006b), op. cit.
[265] Tsai (2003), op. cit.
[266] Cheng (2001), op. cit;Huang (2000), op. cit.
[267] The principle of legality is the legal ideal that requires all laws to be clear, ascertainable and non-retrospective.
[268] In a case where an employee obtained customers' magnetic strip codes from their credit cards by using an interception machine, the court considered that the destruction of the original possession was not a requisite for satisfying the elements of larceny. According to this interpretation in the above case, whether or not the possessor had lost their possession of electromagnetic records *de facto* did not affect the commitment of larceny. *Taiwan High Ct. Kaohsiung Branch Ct., Criminal Division, 89 Shang-Yi No. 1264 (2000) (Taiwan)*

generally hold the same opinions as the scholars about the compatibility of the larceny law and electromagnetic records. For example, in a case where an employee allegedly duplicated all of the other personnel's user IDs for accessing the Internet through a Management Information Service, the court decided that the defendant was not guilty of larceny, as the control of the said information of the original possessor was not destroyed.[269]

In my opinion, it is questionable to add electromagnetic records to the objects under the provision of larceny as well as fraud. Electric energy and thermal energy, the objects which were also listed in Art. 323 with electromagnetic records, are consumable energy. Once the energy has been consumed by another person, the original energy possessor will not be able to use it. However, it is most unlikely that an electromagnetic record be used up as it can be obtained by duplication without affecting the original possession relationship.

Similarly, a person who by fraud makes another person deliver financial or other sensitive data to him or a third party does not simultaneously cause a loss of control of that person over his data (Art. 339 I). Moreover, as most researchers suggested,[270] the commitment of the offence of fraud requires an occurrence of actual damage to property. This is very unlikely to happen in the case of phishing unless that information itself has business value and this value will be immediately transferred to another person following the delivery of information.

There was apparently a lack of careful consideration by the lawmakers about the peculiar characteristic of electromagnetic records. To respect the principle of legality, neither the expansion of the elements nor the expansion of a penalty should be admitted. Electromagnetic records, strictly speaking from a legal perspective, can be "obtained", not "stolen". Since it is inappropriate to

[269] *Taiwan High Ct., Criminal Division, 91 Shang-Yi No. 2258 (2002) (Taiwan)*

[270] Hsueh (2013), op. cit;Lin (2006b), op. cit;Lin, Dung-Mau (2012), *The overview of the Criminal Code* (7 edn.; Taipei: Yi-Pin Publisher);Shiu, Tze-Tian (2011b), 'The provisions and debates of the offence of fraud', *Ywe-Dan Jurisprudence Magazine*, 197, 197-200.

include electromagnetic records in the objects of the offences against moveable property, both the larceny and fraud laws are not suitable for dealing with phishing.

4.4.2. The 2003 Act

The debates over the 1997 Act pressed the Ministry of Justice to take steps for another legislative amendment to the Criminal Code. After three years following the proclamation of the 1997 Act, the Ministry of Justice started to draft an amendment bill to the Criminal Code which was passed and came into force in June 2003. The 2003 Act set a landmark in the developemnt of cyber criminal laws of Taiwan by introducing a new Chapter 36 that specifically focused on the offences gainst computer use to enhance the legal protection of computer use, computer efficiency, and control over electromagnetic records. Although researchers argued that a perfect solution for combating computer crime does not exist and the criminal law merely provides a sense of mental security by responding to the general fear of computer crime,[271] this Act is of particular significance to the regulation of phishing, as it granted electromagnetic records an individual legal status distinct from physical property, made it an offence to obtain electromagnetic records without authorisation (Art. 359), and criminalised the production of malicious computer programs (Art. 362).

However, there have existed many arguments, both academically and practically, regarding the elements of the offences related to phishing. This has given rise to the difficulties of application of legislation and even caused loopholes of legal protection against phishing. In addition, the 2003 Act made it an offence to produce malicious computer programs (Art. 362) which may be helpful, more or less, to tackle the supply chains of phishing articles but the effort appears to be inadequate. Importantly, as phishing is frequently a global phenomenon, effective law enforcement

[271] Jeng, Y. J. (2003), 'Boost courage by whistling – comments on the augmentation of the Chapter 36 of the Criminal Code', *Ywe-Dan Jurisprudence*, 201, 104-15;Liou, Guang-San (1999), *The Theory of Computer Crimes* (Beijing: The Publisher of the People's University of China) 4.

predominately relies on mutual legal assistance and cross-border cooperation. This is a particularly crucial challenge for Taiwan because Taiwan has been in a very difficult position in matters involving international cooperation because of its complex position relating to statehood.

This section first provides a brief review of the legislative background of the 2003 Act. To provide an understanding of the extent to which the 2003 Act is able to deal with phishing, it considers the key provisions of the 2003 Act and the difficulties in applying them, especially its effectiveness in dealing with phishing supply chains and prosecutions in the Taiwanese context.

4.4.2.1. Background

In May 2001, the Ministry of Justice invited the experts concerned from industrial, governmental, and academic circles to form a research team on legislation related to the prevention of computer crimes which took the Council of Europe Convention on Cybercrime[272] as the principal referral model for drafting the amendment bill.[273] Two years later, a hacking event highlighted the inadequacy in relation to cybercrime and triggered the fast passing of the amendment bill.

On 28th March 2003, a secondary school student hacked into the official website of the presidential palace of Taiwan as a joke. This student was reportedly not prosecuted for the offence as he was very regretful and sincerely apologised for his wrongdoing. The truth, however, was that there was no available legal provision for dealing with a hacker attack at that time. In order to quickly remedy the legislative loophole, the amendment bill was submitted to the Legislative Yuan hurriedly on 3rd April 2003 and came into force on 25th June in the same year.

[272] The Council of Europe Convention on Cybercrime, which was signed in 2001 and enforced in 2004, is the first and only binding international instrument dealing with crimes committed via the Internet and other computer networks. More examination of the CoE's Convention on Cybercrime, see Chapter 6, section 6.3.2.2.

[273] Ye, C. S. (2003), 'The comparison of legislation amendments to the Criminal Code in relation to computer crime and the research on practical problems', in Ministry of Justice (ed.), *Collection of Papers on Criminal Policies and Research of Crimes* (6:4), 1-17.The author held a post in the Department of Prosecutorial Affairs of the Ministry of Justice during 2002-2006 and had fully participated in the process of drafting and amending the 2003 Act.

The 2003 Act amended the provisions which had received intense criticisms in the 1997 Act by removing electromagnetic records from the objects of larceny (Art. 323) and interference with the processing operation of electromagnetic records (Art. 352 II). The Act also introduced a new chapter entitled ‘Offences against Computer Use’ to the Criminal Code which was intended to combat the crimes that targeted computers and electromagnetic records. This new chapter inserted the offences of unauthorised access to computers (Art. 358), unauthorised obtainment of electromagnetic records or deletion of or alteration to electromagnetic records (Art. 359), unauthorised interference with computers or related equipment (Art. 360) and the production of computer programs for the commitment of the offences regulated in this chapter (Art. 362).

4.4.2.2. Key amendments in relation to phishing

To obtain a clear picture of these amendments related to phishing, this section provides a comparison of the 1997 Act and the 2003 Act as indicated in the diagram below.

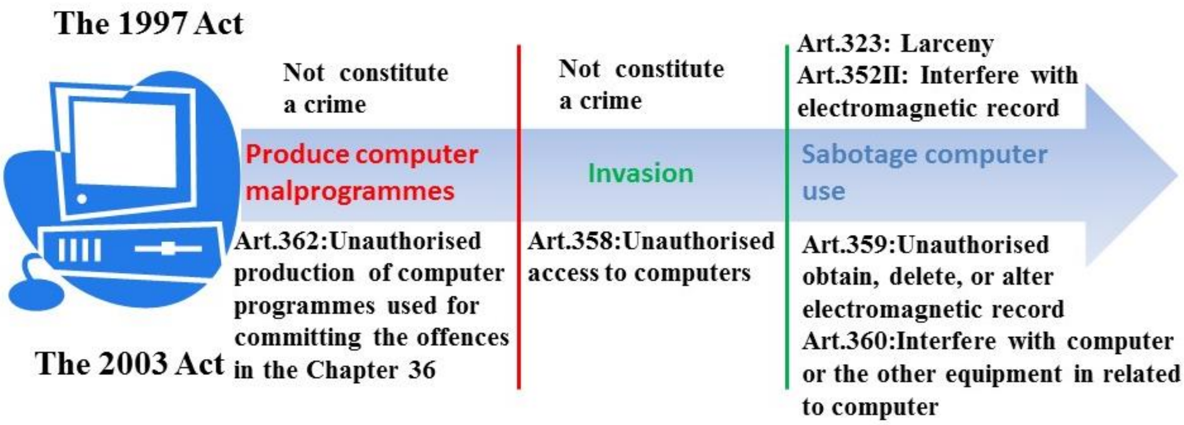

The 1997 Act
Not constitute a crime
Not constitute a crime
Art.323: Larceny
Art.352II: Interfere with electromagnetic record
Produce computer malprogrammes
Invasion
Sabotage computer use
Art.362:Unauthorised production of computer programmes used for committing the offences in the Chapter 36
Art.358:Unauthorised access to computers
Art.359:Unauthorised obtain, delete, or alter electromagnetic record
Art.360:Interfere with computer or the other equipment in related to computer
The 2003 Act

Diagram 4.1: Comparison of the 1995 Act and the 2003 Act of the Criminal Code

Penalisation of access to computers without authorisation (Art. 358)

The 2003 Act made it a crime to access another person's computer without authorisation (Art. 358), for the purpose of dealing with hacker attacks. As the legal interest that this provision aimed to protect is the security of computer use, whether this offence is constituted depends on whether the owner or possessor of a computer has a reasonable expectation of computer security evidenced by the use of certain protection measures. The lawmakers hence considered it necessary to place a limitation on the access methods.[274] An offence under Art. 358 is committed once a person accesses another's computer either by inputting the password of other person, breaking down a computer's protection measures or utilizing a loophole in the computer system. Whether or not this access has resulted in any damage to the public or another person does not affect the commitment of the offence.

Unauthorised obtainment of electromagnetic records (Art. 359)

The 2003 Act removed electromagnetic records from the protected objects of larceny (Art. 323),[275] and this removal also produced the same effects on the law of fraud (Art. 339, 343). The Act added a replacement article, Art 359, which deals with the offence of the unauthorised obtainment of electromagnetic records.

To protect information privacy, integrity and availability, Art. 359 made it an offence to obtain, delete, or alter the electromagnetic records of another person's computer or related equipment without authorisation. While the larceny law aimed to protect the property interests of

[274] Ye (2003), op. cit.

[275] As Art. 323 shall apply to other offences against property interests where appropriate, the removal of electromagnetic records from the protected objects of Art. 323 also produced the same effects on the laws of abrupt taking, robbery, piracy, criminal conversion, fraud, and breach of trust.

electromagnetic records generated from possession, Art. 359 was intended to ensure the security of electromagnetic records against unauthorised obtainment, deletion or alteration. An Art. 359 offence is only committed when obtainment conduct has caused damage to another person or the public, differing from what is laid down in Art. 358. Unauthorised access to computers (Art. 358) was hence compared with housebreaking, while the unauthorised obtainment of electromagnetic records (Art. 359) was compared with moving or taking property from a house in addition to housebreaking.[276]

Unauthorised interference with computers or related equipment (Art. 360)

Art. 360 intended to substitute for Art. 352 II by changing the protection object from electromagnetic records to computers and computer-related equipment and by detailing the methods of interference. Ke suggested that ‘interference’ herein refers to a temporary loss of function of computer or Internet system, and this function can be reinstated once the interference is eliminated.[277] The legislators also limited the interference methods to the use of computer programs and other electromagnetic ways. Art. 360 also requires occurrence of damage to the public or another person.

Criminalization of production of malicious computer programs (Art. 362)

The 2003 Act made it an offence to produce computer programs for the commitment of the offences outlined in Chapter 36 (Art. 362). In order to diminish the negative effect on the computer software industry or academic research, Art. 362 places a restriction on the intention of the perpetrator. The offence of the production of malware is committed only when the perpetrator intends to provide that

[276] See the speech of Yan, Da He, the standing vice-minister of the Ministry of Justice, the 16th meeting record of the Judiciary Committee, session 3, 5th term, *Legislative Yuan Bulletin*, vol.92, issue 26, 137.

[277] Ke, Y. C. (2003), 'The comments on the legislation relating computer (Internet) crimes of the Criminal Code', *Ywe-Dan Jurisprudence Classroom*, 11, 117-29.

malware for the purpose of committing the offences regulated by Chapter 36. It does not constitute a crime under Art. 362 if the production of malware does not result in any damage to another person or the public, which is the same as the offences laid down in Art. 359 and 360.

No trial without complaint (Art. 363)

How to strike a balance between the criminal punishment of cybercrime and the autonomy of the cyber world is always a question that needs to be considered when dealing with criminalization of certain online behaviours. To avoid excessive government intervention in cyberspace as well as to concentrate the limited judiciary resources on combatting grave computer crimes, the 2003 Act concluded that the offences in Chapter 36, except for offences involving using computers of government organizations (Art. 361), are indictable only upon complaints (Art. 363).[278]

4.4.2.3. The arguments over the elements of the provisions

There have existed different academic and judicial opinions about the elements of the provisions related to phishing, which has made it difficult to apply the 2003 Act to phishing.

Obtainment

In terms of Art. 359, it has been argued by several researchers that putting three conducts - obtainment, deletion, and alteration which were different in nature into one article was likely to have a negative influence on the integrity of the legislative system.[279] More importantly, what is the

[278] According to the Criminal Procedure Code, the victim of a crime can file a complaint (Art. 232). A statutory agent or the spouse of the victim may also file an independent complaint even it is against the opinion of the victim (Art. 233 I). In the case if the victim is dead, his/her lineal blood relative, collateral blood relative within the third degree of kinship, relative by marriage within the second degree of relationship, family head, or family member may file a complaint as long as this complaint is not contrary to the opinion of the victim (Art. 233 II).

[279] Hsueh (2013), op. cit;Ke (2003), op. cit;Lin, Guan-Hong (2006a), 'A research on the Chapter 'Offences against

‘obtainment’ recognised under this provision? Literally, Art. 359 did not the manner in which a person obtains electromagnetic records into a particular requirement. However, it was suggested that ‘obtainment’ in Art. 359 should be understood as accessing the victim’s computer and acquiring information from the storage of the computer. A typical example is where a person intentionally infects another person’s computer with the Trojan malware and thereby gains access to the information in the storage. This opinion has also been advocated by several judicial interpretations.[280] Therefore, simply learning the contents of electromagnetic records by browsing a computer without obtaining of a copy of the records or obtaining the records by the way other than accessing to the victim’s computer does not constitute an offence under Art. 359.

Nevertheless, the above interpretation of ‘obtainment’ has caused a problem in applying Art. 359 to phishing. A phishing perpetrator may be found guilty of the crime of unauthorised obtainment of electromagnetic records (Art. 359) if he acquires confidential information from the victim’s computer via a technical subterfuge scheme such as malware infection or keylogger. However, Art. 359 is inapplicable to other cases of phishing. For example, there is a loophole where a person directs users to a spoofed website and obtains the data from users’ response.

Phishing can be carried out in various ways, and is sometimes accompanied by accessing someone’s computer, but this is not always the case. In fact, Art. 359 was enacted for the protection of information security and integrity rather than computer security. A discrimination between the obtainment methods is unhelpful in protecting information against unauthorised collection but could cause a gap of criminalization of phishing. In my opinion, the term ‘obtainment’ should be interpreted broadly and Art. 359 should be valid for all forms of unauthorised acquisition of electromagnetic records, irrespective of the method employed to obtain it.

Computer Use' of the Criminal Code ', *Criminal Law Magazine*, 50: 6, 82-118.

[280] For example, it was judicially interpreted in *Hsinchu Dist. Ct., Criminal Division, 93 Chu-Jen No. 685 (2004) (Taiwan)* that obtainment of electromagnetic record referred to duplicating it to a storage which was under the possession of another person. Chu-Jen is the contracted form of the Hsin-Chu District Court Dispute Tribunal.

Unauthorised

The 2003 Act largely used the term ‘unauthorised’ as an element in the new provisions (Art. 358-360) without specifically defining its context. The arguments over the term ‘unauthorised’ mostly focused on two questions:

a. Does ‘unauthorised’ include doing something exceeding the authorisation?
b. Does ‘unauthorised’ cover ‘consent obtained by fraud’?

a. Exceeding the authorisation

Some researchers suggested that ‘unauthorised’ means doing something without proper reason or legal authorisation,[281] while an alternative view argued that ‘unauthorised’ conveyed not only doing something without authorisation but also doing something exceeding that authorisation.[282] The disagreements about the line between authorised and unauthorised have resulted in divergent judicial interpretations and produced different legal effect – a breach of the criminal law or an infringement of a civil contract. The Taipei District Court has interpreted Art. 359 in a case where a bank employee was accused of downloading the customers’ credit card data to a hard disk attached by the defendant to his personal computer issued by the working bank. The court found that the defendant had not committed the offence of unauthorised obtainment of electromagnetic records as he was allowed to download the customers’ data to his computer in order to test the maximum flow of the back website within the range of his responsibility. Although the judgment indicated that the employees of that bank were strictly prohibited from attaching a USB or any other equipment used

[281] Gan, Tian-Guei (2011), *The Specific Provisions of the Criminal Code -Part I* (2 edn.; Taipei: San Min Ltd);Lin (2006b), op. cit.

[282] Liao and Jin (2006), op. cit.

for data storage to the computer, downloading customers' data onto an additional hard disk was not an offence against Art. 359, but merely a violation of the internal regulations of the bank.[283]

The above judgment was later abandoned by the Appeal Court. The Taiwan High Court found the appellant guilty of the crime of the unauthorised obtainment of electromagnetic records (Art. 359), as all the internal employees except for the personnel specified were strictly prohibited to access the credit card system as well as the customers' credit card information. The appellant's conduct of gaining a copy of the customers' credit card information without permission to access the credit card system had constituted an offence under Art. 359.[284]

The context of 'unauthorised obtainment', in my opinion, should refer not only to obtainment without authorisation but also to obtainment which goes beyond authorisation. According to the theory of agency in Taiwanese civil law, exceeding the authority conferred by the principal is deemed as unauthorised agency, unless it is subsequently acknowledged by the principal (Art. 170 of the Civil Code). Collecting electromagnetic records while overstepping the range of authorisation thereof should be seen as the unauthorised obtainment of electromagnetic records and be penalized under Art. 359.

b. Consent obtained by fraud

Another question is: should a person be found guilty of unauthorised obtainment of electromagnetic records if he causes another person to give away his records by fraud? This is often the case in phishing. A social-engineering phishing attack is usually carried out by delivering a genuine-looking email or website to deceive the users into believing it is from a legitimate source.

[283] *Taipei Dist. Ct., Criminal Division, 98 Su No. 245 (2009) (Taiwan)*

[284] *Taiwan High Ct., Criminal Division, 98 Shang-Su No. 3246 (2009) (Taiwan)*

Even if it is a consent obtained by deception, researchers suggested that it should be understood as "non-unauthorised" and hence does not satisfy the subjective elements of the offence of unauthorised obtainment of electromagnetic records (Art. 359).[285]

Hsueh[286] provided a detailed analysis of the criminal penalties for phishing by examining how the Taiwan Criminal Code deals with phishing. He indicated that Art. 359 can be used to deal with phishing only if it is carried out without the awareness of the victims. For example, in the case of phishing through malware infection, the victims are unlikely to make consent because they are completely unaware of the data collection matter. According to Hsueh, Art. 359 is not applicable to the case that a person obtains information by fraud as it is performed under the consent of the data possessor and hence does not constitute unauhorised obtainment. Whether it is a fraud-induced consent does not influence the effect of consent. In addition, Hsueh indicated that Art. 339 II, which makes it an offence to cause another person to deliver property by fraud and thereby taking illegal property benefit is adequately capable of dealing with phishing that is carried out by deception. The law of fraud (Art. 339) was intended to protect the integral property interest of the property possessor; and as suggested by Hsueh, in the example that a person who uses another's fraudulently-obtained login information for Internet banking service to transfer the victim's money to himself or to a third party should be found guilty of the offence under Art. 339 II because the integral property of the victim has been damaged.

However, I have a different opinion about the applicability of Art. 339 II and Art. 359 to phishing. An electromagnetic record has been no longer the object of fraud since the enactment of the 2003 Act. The 2003 Act made significant amendment to the 1997 Act, and one of the key amendments

[285] Hsueh (2013), op. cit;Huang, Chang-Ren (2009), *The General Provisions of the Criminal Code* (2 edn.; Taipei: New Sharing Publishing Ltd);Lin, Yu-Shiung (2011b), *New General Provisions of the Criminal Code* (3 edn.).

[286] Hsueh (2013), op. cit.

was to remove electromagnetic records from the protected objects of larceny (Art. 323).[287] As Art. 323 shall apply mutatis mutandis to the provision of fraud (Art. 343), this removal naturally produced the same effects on the offence of fraud (Art. 339). Since an electromagnetic record is no longer the object protected under the provision of fraud, it is inappropriate to still make Art. 339 II to deal with phishing. Assuming that electromagnetic records are still the object that the fraud law is intended to protect, as I have indicated in section 4.4.1.3, there are several questions about the compatibility of the elements of the fraud law and phishing. Taking the example provided by Hsueh, a person who is defrauded of login information for Internet banking service does not **necessarily** nor **directly** result in loss of property but only increases the risk that someone might take his money by using the said information. The login information itself does not have business value and cannot be transacted, therefore a delivery of the said information does not necessarily mean damage to the victim's integral property interest. Given the incompatibility of phishing and the elements of the fraud law, I doubt that Art. 339 II is capable of dealing with phishing.

In terms of Art. 359, I realize that fraud-induced consent is generally regarded as legally valid and may be used as an excuse to prevent the defendant from satisfying subjective elements of the offences against personal legal interests.[288] The offences against personal legal interests are generally divided into two: offences against property and offences against personality. As people are allowed to dispose their property at free will, a consented disposal of property is usually valid even if the consent is obtained by deception. However, whether consent can be used as an excuse for the offences against personality is another question. By looking into the Criminal Code, we can find the lawmakers put the element of 'unauthorised' in 10 articles, including offences against freedom (Art. 306), offences against privacy (Art. 315, 315-1, 316, 317, 318, 318-1), and offences against computer use (Art. 358, 359, 360). Although the lawmakers did not specify the nature of legal

[287] See section 4.4.2.2.

[288] Baker, Dennis J (2009), 'The moral limits of consent as a defense in the criminal law', *New Criminal Law Review,* 12 (1), 93-121;--- (2011), *The right not to be criminalized: demarcating criminal law's authority* (Ashgate Publishing, Ltd.).

interest about computer use, they stated that Art. 359 was enacted to protect the security of information with respect to information privacy, integrity and availability (see section 4.4.2.2). ‘Unauthorised’ seems to be a special element laid down by the lawmakers in the offences against personality. The obtainment of electromagnetic records without authorisation should not be seen as an offence against property, but an offence against personality. Whether it is appropriate to take consent obtained by fraud as a proper reason and an excuse to prevent satisfaction of the element of ‘unauthorised’ is hence questionable.

Damage

Under the provision of Art. 359, a person who obtains financial or sensitive data from another either by malware infection or deception will not be found guilty if this obtainment has not resulted in damage to another person or the public. It was hence suggested that ‘electromagnetic records’ herein should be sensitive information, such as business confidential data, financial information or other personal sensitive information, the disclosure, destruction, or alteration of which may cause loss or damage to another person.[289] Similarly, the offences of Art. 360 and 362 also require occurrence of damage but there is controversy about the context of damage and whether damage has been caused.

While researchers argued that the damage to another person or the public should be capable of a broad interpretation,[290] the judicial interpretation of damage is rather restrictive. The first judgment to interpret Art. 359 and 360 of the Criminal Code in *Taipei Dist. Ct., Criminal Division, 94 Su No. 1514 (2005) (Taiwan)* resulted from the conduct of two employees of a company which operated a website that redirected users back to their site through the unauthorised alteration of the users’

[289] Tsai (2003), op. cit.

[290] Kennedy, Gabriela and Doyle, Sarah (2007), 'A snapshot of legal developments and industry issues relevant to information technology, media and telecommunications in key jurisdictions across the Asia Pacific–Co-ordinated by Lovells and contributed to by other leading law firms in the region', *Computer Law & Security Review,* 23 (2), 148-55.

computer files with a computer program in order to increase the amount of traffic to its website and to prevent users from accessing websites which provided similar services. The court found that the malware had interfered with the capability of the users' computer to connect to the Internet and thereby disabled the users to freely access specific Internet content, thus causing damage to the individuals. However, a later Appeal Court decision found that the malware had not damaged the users, as it had not caused vital interference with the "major" function of the computer system but merely influenced the users' visit to specific websites through changing the host files in the users' computers.[291]

While Tsai suggested that the damage should not be limited to monetary loss,[292] in judicial practice, Art. 359 has not applied to unauthorised obtainment of electromagnetic records unless this obtainment has led to monetary loss to another person. In one case a man intercepted another person's keystrokes through planting a keylogging program onto the PC in an Internet café and thereby obtained the victim's ID and password of online game account. He then logged onto the victim's online game account to acquire virtual property. The court only found the defendant was guilty of having unauthorised access to another person's computer (Art. 358) and unauthorised obtaining of another person's virtual property existing in the form of electromagnetic records (Art. 359) without considering the issue of the interception of another person's account credentials.[293]

Although the 2003 Act recognized that an electromagnetic record is entitled to independent legal protection separate from property law, the judges of Taiwan have appeared not to change the old way of thinking. Many of them still see the unauthorised obtainment of electromagnetic records to be property crimes and hence give discordant interpretations of Art. 359 between cases relating to the records that are generally acknowledged as 'valuable', such as virtual currency or credit card or

[291] *Taiwan High Ct., Criminal Division, 95 Shang-Su No. 3830 (2006) (Taiwan)*

[292] Tsai (2003), op. cit.

[293] *Fuchien Lienchiang Dist. Ct., Criminal Division, 93 Su No. 4 (2004) (Taiwan)* Similar interpretation can be seen in *Kaohsiung Dist Ct., Criminal Division, 93 Jen No. 2416 (2004) (Taiwan)*

banking information, and the records other than these, which is often true in the case of phishing such as username, password or personal sensitive information. An offence under Art. 359 is constituted only when there is damage to another person or to the public, but the damage does not have to be monetary damage. It is nevertheless practically difficult to prove the existence of damage other than monetary loss. Therefore, whether it is necessary to require for occurrence of damage in Art. 359 is worthy of proper consideration.

4.4.2.4. Inadequate effort to tackle phishing resources

As discussed in Chapter 2 regarding successful phishing attacks (section 2.5.2), the readily availability of a variety of phishing resources, such as pre-generated counterfeit pages, list of email and proxy server, scripts for processing user input, and even hosting services for phishing websites which can be easily purchased or downloaded for free has been an important factor that boosts the growth of phishing attacks.[294] This should be addressed by placing legal prohibition of the production, transfer, or possession of phishing articles to make a person who produces, supplies, transfers or possesses any computer programs, data or service intending to facilitate the practice of phishing to be liable for his conduct.

A major amendment under the 2003 Act was to make it a crime to produce computer programs for the commitment of the offences provided under Chapter 36 (Art. 362). Art. 362 nevertheless only penalizes the person who makes malicious computer programs without addressing the punishment to the person who disseminates them. In addition, it only focused on the ban of computer programs without taking into account the other resources that are actually frequently provided for assisting in offence commitment.

[294] Bose and Leung (2007), op. cit;Brody, Mulig, and Kimball (2007), op. cit;Dunn (2007), op. cit;Messagelabs (2009), op. cit;Milletary (2005), op. cit;Sophos (2004), op. cit.

Raising the difficulties for potential phishers in performing phishing attacks is a good way to curb phishing activities, which can be done by diminishing available resources for phishing attackers. However, the 2003 Act does not address this issue satisfactory, and Art. 362 needs to be reviewed.

4.4.2.5. The failure to prosecute phishing[295]

The failure of prosecution of phishers can be attributed to two major factors: lack of complaint and ineffective law enforcement. The offences laid down in Chapter 36, except for Art. 361, are indictable only upon complaint (Art. 363). A court shall dismiss phishing cases if the accuser withdraws the claim against the defendant after the two parties have reached a compromise. In some cases, phishing victims are completely unaware that their information has been stolen, even after the phishing conduct has been detected.[296] A court shall dismiss a case on the ground of absence of complaints if there is no complaint raised by any victim of a phishing attack.

If the victim of phishing raises a complaint, it mostly ends up with non-prosecution as the defendant cannot be specified. In a case where Microsoft Corporation was accused of conspiring with an unknown person and let that person use the MSN message service to send the victim a web link leading the victim to a counterfeit MSN login page which spoofed the victim into leaking his username and password, the prosecutor did not bring the case to court, as a corporation could not be a defendant in criminal law and the said unknown person could not be specified either.[297]

Cyberspace, by its borderless nature and anonymity characteristic, permits people to reach anyone through the power of network and adopt different persona during online communication. While

[295] Chapter 6 will specifically look into the challenges posed by phishing to law enforcement work combined with the national and international responses to this issue.

[296] For example, *Banciao Dist. Ct., Criminal Division, 94 Jen No. 3682 (2005) (Taiwan)*

[297] See *Taipei Dist. Prosecutor Office, 96 Jan No 2275 (2007) (Taiwan)*

cyberspace allows people to enjoy a totally different life from what they have in the real world, it brings new challenges to the traditional legal system. Phishing attackers usually intentionally include several different jurisdictions and host phishing websites in free web-hosting environment or bot-infected machines[298] to obscure their location and identity in order to make investigation and prosecution as difficult as possible. Effective law enforcement, to a significant degree, depends on traceability and successful prosecution of phishing attackers, which is nevertheless difficult to achieve and demands cross-border cooperation between law enforcement, legislation and private sectors.[299] Establishing cooperation with other countries in the absence of bilateral or multilateral mutual legal assistance agreements is an uneasy task, and it becomes even more difficult in Taiwan because of its awkward position in international society and the political pressure from China.[300]

Chang, Yao-Chung[301] conducted an important academic work that introduced the existing model of cooperation between Taiwan and China in combating cross-Strait crime and examined the extent that this existing cooperation is able to apply to cybercrime. Although there are two agreements signed through non-governmental organizations between Taiwan and China in 1990[302] and 2009,[303] Chang pointed out that the current cooperation model seems not to be working when it comes to cooperation against cybercrimes, probably because cybercrime is a too sensitive issue to both governments as they are frequently the target of cyber-attacks on each other. The author further

[298] Mcgrath and Gupta (2008), op. cit;Moore and Clayton (2009), op. cit.

[299] Lynch (2005), op. cit;Sullins (2006), op. cit.

[300] The examination of the political obstacles to Taiwan to engaging in international cooperation, see Chapter 3, section 3.6.

[301] Chang (2012), op. cit.

[302] The *Kinmen Agreement* was signed in 1990 between the Red Cross Societies of Taiwan and China authorised by their respective governments. This Agreement primarily focuses on the repatriation of criminals and suspects who have illegally entered each other country and implies cooperation between Taiwan and China in arresting the above individuals.

[303] The *Agreement on Cross-Strait Mutual Assistance in Crime Matters* was signed between the Taiwan-based Straits Exchange Foundation (SEF) and the mainland-based Association for Relations across the Taiwan Straits (ARATS) in 2009. The SEF is an organization set up by the ROC government (Taiwan) in 1991 for handling technical or business matters with the RPC. Its counterpart in China is the ARATS. Both sides agreed on collaboration on combating crimes recognized in both jurisdictions, particularly focusing on majors crimes involving kidnapping, weapons, drugs and human trafficking, corruption, money laundering, terrorism, fraud, forgery, cross-Strait organized crimes and other crimes.

indicated that, in some cases involving serious crimes, Taiwanese investigators will seek cooperation through informal channels like guan-xi (interpersonal relationship) or assistance from international companies to locate the source of attack. This may be helpful to the investigators in clearing the cases once the criminal is located but can do very little to further arrest and prosecution without mutual legal assistance.

Mutual legal assistance, either based on bilateral or multilateral treaty or convention or non-treaty request, is the key to effective law enforcement cooperation against cybercrime. However, Taiwan has been suffering from seeking legal assistance in investigation into cybercrimes due to its disadvantaged political position.[304] It is fundamentally important to look for alternative methods of cooperation with other countries against cybercrime for effective legal enforcement.

4.5. Conclusion

This chapter examined Taiwan's phishing legislation, including the Civil Law, the Copyright Act, the Trademark Act, and the Personal Information Protection Act and focusing especially on the Criminal Code and the two legal reforms, the 1997 Act and 2003 Act.

Personal information is not only the main target of phishing attacks but also frequently exploited to craft a spear phishing message as a leading vector to a data breach that is very likely to result in numerous phishing attacks. The protection of personal information against unlawful or unauthorised collection and use is hence a fundamental component which should be included in the regulation of phishing. Although the enactment of the PIP Act in 2010 attempted to strengthen protection of personal information and redress the problems that previously existed in the old law, this chapter

[304] Chapter 7 will demonstrate the empirical evidence of the difficulties experienced by Taiwan in seeking legal assistance by an analysis of the interviews with the key persons from Taiwanese law enforcement authorities as well as other fields. See Chapter 7, section 7.8.3.

argued that the Act, instead of correcting the pre-existing problems regarding the improper use of indeterminate legal concepts, actually adopted more vague legal concepts in the exceptional conditions to data collection and even created loopholes of legal protection. While the use of an indeterminate legal concept itself is not harmful and sometimes is unavoidable given the administrative flexibility, it may become a trouble if there is no specific authority taking charge of disputes over indeterminate legal concepts by providing a uniform interpretation after a coordination of the opinions of different organizations or authorities. This is exactly the case in Taiwan. Taiwan currently has no independent authority responsible for the tasks of personal information protection, in this case, a large employment of indeterminate legal concepts in the exceptional conditions to data collection prohibitions is not only improper but also increases the risk of abusing these concepts to evade liability for illegal data collection and may even encourage phishers to leverage efforts to obtain personal information from so-called 'publicly available resources' for subsequent malicious use.

Taiwan, like many other countries, does not make sui generis law that aims at prohibiting phishing but deals with phishing by applying the existing criminal law. Taiwan undertook a succession of legal amendments to the Criminal Code and introduced two Acts in 1997 and 2003 to respond to the rising of new forms of offences following the rapid growth of information technology; however, this chapter questioned their applicability to the conduct of phishing. The 1997 Act granted an electromagnetic record the same legal status directly as a movable property, but it failed to consider the conflict between the elements of the property crimes, especially larceny, and the object of electromagnetic records. The 2003 Act introduced a new Chapter 36 which was specially designed for the protection of security of computer use and electromagnetic records to the Criminal Code. Yet, there have existed discordant opinions, both academic and in judicial practice, on several elements of the offences relating to phishing, such as 'obtainment', 'unauthorised' and 'damage'. While researchers suggested that the element of 'damage' should be capable of broad interpretation, the judges in Taiwan often gave different decisions depending on whether monetary damage has occurred. This has given rise to the difficulties in applying the Criminal Code to phishing which in turn undermined its capability of dealing with phishing.

This chapter especially argued the inadequate effort that the 2003 Act has made to combat the supply chains of phishing resources as it only penalizes the makers of malicious computer programs and its focus is only on the prohibition of computer programs without punishing the disseminators or dealing with the creation or transfer of other phishing articles. Most importantly, the transnational nature of phishing often leads to failure of prosecution because of a shortage of mutual legal assistance and legal enforcement cooperation. The political dilemma of Taiwan makes effective law enforcement difficult to achieve, which highlights the need for a broader thinking of legal regulation that goes beyond criminal laws as well as the necessity of looking for other forms of regulation that goes beyond laws. The following chapter examines how personal information protection laws can contribute to the regulation of phishing in different aspects other than imposing punishment on phishing perpetrators.

CHAPTER 5 THE ROLE OF INFORMATION PRIVACY LAWS

Synopsis

This chapter looks into the role of information privacy protection in the regulation of phishing and examines the laws relating to personal data protection that have been developed in the global, regional, and Taiwan national interfaces, focusing especially on the interaction between these three regulatory interfaces and the extent to which Taiwan's personal information protection legislation is able to address the requirements raised from the regulation of phishing.

5.1. Introduction

This chapter argues that the need for legal control over phishing to go beyond the criminal law to take prevention into account by ensuring the security of personal information against unauthorised or illegal collection and disclosure. While criminal law has an important role in standard setting to determine the boundaries of permissible behaviour and penalize those who do not comply, whether it can actually deter phishing attackers still remains a question.[305] Legal regulation in the context of phishing demands a broad thinking which goes beyond criminal liability. However, as I have argued in previous chapters,[306] both international and Taiwan legal debates over phishing have too often concentrated on the discussion of criminal laws in terms of liability rules, legal reform, and

[305] The challenges of phishing to criminal legal enforcement have been discussed in Chapter 2 and 4 and will be explored in greater detail in the next chapter.

[306] See Chapter 2 (section 2.5.1), Chapter 3 (section 3.4) and Chapter 4 (section 4.3.4).

challenge to enforcement. While several researches and media press have suggested an increase of phishing-leading data breach incidents[307] and revealed a substantial growth of spear-phishing campaign which exploits freely available data on social networking websites,[308] very little scholarly discussion could be found that addresses how protection of information privacy and regulation of phishing relate to each other in different respects.

This chapter aims to contribute toward an understanding of the role of information privacy in the regulatory framework of phishing. It first highlights the relationship between phishing and information privacy and identifies the essential requirements raised from the regulation of phishing for legal protection of personal information. It then examines the privacy legal frameworks that have been developed at the global, regional, and Taiwan national levels, with a particular focus on the impacts of international developments upon Taiwan in passing its first data protection law in 1995 and subsequently amending it in the enactment of the Personal Information Protection Act in 2010. Most importantly, the chapter assesses whether the above Act is capable of providing adequate protection for personal information to facilitate better management and control of phishing or it may cause reverse effect on personal data protection by drawing the key problems observed from this Act.

5.2. Information Privacy and Phishing

[307] Baker, Wade, et al. (2011), '2011 data breach investigations report', *Verizon RISK Team*, 1-72. <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf>, accessed August 30 2014;Rivner, Uri (2011), 'Anatomy of Attack', *RSA Blog*. <http://blogs.rsa.com/rivner/anatomy-of-an-attack/>, accessed 17 September 2014;Tsukayama, Harley (2011), 'Cyber attack on RSA cost EMC $66 million', *The Washington Post*. <http://www.washingtonpost.com/blogs/post-tech/post/cyber-attack-on-rsa-cost-emc-66-million/2011/07/26/gIQA1ceKbI_blog.html>, accessed September 17 2014.

[308] Bonneau, Joseph and Preibusch, Sören (2010), 'The privacy jungle: On the market for data protection in social networks', in Tyler Moore, David Pym, and Christos Ioannidis (eds.), *Economics of information security and privacy* (Springer), 121-67;Jagatic, Tom N, et al. (2007), 'Social phishing', *Communications of the ACM,* 50 (10), 94-100.

There are three significant aspects to the relationship between information privacy and regulation of phishing.

First, phishing, as conduct which targets the unauthorized obtainment of a variety of confidential information including personally identifiable data, financial or other sensitive information by means of deceptive email messages or malware infection, undoubtedly, is a typical example of the use of information technology to threaten information privacy. The personal data protection law may constrain phishing attempts by imposing punishment on illegal collection of personal information.

Second, phishing has been increasingly used as a leading vector of large-scale data breach. Instead of individual users, more and more phishing attacks, especially spear phishing, target the public or private entities that hold large databases of personal information. While the issue of phishing-leading data breach has received increasing media attention,[309] it seems to draw little academic attention.

Third, a social networking service enables individuals to communicate and share information with their family, friends and hundreds of millions members instantly, whereas it also makes them expose their personal information with or without consciousness on a global scale. This has inspired a growing privacy concern and prompted significant number of research studies over information privacy with regards to social networking sites,[310] which nevertheless did not particularly address

[309] Hipolito, Joahnna Marie 'Anatomy of a Data Breach', (updated November 15 2011) <http://about-threats.trendmicro.com/RelatedThreats.aspx?language=tw&name=Anatomy+of+a+Data+Breach>, accessed August 15 2014;Rivner (2011), op. cit;Seybold, Patrick (2011), 'Update on PlayStation Network and Qriocity', *PlayStation.Blog*. <http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/>, accessed September 19 2014;Tsukayama (2011), op. cit.

[310] Acquisti, Alessandro and Gross, Ralph (2006), 'Imagined communities: Awareness, information sharing, and privacy on the Facebook', in George Danezis and Philippe Golle (eds.), *Privacy enhancing technologies* (Cambridge, UK,: Springer), 36-58;Ellison, Nicole B (2007), 'Social network sites: Definition, history, and scholarship', *Journal of Computer-Mediated Communication,* 13 (1), 210-30;Fogel, Joshua and Nehmad, Elham (2009), 'Internet social network communities: Risk taking, trust, and privacy concerns', *Computers in Human Behavior,* 25 (1), 153-60;Gross, Ralph and Acquisti, Alessandro (2005), 'Information revelation and privacy in online social networks', *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (ACM), 71-80;He, Jianming, Chu, Wesley W, and Liu, Zhenyu Victor

phishing. The most important academic work about phishing and social networking sites was provided by Jagetic et al.[311] in 2007 where the authors found that the vast amount of personal information available from the social networking websites dramatically enhances the success of phishing attacks which is evidenced by the result of their experiment conducted upon the students at the Indiana University in 2005. Bonneau and Preibusch[312] provided an analysis of the privacy practices and policies of over 45 social networking sites in which the authors indicated that the privacy market did not function properly in social networks, and the social networking sites surveyed disregarded anti-phishing work and hardly took any measure to protect their users from phishing attacks. This can be addressed by strengthening legal regulation with regard to social networking service providers in terms of reinforcing data security measures, enhancing the privacy environment for their users, and ensuring their users are well-informed about the risk potentially relevant to their creation of profiles on the sites.

This section begins with a brief review of the historical development of the concept of information privacy, which is followed by an examination on the sources of threat to information privacy, with a particular focus on phishing. It also suggests the key elements that should be particularly included in the personal data protection legislation in order to better correspond to the requirements raised from phishing regulation.

(2006), 'Inferring privacy information from social networks', in Sharad Mehrotra, et al. (eds.), *Intelligence and Security Informatics* (Springer), 154-65;Lindamood, Jack, et al. (2009), 'Inferring private information using social network data', *Proceedings of the 18th international conference on World wide web* (Madrid, Spain: ACM), 1145-46;Marsoof, Althaf (2011), 'Online social networking and the right to privacy: The conflicting rights of privacy and expression', *International Journal of Law and Information Technology*, eaq018;Xu, Wanhong, Zhou, Xi, and Li, Lei (2008), 'Inferring privacy information via social relations', *IEEE 24th International Conference on Data Engineering Workshop, 2008 (ICDEW 2008)* (Cancun, Mexico: IEEE), 525-30;Zheleva, Elena and Getoor, Lise (2009), 'To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles', *Proceedings of the 18th international conference on World wide web* (Madrid, Spain: ACM), 531-40.

[311] Jagatic et al. (2007), op. cit;Johnson, Nathaniel A., Jakobsson, Markus, and Menczer, Filippo (2007), 'Social Phishing', *Communications of the ACM,* 50 (10), 94-100.

[312] Bonneau and Preibusch (2010), op. cit.

5.2.1. Concept of information privacy

Gavison suggested that the concept of privacy is constituted by a complex of three independent and interrelated elements, namely *secrecy*, *anonymity*, and *solitude*, which were shorthand for "*the extent to which an individual is known, the extent to which an individual is the subject of attention, and the extent to which others have physical access to an individual*".[313] A loss of privacy occurs, accordingly, when others obtain information about an individual, pay attention to him, or gain access to him.

Privacy has several dimensions, which usually cover *bodily privacy*, *territorial privacy*, *privacy of communication*, and *information privacy*.[314] It involves the protection of a person's body against invasive procedures such as drug testing and cavity searches; the resistance to intrusion into the close physical areas surrounding a person, such as residence and the workplace; the privacy of mail, telephone calls, email and other forms of communication; and the control of whether or how personal data can be gathered, stored, processed or disseminated. Privacy is a term which has been broadly interpreted; as Volio observed, "*In one sense, all human rights are aspects of the right of privacy.*"[315]

In 1890, Warren and Brandeis[316] took "*the right to be let alone*", the phrase coined by Judge Cooley, as a distinct ground for the protection of the private individual against the unjustifiable infliction of mental distress caused by the growing abuse of the press.[317] The work of Warren and

[313] Gavison, Ruth (1980), 'Privacy and the Limits of Law', *Yale law journal*, 421-71.

[314] Banisar, David and Davies, Simon (1999), 'Privacy and human rights: an international survey of privacy laws and practice', *Global Internet Liberty Campaign*. Rosenberg, Richard S (1992), *The social impact of computers* (Academic Press Professional, Inc.).

[315] Volio, Fernando (1981), 'Legal personality, privacy and the family', in Louis Henkin (ed.), *The International Bill of Rights* (New York: Columbia University Press).

[316] Warren, Samuel D and Brandeis, Louis D (1890), 'The right to privacy', *Harvard law review*, 193-220.

[317] Gavison argues that Warren and Brandeis regarded the right to privacy as a special case of the right to be let alone rather than equating the two. Gavison (1980), op. cit..

Brandeis has not only had a profound impact upon American law[318] but has also been significantly influential internationally on the subsequent theoretical and legal development of the right of privacy.

The 1960s and 1970s saw the advent of information technology which enabled the surveillance potential of powerful computer systems, in conjunction with a distinct shift in the direction of information privacy from the sustainability of a seclusion space to the defence of the data subjects' control and determination over the handling of data about themselves. Although Zamyatin[319] sensed the forthcoming change long before it happened, his concern was aroused by the threat of authoritarian governments harnessing technology to achieve anti-democratic ends. Technology, itself a determinant of the change, has been gradually recognized from about 1950 onwards.[320]

The dramatic growth of automatic data processing and the Internet has largely accelerated the capacity and speed of information storage and transmission, bringing us to a new information age – an age in which the vast bulk of personal information can be accessed, stored and transmitted within seconds across national frontiers. A rapid cross-border data flow significantly assists the development of social and commercial activities; however, it has also posed a crucial challenge to data protection with regard to ensuring that the data subjects have sufficient control over their data.

[318] The views of Warren and Brandies were accepted and the existence of a right to privacy was first recognized in a 1905 case, *Pavesich v. New England Life Insurance Co.*, in the state of Georgia. Although there was continued debate for the following thirty years on whether the right of privacy existed at all, the majority of American courts allowed the plaintiffs to seek legal remedies for the invasion of the right of privacy. In the first half of the 20th century, the American courts created an independent basis for liability which in fact comprises four distinct kinds of invasion of the four different interests of the plaintiff – intrusion into the plaintiff's seclusion or solitude, public disclosure of private facts which would be offensive and objectionable to a reasonable man, placing the plaintiff in a false light in the public eye, and the appropriation of the plaintiff's name or likeness for the defendant's advantage. Prosser suggests that these four invasions were built on the same basis, i.e. the right to privacy; however, they differ and have little in common. While intrusion and public disclosure involve an invasion of private things, false light does not, nor does appropriation. Publication disclosure and false light rely on publicity, whereas intrusion and appropriation do not. Only appropriation requires use for the defendant's advantage, which is not seen in the other three types of invasion. Prosser, William L. (1960), 'Privacy', *California Law Reivew,* 48 (3), 383-423.

[319] ZAMYATIN, Evgeny Ivanovich, GLENNY, Michael V, and GUERNEY, Bernard Guilbert (1972), *We... Translated [from the Russian MS.] by Bernard Guilbert Guerney. Introduction by Michael Glenny* (Penguin).

[320] Clarke, Roger (2000), 'Beyond the OECD guidelines: privacy protection for the 21st century', *Canberra, Australia: Xamax Consultancy Pty Ltd. Retrieved August,* 5, 2009.

It has hence inspired an increasing demand for the data subjects to choose freely under what circumstances and to what extent their personal data will be collected, used, and processed, whether they are held by themselves, other individuals or public or private controllers. In this context, privacy, as Westin defined, *"is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."321*

Over the past few decades, the rapid technological development and intensive collection of personal data have profoundly changed the world around us, and posed new challenges regarding the protection of personal data. Today, technology allows individuals to communicate, share and exchange information about their life, family, or work with others in a highly efficiently manner; however, this at the same time makes their information publicly and globally available on an extraordinary scale. Social networking sites, such as Facebook, MySpace and Twitter, which provide networking services that enable individuals to share and update their ideas, activities, interests and events with hundreds of millions of members across the globe, may serve as an obvious example of this phenomenon. Although the development of information technology may have brought about a more convenient communication method, it has been accompanied by an increase in the extent and potential risk of the invasion of information privacy.

To conclude, privacy has varied dimensions and can be defined widely according to the specific context and environment. The protection of privacy initially focused on the right to solitude of an individual, including his home and family but there has been a tendency to broaden the traditional concept of privacy to one which perhaps more precisely corresponds to the demands of the modern age. The increasing sophistication of information technology in terms of its speed and capacity to collect, analyze and disseminate information has inspired a greater concern about information privacy and introduced a sense of urgency to protect personal data against inappropriate disclosure,

[321] Westin, Alan F (1970), *Privacy and freedom* (London: Bodley Head).

collection, use, and process.

The threats to information privacy come from various sources, which may include information technology, government, commercial corporations, and cyber criminals. The following subsection will look into the sources of threats to information privacy, particularly focusing on the threat posed by phishing.

5.2.2. Threats to information privacy

5.2.2.1. The sources of threats

It cannot be denied that the Internet provides a platform for new forms of communication and interaction that, to a certain extent, better safeguard privacy because of its characteristic of anonymity. People may feel more comfortable about expressing themselves, communicating with others, or engaging in cyber activities without being identified. Information technology can also enhance privacy through the use of encryption techniques in browser software, which permits the transfer of credit card numbers, login information and other personally sensitive data in a secure manner.

However, in the digital era, information technology has also been viewed as the source of many privacy concerns. It is possible, using the current protocols for Internet communication, to record every activity of an individual, the information he receives, the people he communicates with and his preferences. Technological development has created tools for collecting personal data which have become increasingly elaborate and less easily detectable. For example, cookies[322] allow

[322] A cookie is "a small piece of data sent from a website and stored in a user's web browser while the user is browsing that website. The browser sends back the cookie to the server to notify the website of the user's previous activity every time when the user loads the website." See: http://en.wikipedia.org/wiki/HTTP_cookie#cite_note-1.

publishers to monitor a user's web behaviour to generate customized advertising across websites for a particular user based on what is known about the website he has visited. A server may uses cookies for various purposes, which may include maintaining data related to a user such as shopping cart contents or authentication credentials, personalizing web content based on the user's preferences, and tracking the user's web browsing habits. A cookie per se is harmless, as it cannot carry a virus, nor does it install malware on the user's computer. Cookies may help users to navigate faster around those websites that they visit regularly and find the goods that interest them; however, it may lead to an invasion of privacy, especially when users are unaware that they are being tracked or, even worse, when cookies are stolen by hackers to gain access to users' web accounts.[323]

The government can also diminish the privacy of information through schemes for compelled identification, census enumeration, database profiling, and the regulation of the use of privacy enhancing techniques, such as encryption. The threat to privacy posed by government actions is particularly harsh, as citizens often have little choice but to comply. The great power of government surveillance has been a major source which substantially endangers people's right of privacy. Particularly, after the event of 9/11/2001, the anti-terror climate led to the expansion of surveillance and government control over digital personal information by enthusiastically adopting surveillance measures, such as CCTV cameras in public spaces, increased border scrutiny, accessing personal information collected by the private sector and observing online speech and activities.

[323] EU Directive 2009/136/EC, known as the Cookie Directive, states that a cookie can only be stored on a computer or accessed from a computer if a user has given his consent, having been provided with clear, comprehensive information. The full text of the Cookie Directive is available at: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=EN&numdoc=32009L0136. Art. 5(3) of EU Directive 2002/58/EC, known as the e-Privacy Directive, requires users to be informed about the use of cookies, the purpose that the cookie will be used for, and their right to opt-out of the use of cookies. This was replaced by the new Cookie Directive that establishes an opt-in requirement for the use of cookies where the storing or accessing of information on computer is only permitted if the user has given his explicit consent to this. The full text of the e-Privacy Directive is available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT.
The U.S. Federal Trade Commission's report of December 2010 proposes a "Do Not Track" system by enforcing opt-out for behavioural advertising. Technically, several opt-out services are available, including the tools provided by Google's Chrome and Mozilla's Firefox, both of which allow users permanently to stop advertisers from monitoring their browsing data.

Another noticeable threat to privacy comes from corporations based on the 'personalization' or 'one-to-one marketing' business models. As Lloyd suggested, we are moving to a situation where information becomes the major measure of wealth and power.[324] Because of the strong commercial incentive, the majority of business corporations tend to extract as much information as possible from their customers by asking extensive questions. It is no longer sufficient for customers to make payments for goods and services, as they must also provide their personal details that are not really related to a particular transaction before any commercial relationship is established. While some requests may be necessary and appropriate, much more data collection appears to be unrelated to the transaction purpose. For example, a customer should expect to provide his home address if he wishes an item to be sent to his home, but he need not answer questions about his buying preferences, shopping habits, how he learnt about the website, or other questions which appear unrelated to the transaction.

In fact, data subjects should be entitled freely to exercise their right to information privacy without suffering from a potential disadvantage. However, on the overwhelming majority of websites, individuals are not allowed to purchase goods or access services unless they have registered for a new account by providing the so-called mandatory information about themselves. This may involve inappropriate interference with the individuals' right of information privacy if they can only choose to leave the website or yield to them, which means that they are not allowed to have any discretion over the extent of information they provide.

Cyber criminals, especially those who directly target acquisition of confidential information such as hackers or phishers, have also been a major source responsible for the increasing threat to information privacy. The following subsection will particularly look into the relationship between

[324] Lloyd, Ian J (2000), *Legal aspects of the information society* (Butterworths).

phishing and information privacy and examine the role of personal information protection in the regulation of phishing.

5.2.2.2. Phishing

A direct infringement of information privacy

A phishing attack, which directly targets the unauthorized obtainment of various confidential information such as personally or financially sensitive data, without a doubt, is an immediate invasion *per se* of information privacy. Accordingly, imposing threat of punishment on the people who access, collect, process or use personal information without authorization can be a way to deter phishing attempts.

A leading vector for data breach

Phishing schemes, especially spear or targeted phishing, have been intensively used to gain a toehold in the victim's environment for a data breach.[325] It is no longer only the end user who becomes the victim of a phishing attack, but enterprises and even governments are now truly at risk. It is a comparatively efficient way to obtain information, as the attackers can easily walk off with masses of personal information as long as they can gain access to the database systems operated by the private or public sector.

A data breach refers to an unauthorized or unintentional exposure, disclosure or loss of data. These

[325] Baker et al. (2011), op. cit;Oussayef, Karim Z (2008), 'Selective privacy: Facilitating market-based solutions to data breaches by standardizing internet privacy policies', *BUJ Sci. & Tech. L.,* 14, 104;Symantec (2014), 'Internet Security Threat Report 2014', 19. <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf>, accessed August 31 2014.

data are generally kept in the target organization's systems or networks, and are usually confidential and sensitive in nature. They may include personally identifiable information, customer data, trade secrets, etc. Data breaches can be triggered by insiders; for example, employees who intend to do harm to the company by purposely taking information from it. A data breach can also accidentally occur[326] or can be actuated by malicious attackers. Hacking, malware, and social (phishing) were indicated to be the common threat actions that cause a data breach.[327] A data breach is often committed by breaking into the targeted data base through making use of a weakness in the targeted infrastructure, system, and application, or employing techniques such as SQL injection[328] and session hijacking.[329] It is also frequently triggered by phishing individuals who work for or are closely associated with the targeted entities and so can gain access to a database through the compromised computers or network.

Although network infrastructure weakness has been a main object targeted by cybercriminals to intrude into database systems, recent data breach incidents reveal the increasing interest of cybercriminals in attacking a critical element, which is extremely difficult to manage and control but easy to overlook, namely, humans. The manipulation of human weakness, such as trust or curiosity, is described as "an ever-present bane" to any robust secure infrastructure.[330]

The Executive Chairman of RSA[331] sent an open letter to its customers on 17 March 2011,

[326] For example, lost or stolen devices that carry information or the unintentional disclosure of information in conversations or online, such as through instant messaging or via social networking platforms.

[327] Baker et al. (2011), op. cit.

[328] For example, a hacking group, LulzSec, claimed on June 2, 2011 that it has broken into several Sony Pictures websites and gained access to more than a million customers' confidential information, including their passwords, contact details and other personally sensitive information. This attack against SonyPicture.com, according to the statement of LulzSec, was carried out by employing a "very simple SQL injection". Vijayan, Jaikumar (2011), 'Sony Pictures falls victim to major data breach', *COMPUTERWORLD*. <http://www.computerworld.com/s/article/9217273/Sony_Pictures_falls_victim_to_major_data_breach>, accessed September 15 2014.

[329] Session hijacking is the theft of a user's session ID to gain unauthorized access to information or services on a computer system.

[330] Hipolito (2011), op. cit.

[331] RSA is the security division of EMC corporations, famous for its encryption and network security products such as

disclosing that a data breach had occurred within RSA. It was reported that this incident resulted in the compromising of information on nearly 40 million RSA security tokens and a reported cost of US$66 million.[332] The attackers behind the RSA breach, as explained in the report by Uri Rivner,[333] launched a social-engineering attack by sending two different phishing emails with the subject "2011 Recruitment Plan" to two small groups of RSA employees over a two-day period. One of the said employees opened the attached Excel file with the same file name as the subject after he retrieved the email from his Junk Mail folder, unaware that the attachment contained a zero-day exploit.[334] This exploit installed a backdoor that allowed the attacker to gain elevated access to the network until he had gathered the information that he sought from the target server and staged data exfiltration.

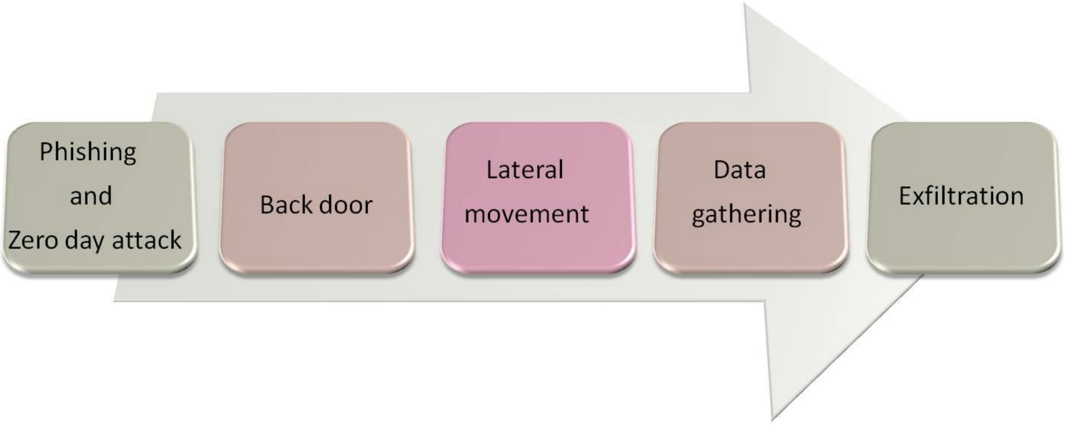


Diagram 5.1: RSA breach 2011

Another well-known phishing-leading data breach happened between 17 and 19 April, 2011, where Sony PlayStation Network underwent an illegal unauthorized intrusion which resulted in the personal information of 77 million user account holders being stolen. According to Sony's blog announcement of 26 April, the stolen information included names, addresses, log-in and password

the RSA BSAFE security software and the SecurID authentication token.

[332] Tsukayama (2011), op. cit.

[333] Rivner (2011), op. cit.

[334] A zero-day attack is a computer threat that seeks to exploit computer application vulnerabilities those are unknown to the software developers.

details, password security answers, email addresses, and birth dates. The users' purchase history and credit card information had probably been compromised too.[335]

A mutually complementary relationship is found between phishing and data breach, where phishing significantly facilitates the chance and success of data breach, the large volume of stolen personal information obtained from a data breach, at the same time, remarkably enriches the creation of targeted phishing attacks which in turn leads to numerous phishing scams.[336] For example, in August 2007, hackers broke into a U.S. online recruitment site, Monster.com, and swiped the contact information such as names, addresses, phone numbers or email addresses of more than 1.6 million jobseekers. The stolen information was subsequently used in phishing scams by sending the victims legitimate-looking Monster messages with attempt to infect their machines with a Trojan horse.[337]

Phishing and data breach can mutually enhance each other, which means a single phishing incident may result in countless phishing attacks coming after a data breach. Today's growing population relies on computers[338] to engage in their daily social or commercial activities. While corporations tend to extract as much personal data as possible from their customers, the extensive collection of individual's personal data may involve not only an inappropriate interference of individual's control over their data but also an unpredicted danger of unlawful access if the data cannot be properly safeguarded. The dramatic increase of phishing-leading data breach incidents makes it a pressing task for data controllers to take necessary security measures such as technology or organizational measures to protect personal information database against malicious access or collection. This

[335] Seybold (2011), op. cit.

[336] Acquisti, Alessandro, Friedman, Allan, and Telang, Rahul (2006), 'Is there a cost to privacy breaches? An event study', *27the International Conference on Inofmration Systems (ICIS 2006)* (1; Milwaukee, Wisconsin, USA), 1563-80;Armerding, Taylor (2012), 'The 15 worst data security breaches of the 21st Century', *CSO Security and Risk, February 2012*.

[337] Hidalgo, Amado (2007), 'A Monster Trojan', *Symantec Blog*. <http://www.symantec.com/connect/blogs/monster-trojan>, accessed August 17 2014.

[338] This includes all devices that can provide Internet access, such as PCs, mobile Internet devices or smartphones.

should be guaranteed by distinct legal obligation provided by the law.

Exploitation of social networking sites (SNSs)

A standard phishing attack is usually broad-based, whereas the strategy engaged in the foregoing RSA case is highly-targeted, which is known as a spear phishing attack. As I have mentioned in Chapter 2 (section 2.4.1), there is a substantial growth of spear-phishing campaign in terms of both quantity and quality. A recent Symantec's report[339] showed an increasing number of users, in particular their work-related email accounts, have been targeted by spear phishing attacks over the past decade. In addition to individual users, 61 percent of business-targeted spear phishing attacks aimed at SMBs with less than 2,500 employees and 39 percent of which were sent to large enterprises comprising over 2,500 employees. This caused nearly 1 in 2 of large enterprises suffered at least one spear phishing email in 2013.

Compared with standard phishing which employs mass-mail attacks in a hope that some would take the bait, spear phishing attacks are much more targeted which involve low volume of customized messages used to dupe particular individuals within a specific organization into visiting a fake website or downloading malware onto their machines. Although spear phishing campaigns are limited in volume, they offer higher user open and click-through rate of 19%, compared to only 5% for standard phishing attacks.[340] Despite that a spear phishing attack is much more complex and costly than traditional phishing, the rewards are much greater too. A report from Cisco Security Intelligence Operations (SIO)[341] estimated that while a spear phishing attack can cost 5 times as

[339] Symantec (2014), op. cit.

[340] Searchitchannel (2006), op. cit.

[341] Cisco (2011), 'Email attacks: this time it's personal', *Cisco Security White Paper*. <http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/targeted_attacks.pdf>, accessed September 8 2014.

much as a mass-mail phishing, it can yield profit of more than 10 times.[342]

The success of spear phishing campaigns can be imputed to a number of factors, most of which have been discussed in Chapter 2 (section 2.5). The most important reason for why spear phishing emails are so convincing is that they are designed to be highly personalized which significantly improves their authenticity and thus increases the likelihood of the recipient complying with their request. Spear phishing messages are well-crafted and customized based upon knowledge about the recipients, including their personal information, position in the company, work, interests or interpersonal relationships. Conducting a background research on the recipients is extremely helpful to attackers when concocting a compelling phishing message that can solicit the recipients to follow the link enclosed or open the attached file. This can be illustrated by the attack experienced by Google where an attacker targeted an individual within Google who had access to high-value information by sending the target a web link from a friend's Facebook account which was embedded with new piece of malware after spending a few months on monitoring the target's online activities and collecting personal information via social networking sites. This message successfully fooled the unsuspecting target into believing it really came from a friend and clicking on the link which ultimately allowed the attacker access to Google mainframe server.[343]

The exponential growth in usage of social networking services, such as Facebook and Twitter, has

[342] While a traditional phishing attack mostly targets the confidential information of individual users, including their personal data, login credentials or banking information, spear phishing attackers turn their greedy eyes towards more lucrative targets of high-value victim, ranging from massive customer database, the trade secrets of enterprises and even government political or military secrets. Symantec revealed a spear phishing campaign directed at nearly fifty (at least) companies primarily involved with chemicals, defence and advanced materials in its newly released report. The attacks, which occurred between late July and mid-September 2011, appear to collect intellectual property, such as R&D and manufacturing information. As the attackers focus on information about chemical compounds and other advanced materials used by the military, this campaign was code-named Nitro. A Nitro attack is carried out by sending the employees of the target companies, ranging from a handful to 500 recipients, an email containing an executable file which carries a backdoor Trojan that allows the attackers to traverse the network, infecting additional computers and searching for access to a system storing intellectual property secrets. See: Chien, Eric and O'Gorman, Gavin (2011), 'The Nitro Attacks, Stealing Secrets from the Chemical Industry', *Symantec Security Response*.

[343] Parmar (2012), op. cit.

dramatically changed the interconnection between individuals through establishing a mobile communication capacity. The users of these services can make instant contact with their friends and also meet new people by sharing their profiles, interests, and diaries, as well as updating their activities. While social networking sites (SNSs) allow individuals to exchange and share information instantly, they make their personal information publicly available to many around the world. This has inspired a growing concern about privacy with regard to SNSs. Most importantly, SNSs have become a dominant source providing large amount of sensitive and personal information, such as name, data of birth, living place, occupation and hobbies, for phishers to compose a targeted phishing message for a specific individual.

The popular press stressed the danger of SNSs to privacy especially among younger users.[344] Researchers have investigated the potential threat to privacy concerning SNSs.[345] One of the first academic studies of privacy and SNSs was conducted by Gross and Acquisti in 2005.[346] The authors analyzed the Facebook profiles of more than 4,000 Carnegie Mellon University students and found that while the users generously provide a large amount of personal information in an online social network, they care very little about the potential privacy risk and barely use privacy preference settings, which had exposed themselves to various risk in both real and virtual world. In another work,[347] Acquisti and Gross found that privacy concerns do not lead to obvious changes in the bahaviours of SNSs users. The authors also suggested that while some users feel confident in their ability to control the information they provide and manage external access to their information, they may misunderstand or ignore the visibility of members' profiles and the actual size and compositions of SNSs. In addition, women were found to be more concerned about privacy and

[344] George, Alison (2006), 'Living online: The end of privacy', *New Scientist,* 2569, 1-50;Kornblum, Janet and Marklein, Mary Beth (2006), 'What you say online could haunt you', *USA Today*. <http://usatoday30.usatoday.com/tech/news/internetprivacy/2006-03-08-facebook-myspace_x.htm?csp=N007>, accessed September 7 2014.

[345] Ellison (2007), op. cit.

[346] Gross and Acquisti (2005), op. cit.

[347] Acquisti and Gross (2006), op. cit.

identity information disclosure than men.[348]

Several studies indicated that the released data obtained from social networking sites can enable accurate inference of information about an individual which is supposed to be private and undisclosed.[349] Network's ties can not only connect someone's profile to hundreds of peers directly but also extend the connection to thousands of others who may be actual friends but many are complete strangers.[350] It is almost impossible in practice to maintain a real private profile once you decide to build social relations with others through online social networking sites.

Users' account information for accessing social networking service itself is often targeted by phishing attackers,[351] and the stolen account credentials are frequently exploited to assist in various phishing attacks over social networks, for example spreading worms through infected links[352] or even requesting money from unsuspecting online 'friends'.[353] Most importantly, the plentiful personal information that is able to be found on SNSs provides the best material for phishers to generate a highly convincing message and increases the power of a phishing attack. A number of studies have been conducted to explore how effectively publicly available personal information from social networks helps to yield successful phishing attacks.[354] Jagatic et al. used freely available data by crawling SNSs to build a database with tens of thousands of relationships. They then performed an actual but harmless phishing attack on students aged 18- 24 at the Indiana

[348] Fogel and Nehmad (2009), op. cit.

[349] He, Chu, and Liu (2006), op. cit;Lindamood et al. (2009), op. cit;Xu, Zhou, and Li (2008), op. cit;Zheleva and Getoor (2009), op. cit.

[350] Gross and Acquisti (2005), op. cit.

[351] Arrington, Michael (2008), 'Phishing For Facebook', *TechCrunch*. <http://techcrunch.com/2008/01/02/phishing-for-facebook/>, accessed September 8 2014.

[352] Waugh, Rob (2010), 'Watch your wall: New Facebook attack has stolen passwords from 45,000 users - and could be spreading through infected links', *Daily Mail*. <http://www.dailymail.co.uk/sciencetech/article-2083118/Facebook-hacked-Ramnit-worm-stolen-passwords-45-000-users.html>, accessed September 13 2014.

[353] Frommer, Dan (2009), 'What a nigerian facebook scam looks like', *The Business Insider*. <http://www.businessinsider.com/2009/1/nigerian-scammers-still-roosting-on-facebook>, accessed September 11 2014.

[354] Jagatic et al. (2007), op. cit;Johnson, Jakobsson, and Menczer (2007), op. cit.

University in April 2005. The above experiment revealed that the exploitation of social network data dramatically enhances the success of a phishing attack, which increased more than 4 times success rate to make users become victims, compared to a traditional phishing attack.

New technological development and the changing online environment have led to the explosive online-disclosure of personal information, with or without the consciousness of the data subjects. This has made it an increasingly difficult task for individuals to control and protect their information against unauthorized collection, processing and use. While educational campaigns about privacy concerns with regard to SNSs are essential to help users be less vulnerable to phishing by heightened awareness of the risk and the potential misuses of publicly accessible personal information, SNSs should also take responsibility to provide their users adequate protection of privacy. However, Bonneau and Preibusch,[355] in their analysis of the privacy practices and policies over 45 SNSs, argued that significant variation in privacy controls, data collection requirements, and legal privacy policies among SNSs has resulted in a "dysfunctional" privacy market in social networks. The authors found that the SNSs surveyed paid no attention to anti-phishing work and hardly took any particular measure to protect their users from spoofed SNSs or protect the users' account credentials from being stolen. In addition, while the privacy policy is crucial for users to rely on when they give informed consent to data collection, the authors indicated that the privacy policies of most SNSs surveyed were too long to be expected to be read by most users. All the SNSs surveyed reserved the right of data collection and most reserved the rights of data sharing in their privacy policies, whereas few provided the duration of data detention and nearly half of the SNSs did not explicitly grant users the right to have their data deleted upon request.

Vast amount SNSs data have been increasingly abused by phishers to craft a spear phishing attack

[355] Bonneau and Preibusch (2010), op. cit.

which usually leads to large-scale data breach incidents and subsequent numerous phishing attacks. To ensure users' control over their personal information and prevent potential exploitation for phishing, it is hence important to strengthen the role of law in the protection of personal information by requiring SNSs, as well as other data controllers that hold great number of highly sensitive information such as banks or other financial institutions,[356] to make sure their users are well informed of the risk they are taking and are provided with a proper environment to best manage and control their personal information, for example, enhancing accessibility of privacy policies both technically and linguistically, reducing permissive privacy default settings and improving usability of privacy setting interfaces. SNSs should also avoid unnecessary data collection and undue limitation on users' management of privacy control.

5.2.2.3. The demands for personal information protection laws in terms of phishing

The growing challenges and threats posed by phishing to privacy have prompted an urgent demand for the strengthened protection of personal information and specific regulations governing the collection, use, and processing of personal data. The following elements need to be particularly included in the personal information protection laws in order to effectively address phishing.

Maintaining the confidentiality of personal data

Keeping personal information in a 'personal' and 'confidential' status is the most basic requirement for data protection, whether it is held by the data subjects themselves or other data controllers. The unnecessary disclosure of personal information should be avoided and the data controllers should strictly limit the number of personnel who are authorized to access the data. To reduce the risk of

[356] Fox, Mark A. (2006), 'Phishing, pharming and identity theft in the banking industry', *Journal of International Banking Law and Regulation,* 21 (9), 548-52.

phishing, the data controllers especially banks or other financial institutions should also avoid sending emails or texting messages to request their customers to transmit personal information via emails or messages.[357]

Ensuring the security of databases

The dramatic rise in the number of data breach incidents carried out via phishing schemes or exploiting the infrastructure weakness has generated increasing demand for sufficient and appropriate security measures that can effectively safeguard the privacy of personal data. In addition to technological measures for monitoring and detecting any invasion or unusual activity, personnel should receive training on information security and management, as well as the response to threats. It is also essential for data controllers to enhance their protection against unlawful access by adopting routine security practices such as penetration tests or system vulnerability scanning to elevate the overall defensive ability of both the personnel and systems.

Strengthening the data subjects' control and choices regarding their data

When users decide to hand over their personal data, it does not mean they intend to render or ease their control over the data. In contrast, the data controller should be obligated fully to respect the data subjects' right to their personal information, including the right of access, correction or deletion, and the right of choice regarding the collection, processing and use of their information. Any collection from either the data subjects or data controllers, or any disclosure of personal information to a third-party should not be permitted unless it is with the consent of the data subjects. The data subjects should be well informed regarding the handling of their personal data and their consent should be seen as a requisite condition which can only be dispensed under very limited

[357] Ciocchetti, Corey (2007), 'The Privacy Matrix', *Journal of Technology Law & Policy,* 12, 245.

circumstances. Also, it is important to enhance the protection of the data subjects' free choice of how and to what extent they would expose their personal data without inappropriate interference or limitation.

5.3. Information Privacy Laws

This section examines the multilayered privacy laws, including the international, regional and in particular Taiwanese national laws based on the specific requirements appropriate to the regulation of phishing. This section also includes a study of the data privacy frameworks that have been undertaken by several international instruments since the 1970s, with a particular focus on their impacts on the development of data protection laws in Taiwan.

5.3.1. Privacy as a human right

5.3.1.1. International agreements

A few may argue for the end of privacy as a human value;[358] however, for the vast majority of people, privacy is a critical human right that must be defended. The core privacy principles in international human rights instruments can be found in the *1948 Universal Declaration of Human Rights (UDHR).*[359] Art. 12 of the UDHR, which specifically focused on the protection of territorially and communication privacy, states:

[358] Whitaker, Reginald (1999), *The end of privacy: How total surveillance is becoming a reality* (The New Press). Whitaker argues that the introduction of new technologies and surveillance are constantly compressing the private spaces of individuals and making them more and more transparent.

[359] The Universal Declaration of Human Rights (UDHR), adopted by the United Nations General Assembly in Paris in December 1948, consists of 30 articles and represents the first global instrument of rights to which all human beings are inherently entitled. Full text of UDHR, http://www.hrweb.org/legal/udhr.html.

> No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks. (Art. 12 of UDHR)

By adopting similar language, Art. 17 of the *International Covenant on Civil and Political Rights (ICCPR)*[360] provides:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> Everyone has the right to the protection of the law against such interference or attacks. (Art. 17 of ICCPR)

The term 'unlawful' here means that no interference or attack can take place unless it is authorized by law, which itself must observe the provisions, aims and objectives of the Covenant.[361]

The Human Rights Committee stated, in its General Comment 16, that Art. 17 required the legal implementation of data protection guarantees in both the public and private bodies.[362] The

[360] The International Covenant on Civil and Political Rights (ICCPR) was adopted by the United Nations General Assembly in 1966 and entered into force in March 1976. The ICCPR is a multilateral treaty which commits its party states to respecting civil and political rights. It is monitored by the Human Rights Committee through reviewing regular reports of its party states on how the rights are being implemented. The ICCPR, along with the Universal Declaration of Human Rights and the International Covenant on Economic, Social and Cultural Rights, form the International Bill of Human Rights. Full text of ICCPR, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[361] Human Rights Committee, General Comment 16, see: http://www.ohchr.org/EN/HRBodies/Pages/TBGeneralComments.aspx.

[362] General Comment 16: The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of

Committee reads into Art. 17 a limitation on the collection of personal data and mentions the need for security measures to ensure the confidentiality of personal information and also the right to information access and rectification. However, it is worth noting that the protection object, i.e. the personal information or personal data listed here, are formulated differently by the Committee. Whereas the limitation on gathering and holding applies to general ‘personal information’ without specification, the Committee clearly states that effective measures are needed for safeguarding ‘information concerning a person’s private life’. Also, it seems that the right to information access, rectification and elimination is formulated only in relation to ‘personal data stored in automatic (computerized) files’. Nevertheless, three different formulations of personal information provided by the Committee may lead to difficulty and inconsistency of application.

Differing from the above provisions that focus on the prohibition of ‘interference with privacy’, the equivalent provisions of Art. 8 of the *European Convention on Human Rights (ECHR)*[363] are framed in terms of a ‘right to respect for private life’:

> Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic

persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data are stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.

[363] The European Convention on Human Rights (ECHR), a multilateral treaty drafted in 1950 by the Council of Europe, came into force in September 1953 to protect human rights and fundamental freedom in the member states of the Council of Europe. The ECHR established a supra-national court, the European Court of Human Rights, which hears complaints brought by the party states or any person who feels that his rights has been infringed under the ECHR by a party state. The execution of the judgments made by the European Court of Human Rights is monitored by the Committee of Ministers of the Council of Europe.

> society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. (Art. 8 of ECHR)

The ambit of the 'right to respect for private life' has been interpreted by the European Commission of Human Rights as being 'such that it secures to the individual a sphere within which he can freely pursue the development and fulfillment of his personality'.[364] Art. 8 of the ECHR does not merely compel a state party to abstain from interference with private life; it additionally comprises 'positive obligations' of the state party to take action to ensure that private life is effectively respected.[365]

Although Art. 17 of the ICCPR and Art. 8 of the ECHR appear to lack explicit and comprehensive data protection guarantees compared with those found in instruments related specifically to data protection, the above two provisions demonstrate a willingness of the Human Rights Committee and the Strasbourg organs to adapt the provisions to take account of the potential danger that the new form of data processing creates regarding the privacy of individuals.[366]

The Charter of Fundamental Rights of the European Union[367] has specific sections on the privacy of private and family life (Art. 7) and on the protection of personal data (Art. 8), which provide:

[364] *Deklerck v Belgium*, 1980, Application No. 8307/78, 21 *Decisions and Reports of the European Commission of Human Rights*, pp.116-125.

[365] *Marckx v Belgiu*m, 1979, Application No. 6833/74, ibid.

[366] Bygrave, Lee A (1998), 'Data protection pursuant to the right to privacy in human rights treaties', *International Journal of Law and Information Technology,* 6 (3), 247-84.

[367] The Charter of Fundamental Rights of the European Union, drafted by the European Convention, enshrines certain political, social, and economic rights for the citizens and residents of the EU member countries. It was 'solemnly proclaimed' by the European Parliament, the Council of European Union, and the European Commission in December 2000. The Charter's uncertain legal status ended with the entry into force of the Treaty of Lisbon on 1 December 2009. It consists of 54 articles and only applies to EU member states when they are implementing EU law.

> Everyone has the right to respect for his or her private and family life, home and communications. (Art. 7)
>
> Everyone has the right to the protection of personal data concerning him or her.
>
> Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> Compliance with these rules shall be subject to control by an independent authority. (Art. 8)

The above provisions are maintained by the Treaty of Lisbon.[368] The Convention places a restriction on the processing of personal data by indicating the need to ensure that the manner and purpose of the data processing are fair and specified. It also mentions the data subject's right to information access and rectification, as well as the need to ensure that the data are processed on the basis of the data subject's consent or the law. Art. 8 also requires the control of compliance made by an independent authority.

5.3.1.2. Two basic rights invented by the German Federal Constitutional Court

The right of privacy as a fundament human right is expressly recognized in the key international instruments and also recognized by most countries around the world. The recently-written constitutions in some countries, such as South Africa and Hungary, explicitly include specific rights

[368] The Treaty of Lisbon amended the Treaty on the European Union and the Treaty establishing the European Community, signed at Lisbon on 13 December 2007 and came into force on 1 December 2009.

to personal data protection[369] and the right to access these.[370]

In 1983 and 2008, the German Federal Constitutional Court created two important basic rights – the right to informational self-determination and the right to the confidentiality and integrity of information technology systems, which have been regarded as significant landmarks in the history of data protection in Germany.

Right to information self-determination

In 1983, the German federal government planned to conduct a general population census based on the Population Census Act which had been passed in the previous year. However, this led to a fierce public debate, resulting in the filing of a lawsuit at the Federal Constitutional Court due to a fear of government surveillance and unjust invasion of privacy caused by a statistical census. In the same year, the Court decided that the foregoing Act was partially unconstitutional and ruled, on the basis of Art. 1 (human dignity) and Art. 2 (personality right) of the Basic Law of the Federal Public of Germany, (GG) that:[371][372]

> the basis right warrants […] the capacity of the individual to determine in principle the disclosure and use of his/her personal data.

A "right to informational self-determination" was understood by the Court as:

[369] The Constitution of Hungary 2011, Freedom and Responsibility Article IV (2).

[370] The Constitution of Hungary 2011, Freedom and Responsibility Article IV (2); the Constitution of the Republic of South Africa 1996, Section 32(1).

[371] BVerfGE 65, 1; "Volkszählungsurteil" 1983.

[372] Rouvroy, Antoinette and Poullet, Yves (2009), 'The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy', in Serge Gutwirth, et al. (eds.), *Reinventing Data Protection?* (Springer), 45-76.

> *the authority of individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others.*

The reasoning of the Court was based on ideas from the sociological system theory, particularly the work of Niklas Luhmann, who considers that the function of fundamental rights is to guard the demarcation lines between societal sub-systems and the role of privacy is to protect the consistency and the individuality of the individual.[373]

Right to the confidentiality and integrity of information technology systems

On 27 February 2008, the Court ruled Art. 5.2 (11) of the Constitution Protection Act, passed in 2007 in the state of North Rhine-Westphalia, to be null and void.[374] This provision empowered the Constitution Protection Agency to carry out reconnaissance of the Internet and gain secret access to information technology systems (online searches). Having determined that the existing rights are inadequate to protect citizens from the threat to their personality rights, the Court established a new basic right of the confidentiality and integrity of information technology systems to close the regulatory gap.

This new fundamental right, like that to informational self-determination, is not explicitly mentioned in the Constitution but derived from the right of personality (Art. 2 GG) in conjunction with human dignity (Art. 1 GG). Art. 1 GG states that “Human dignity shall be inviolable”, which

[373] Hornung, Gerrit and Schnabel, Christoph (2009), 'Data protection in Germany I: The population census decision and the right to informational self-determination', *Computer Law & Security Review,* 25 (1), 84-88.

[374] BVerfG, NJW 2008, 822, available at: http://www.bundesverfassungsgericht.de/en/press/bvg08-022en.html.

establishes a general overriding principle in the German legal system, and is designed to provide a "stop-gap" solution once the legislation falls behind social changes.[375] In the hierarchical structure outlined by Cannataci by using the example of the 1991 Romanian constitution, legislation on data protection and the right to privacy underpin the realization of the supreme value of dignity and free development of personality.

> It appears to establish a three-tier hierarchy at the top of which one finds supreme values of dignity…and the right to unhindered development of personality. In the second tier immediately below this, one finds three constitutional provisions dedicated in information law: Art 26 tackles the right to private life, Art 30 the right to freedom of expression and Art 32 the right to access public information. These constitutional provisions establish the basis on which the third tier of ordinary legislation on data protection or media or freedom of access to public files provide the more detailed rules which exist to promote a culture in which ground rules for the access, distribution, and use of information […][376]

5.3.1.3. The right of privacy in Taiwan's Constitution

Similarly, the right of privacy is not explicitly enumerated under the Constitution of Taiwan.[377] It was first mentioned by the Justices of the Constitutional Court (hereinafter, the Justices)[378] in 1992 in the Judicial Yuan Interpretation (hereinafter, J. Y. Interpretation) No. 293, which states that Art.

[375] Abel, Wiebke and Schafer, Burkhard (2010), 'The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems–a case report on BVerfG, NJW', in V. Madhuri (ed.), *Hacking: A Legal Quandary* (Icfai University Press), 167-91.

[376] Cannataci, Joseph A. (2008), 'Lex Personalitatis & Technology-driven Law', *SCRPIT-ed,* 5 (1).

[377] The Constitution of Taiwan was announced on 1 January 1947 and adopted on 25 December of the same year.

[378] The Justice of the Constitutional Court of Taiwan, also known as the Council of Grand Justices, is an independent judicial organ that is subordinate to the Judicial Yuan. It is empowered to provide rulings primarily on the interpretation of the Constitution and the uniform interpretation of statutes and regulations. On the authority of the Justice of the Constitutional Court, see http://www.judicial.gov.tw/constitutionalcourt/en/p01_02.asp.

48 II of the Banking Act:[379]

> […] was enacted to protect bank customers' confidential information on their individual properties and to prevent banks from freely and unilaterally disclosing such information, with a view to protect the people's right of privacy.

Nevertheless, the "right of privacy" mentioned in the above interpretation was regarded merely as a legal right rather than a constitutional basic right. The nature of the right of privacy remained ambiguous until 15 December 2004, on which date the Justices expressly recognized the constitutional status of the right of privacy in J. Y. Interpretation No. 585.[380]

> The right of privacy […] is an indispensable fundamental right protected under Article 22 of the Constitution because it is necessary to preserve human dignity, individuality, and the wholeness of personality development, as well as to safeguard the freedom of private living space from interference and the freedom of self-control of personal information.

Art. 22 of the Constitution states that "*All other freedoms and rights of the people that are not detrimental to social order or public welfare shall be guaranteed under the Constitution*". In this Interpretation, the Justices not only recognized that the right of privacy is an indispensable fundamental right under the Constitution but also divided it into two dimensions: the freedom of private living and the freedom of self-control of personal information.

[379] J. Y. Interpretation No. 293, available at: http://www.judicial.gov.tw/constitutionalcourt/en/p03_01.asp?expno=293.

[380] J. Y. Interpretation No. 585, available at: http://www.judicial.gov.tw/constitutionalcourt/en/p03_01.asp?expno=585.

The Taiwanese government planned to implement new national identity cards which were to be issued in July 2005 in accordance with the 1997 Household Registration Act. Under Art. 8 II of this Act, all citizens over the age of 14 shall be fingerprinted for record keeping when applying for a new identity card. However, this programme incurred a strong question of its constitutionality and led to a 'Movement to Refuse Fingerprinting' formed by an alliance of over 100 human rights groups.[381] In June 2005, the Justices issued a temporary injunction to halt the programme. Over a three-month period, the Justices made an interpretation (J. Y. Interpretation No. 603)[382] on 28 September 2005 which ruled that Art. 8 of the 1997 Household Registration Act was inconsistent with the intent of Art. 22 and 23 of the Constitution, and thus no longer applicable.

This was a milestone in the history of personal data protection in Taiwan, as this was the first time that the Justices prohibited the continuous application of a law based on the protection of the right of privacy. They also firstly explicitly defined the right of information privacy as:

> […]the right to decide whether or not to disclose their personal information, and, if so, to what extent, at what time, in what manner and to what people such information will be disclosed.

The above understanding of the Justices with regard to the right of privacy is close to the right to information self-determination created by the German Federal Constitutional Court. In addition, both the right of information privacy and the right to informational self-determination are grounded

[381] "Taiwan Constitutional Court places fingerprinting plan on hold", *Privacy International*, 21 June 2005, at: https://www.privacyinternational.org/article/taiwan-constitutional-court-places-fingerprinting-plan-hold. [Accessed on 15 January 2012]

[382] J. Y. Interpretation No. 603, available at: http://www.judicial.gov.tw/constitutionalcourt/en/p03_01.asp?expno=603.

on the core value of human dignity and personality development. Nevertheless, the Justices further addressed that the right of privacy is also designed to guarantee:

> the right to know and control how their personal information will be used, as well as the right to correct any inaccurate entries contained in their information.

According to the Justices, the right of information privacy is not an absolute right and the State may impose appropriate restrictions on such a right by enacting explicit laws pursuant to Art. 23 of the Constitution, where it is necessary to prevent infringement upon the freedoms of other persons, to avert an imminent crisis, to maintain social order or to advance public welfare.

5.3.2. Personal data privacy frameworks

5.3.2.1. The paradigm of fair information practices

'Fair Information Practices' (FIP) were initially articulated by a US government advisory committee in the Department of Health, Education and Welfare's seminal 1973 report entitled Records, Computers and the Rights of Citizens (hereinafter, the HEW report).[383] In the HEW Report, the Advisory Committee recommended the enactment of legislation establishing a Code of Fair Information Practices for automated personal data systems and formulated five principles for safeguarding the requirements for automated personal data systems:

a. There must be no personal data record-keeping systems whose very existence is secret.
b. There must be a way for an individual to find out what information about him is contained in a

[383] For the full text of the HEW Report, see http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

record and how it is used.

c. There must be a way for an individual to prevent information about himself that was obtained for one purpose from being used or made available for other purposes without his consent.

d. There must be a way for an individual to correct or amend a record of identifiable information about himself.

e. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent their misuse.

The FIP essentially lies in Professor Alan Westin's work on the "criteria for weighing conflicting interests".[384] Since its origin in 1973, the FIP has become the dominant US approach to information privacy protection[385] and has been widely incorporated into the national data protection laws of other countries as well as international data privacy initiatives.

5.3.2.2. Development of international personal data privacy frameworks

The first law that expressly protected information privacy was passed in Europe in the early 1970s. The West German state of Hesse enacted the first data protection statute, the Data Protection Act (Datenschutzgesetz), in 1970. Sweden followed in 1973 with the Data Act, which was the first legislation about data protection at the national level. On 27 January 1977, West Germany introduced a comprehensive data protection legislation – the Federal Data Protection Act – for both the public and private sectors which created an independent Data Protection Commissioner (DPC) who is responsible for ensuring that the Data Protection Act is implemented by advising the Federal government and individual ministers.[386] France followed in the late 1970s by introducing

[384] These were included in chapter 14, 'Restoring the Balance of Privacy in America' in Westin (1970), op. cit.

[385] --- (2003), 'Social and political dimensions of privacy', *Journal of social issues,* 59 (2), 431-53.

[386] Flaherty, David H (1992), *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden,*

legislation relating to personal data and computer files with law Nr. 79-17 of 6 January 1978.

However, inconsistencies among the regulatory regimes in European countries caused concern that it might become a restraint on trade. To address this risk, significant progress in data protection has been made by establishing the basic privacy principles provided by international privacy guidelines since the 1970s. Over the last three decades, countries have begun adopting comprehensive privacy laws which tend to be based on the framework set out by the Organization for Economic Cooperation and Development (OECD),[387] the Council of Europe (CoE),[388] and the European Union (EU).[389]

The 1980 OECD Privacy Guidelines

The OECD's work on privacy and transborder data flows began in the early 1970s. Whereas free flows of personal information make a significant contribution to social and economic development, they also inspired increasing concern about the protection of privacy. While recognizing disparities in the national legislation that created a hindrance to the free flow of personal data between countries, the OECD determined to develop guidelines to harmonize the national privacy legislation which could uphold the fundamental right of privacy and diminish restrictions in the international data flows at the same time.

The *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal*

France, Canada, and the United States (UNC Press Books).

[387] The OECD, constituted of 34 countries, is a forum of countries committed to democracy and the market economy, providing a platform to compare policy experiences, seek answers to common problems, identify good practices, and coordinate the domestic and international policies of its members.

[388] The CoE, founded in 1949, is an international organization promoting co-operation between all of the countries of Europe with regard to legal standards, human rights, democratic development, the rule of law and cultural co-operation.

[389] The EU is an economic and political union that was formally established when the Maastricht Treaty came into force on 1 November 1993. The EU, constituted of 27 member states, has developed a single market through a standardized system of laws which apply in all member states.

Data (hereinafter, the OECD Guidelines),[390] adopted on 23 September 1980, were the first internationally agreed statement of the core information privacy principles. The OECD Guidelines, accompanied by an Explanatory Memorandum which provides information on the formulation of guidelines, embraces eight basic privacy principles in Part Two: the limitation of collection and use, data quality, purpose specification, security safeguards, openness, individual participation, and the accountability of the data controllers.

The CoE's 1981 Convention

The OECD's work was carried out in close co-operation with the CoE. The Committee of Ministers of the CoE adopted two resolutions on data protection concerning electronic data banks in the private[391] and public sector[392] in 1973 and 1974. Both resolutions listed a number of basic rules relating to the obtaining of data, the quality of data, and the rights of individuals to be informed about data and data processing activities, recommending that the governments of the member states should take steps to give effect to the above principles when personal information is stored in electronic data banks.

The Committee of Ministers adopted the *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* (hereinafter, the CoE's 1981 Convention or simply the Convention)[393] grounded on the foregoing two resolutions on 17 September 1980 and opened for signature by the member states of the CoE on 28 January 1981. The Convention laid down the core principles of data protection in Chapter II, which included the quality of the data in terms of its

[390] For the full text of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, see: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part1.

[391] Resolution 73 (22)

[392] Resolution 74 (29)

[393] For the full text of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, see: http://conventions.coe.int/Treaty/en/Treaties/html/108.htm.

collection, processing, storage, and usage (Art. 5), special categories of data (Art. 6), the requirement for data security measures (Art. 7), and the right of data subjects to access their data (Art. 8).

The EU Directive 1995

The shift of the European Union from an economic to a broad-based political union brought it with an urgent need to ensure the uniform protection of information privacy. Nevertheless, the OECD Guidelines are not legally binding and permit broad variation in their national implementation.[394] The CoE's Convention will have legal force in those countries which ratify it; however, it also permits broad variance across various national regimes. As a result of the uneven application of and prevalent variation among national laws, in July 1990, the European Commission[395] published a draft *Council Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data* which was amended by the European Parliament[396] in March 1992 and eventually adopted on 24 October 1995 (with effect from October 1998).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (hereinafter, the EU Directive 1995)[397] is another milestone in the global initiative regarding the protection of personal data. It established a Europe-wide set of legal principles for privacy protection and represented the international consensus on the content of data protection rights. Most importantly, due to the prohibition of the transfer of personal data from member

[394] OECD Guidelines para. 45 expressly "permit Member countries to exercise their discretion with respect to the degree of stringency with which the Guidelines are to be implemented".

[395] The European Commission is the executive body of the European Union which proposes legislation, and oversees and implements decisions and the requirements of the EU treaties.

[396] The European Parliament is the legislative body of the European Union, composed of 754 members, who are elected through direct voting.

[397] For the full text of the EU Directive 1995, see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT.

countries to other countries that lack an “adequate level of protection”,[398] the EU Directive 1995 exerts significant international pressure for increased data protection on countries outside Europe, including the countries in the Asia-Pacific region.[399]

The EU Data Regulation 2012

Rapid technological development and globalization have significantly changed the way and scale how data is collected, processed and used. In addition, the divergence in the implementation of the EU Directive 1995 among the 27 EU Member States has led to an uneven level of protection for personal data accompanied with erosion of the consumer confidence with online activity. In May 2009, the European Commission launched a review of the current legal framework for data protection, starting with a high-level conference and a public consultation that run until the end of 2009. On 25 January 2012, a proposal for a General Data Protection Regulation *(*a *regulation of the European Parliament and of the Council on the Protection of Individuals with regard* to *the Processing of Personal Data and on the Free Movement of such Data)* was published to set out new rules on the processing of personal data (hereinafter, the EU Data Regulation 2012).[400]

To strengthen the online privacy rights, the above proposed regulation provides the data subject’s right to be forgotten and erasure, which enables the data subjects to request erasure of personal data relating to them when they no longer want their data to be processed or there are no legitimate grounds for retaining it (Art. 17). It also introduces the data subject’s right to data portability to

[398] EU Directive 1995, Art. 25 (1). The Directive provides that the adequacy of the protection afforded by the transferee country “shall be assess in the light of all the circumstances surrounding a data transfer”, including “the nature of the data, the purpose and duration of the proposed processing”, “the rules of law, both general and sectoral,” in the transferee country, and the “professional rules and security measures which are compiled in that country” (Art. 25 (2)).

[399] Fischer-Hübner, Simone (1998), 'Privacy and security at risk in the global information society', *Information Communication & Society,* 1 (4), 420-41.

[400] For the full text of the Proposed Directive 2012, see: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

transfer data from one service provider to another without being prevented by the controllers (Art. 18). Data subject’s consent for data processing should be given explicitly pursuant to the Regulation (Art. 4 (8)). In a case of a personal data breach, the controller is obligated to notify the data breach to the supervisory authority without undue delay, where feasible within 24 hours (Art. 31.1). Where the data breach could adversely affect the data subject, the controller is also required to inform the data subject about the data breach without undue delay (Art. 32.1).

The APEC Privacy Principles

In order to promote electronic commerce and to ensure the free flow of information within the APEC started its work on developing a consistent approach to information privacy protection among APEC members while avoiding unnecessary barriers to information flow in 1995.[401] It established the APEC Electronic Commerce Steering Group (ECSG) in 1999 and has tended towards developing a regional privacy instrument since 2002. At a meeting held in Thailand in February 2003, the APEC ECSG set up the APEC Data Privacy Subgroup[402] to develop a common APEC approach to privacy. At this meeting, Australia proposed the development of APEC privacy principles by taking the OECD Privacy Principles as a starting point was coupled with an implementation mechanism which addresses the issue of inter-country personal data transfer. The proposal, developed by the Data Privacy Subgroup, was renamed the APEC Privacy Framework[403] and endorsed by APEC Ministers at a meeting held in Santiago, Chile, in November 2004.

[401] Lam, Tony (2005), 'An Overview of the Principles Established by the APEC Privacy Framework', *APEC Technical Assistance Seminar: Domestic Implementation*. <https://www.pcpd.org.hk/english/files/infocentre/1tonylam1_ppt.pdf>, accessed September 27 2014.

[402] The APEC Data Privacy Subgroup meets twice yearly and reports to the ECSG, which ultimately reports to the APEC Ministers. It comprises eleven members: Australia, Canada, China, Chinese Taipei (Taiwan), Hong Kong, Japan, Korea, Malaysia, New Zealand, Thailand and the United States.

[403] The full text of the APEC Privacy Framework is available at: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

The APEC Framework, for the purpose of promoting electronic commerce and ensuring the free flow of information within the APEC region, sought to establish a consistent approach to information privacy protection among APEC members while avoiding the creation of unnecessary barriers to information flows. The Framework set forth nine APEC privacy principles (I-IX)[404] in Part III, which deal with most of the broad topics laid down in the international or national sets of privacy principles, including the collection, quality, security, use, access to, and correction of personal information.

The APEC Privacy Principles (hereinafter, the APEC IPPs) were rooted in the OECD Guidelines with the addition of two further principles: 'Preventing harm'[405] and 'Choice'.[406] Nevertheless, they did not include the OCED Guidelines concerning purpose specification[407] and openness.[408] Although the APEC IPPs have been criticized for the weakness inherent in the OECD Guidelines,[409] as well as their minor enhancement of the OECD Guidelines that were set up more than twenty years ago,[410] they are generally recognized to be the most significant international privacy instrument since the EU Directive 1995.

[404] The nine APEC Privacy Principles are: Preventing Harm, Notice, Collection Limitation, Use of Personal Information, Choice, Integrity of Personal Information, Security Safeguards, Access and Correction, and Accountability.

[405] The principle of Preventing Harm recognizes that privacy protection should be designed to prevent harm to individuals through the wrongful collection or misuse of their personal information and that the remedy to privacy invasions should be proportionate to the likelihood and severity of the risk of harm. APEC Privacy Framework, Part III at para. 14.

[406] The principle of Choice recognizes that individuals should be provided with mechanisms to exercise choice in relation to the collection, use and disclosure of their information. APEC Privacy Framework, Part III at para. 20.

[407] The Purpose Specification Principle provides that the purposes for which personal data are collected should be specified no later than the time of the data collection. The OECD Guidelines, Part Two, para. 9.

[408] The Openness Principle requires a general policy of openness about the developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. The OECD Guidelines, Part Two, para. 12.

[409] Clarke enumerated the inadequacy of the OECD Guidelines in several aspects, which mainly included: 1. they failed to provide a specialist privacy protection body which is able to supervise government agencies and corporations; 2. they fell short of the protection of the free exercise of the right of privacy without a fear of disadvantage; and 3. they should be enhanced following the development of privacy-invasive technology in order to reflect the need for protection. Clarke (2000), op. cit.

[410] Greenleaf, Graham (2005), 'APEC's privacy framework sets a new low standard for the Asia–Pacific', in Andrew T. Kenyon and Megan Richardson (eds.), *New dimensions in privacy law: international and comparative perspectives* (Cambridge: Cambridge University Press).

APEC is the only inter-governmental grouping and places no treaty obligation on its member economies. Decisions made within APEC are undertaken on a voluntary basis. The APEC Framework does not require any particular means of implementation but only lists several options, including "legislative, administrative, industry self-regulatory or a combination of these methods".[411] It also accepts "a flexible manner that can accommodate various methods of implementation, including through central authorities, multi-agency enforcement bodies, a network of designated industry, or a combination of the above".[412]

5.3.3. The personal data protection law of Taiwan

Taiwan initiated the legislation work regarding personal data protection in the 1980s and adopted the CPPDP Law which was built upon the OECD Guidelines in August 1995. However, as we saw in Chapter 4 (section 4.3.4), this Law failed to provide effective regulation of the collection of personal information nor adequate protection for personal information, which prompted the new enactment of the PIP Act in 2010.

The personal data protection frameworks established in the OECD Guidelines, the CoE's Convention, and the EU Directive, as aforementioned, have provided the most prevalent examples of privacy frameworks and serve as the foundation for many countries, including both member and non-member states around the world, for tailoring or establishing national data protection laws. The APEC IPPs, which are essentially rooted in the OECD Guidelines, have also afforded the criteria of data protection for its member countries. As a member of the APEC, the enactment of the PIP Act not only incorporated several data protection principles set up in the EU Directive but also

[411] The APEC Framework, Part IV, Section A. Guidance for Domestic Implementation, para. 31.
[412] Ibid.

especially adopted the APEC IPPs, particularly the principle of ‘Preventing Harm’, ‘Collection Limitation’ and ‘Notice’.[413]

This section examines the interaction of the data protection legal frameworks between different levels, including global, regional, and Taiwan, by providing an outline of the key amendments of the PIP Act in comparison with the international frameworks and an analysis of the impacts that the EU Directive and the APEC IPPs have produced upon the development of Taiwan’s legislation.

5.3.3.1. Key aspects of the amendment

Scope of application

In tune with the OECD Guidelines and the APEC IPPs, the PIP Act removes the constraint laid down in the CPPDP Law and extends the scope of its application to cover non-computer-processed data (Art. 1). Hence, it is valid for general data, irrespective of the particular methods and machinery employed. The PIP Act also breaks downs the sectoral boundaries and expands the scope of non-government agencies to “natural personal, juridical persons or groups other than government agencies.” (Art. 2 (8))

Definition of personal information

Standing in the point of the EU Directive with regard to the definition of personal data,[414] the definition of personal information given in the PIP Act covers “the information which may be used

[413] MOJ (2010), 'The Passing of the Personal Information Protection Act after Three-reading Procedure of the Legislative Yuan', (The Department of Legal Affairs of the Ministry of Justice, Taiwan).

[414] Art. 2a “personal data” shall mean any information relating to an identified or identifiable nature person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, particularly by reference to an identification number or to one or more factor specific to his physical, physiological, mental, economic, cultural or social identity.

to identify a natural person, both directly and indirectly." (Art. 2(1)) Unlike the Directive, the PIP Act enumerates several types of personal information that is capable of identifying an individual in either a direct or indirect way, including his name, date of birth, I.D. card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical records, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, and social activities.

Security Measures

The privacy of personal information should be underpinned by appropriate security safeguards against accidental or unlawful destruction or loss, authorized access or disclosure or alternation. Based on the division drawn by the OECD Guidelines,[415] security measures can categorized into three types: physical measures, such as locked doors and identification cards, organizational measures, such as authority levels with regard to access to data and obligations for data processing personnel to maintain confidentiality, and technical measures, such as the detection or monitoring of unusual activities and responses to threat. The EU Directive particularly requires the confidentiality of processing that the processor or any person who has access to personal data authorized by the controller or processor is prohibited to process data unless the processing is under the instruction from the controller (Art. 16).

In addition, appropriate security measures should be guaranteed not by the controller but also by the processor who acts on behalf of the controller. The EU Directive stresses the need for the controller to ensure that the data processing carried out by the processor is governed by sufficient technical and organizational security measures and compliance with those measures (Art. 17.2). The level of

[415] The Explanatory Memorandum of the OECD Guidelines, Part II, para. 56.

security measures, according to both the EU Directive (Art. 17.1) and the APEC IPPs,[416] shall be proportional to the likelihood and severity of the harm threatened and the sensitivity and nature of the information to be protected.

In order to protect personal data from being stolen, altered, damaged, destructed or disclosed, the PIP Act provides that a government agency should assign specific personnel[417] to deal with matters regarding the security and maintenance measures of personal information files (Art. 18) and a non-government agency should take proper security measures (Art. 27.1). The central government authority responsible for the subject sector may designate a non-government agency to establish the plan for the security measures for the personal information files (Art. 27.2).

The proper security measures referred to in the PIP Act, according to its Enforcement Rules, are necessary technical and organizational measures to prevent personal data from being stolen, altered, damaged, destroyed or disclosed (Art. 12.1). Notably, the Ministry of Justice (MOJ) adopts the PDCA (Plan-Do-Check-Act) cycle for the management of information security and lists several necessary measures, as indicated in the diagram below (Art. 12.2).

[416] APEC Privacy Framework, Part III at para. 22.

[417] The specific personnel, under the Enforcement Rules of the PIP Act, mean the people who have professional ability to manage and maintain personal information files and are capable to perform the regular task of securing and maintaining personal information for the agency (Art. 25.1).

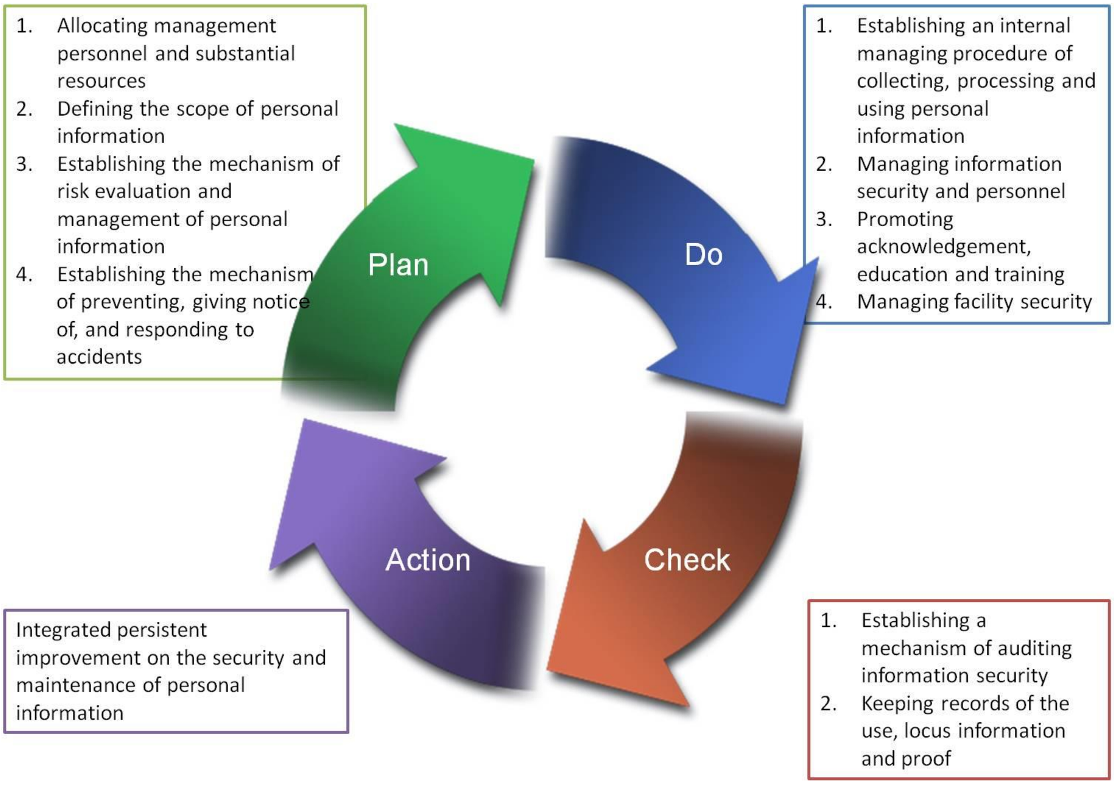

1. Allocating management personnel and substantial resources
2. Defining the scope of personal information
3. Establishing the mechanism of risk evaluation and management of personal information
4. Establishing the mechanism of preventing, giving notice of, and responding to accidents
Plan
Do
1. Establishing an internal managing procedure of collecting, processing and using personal information
2. Managing information security and personnel
3. Promoting acknowledgement, education and training
4. Managing facility security
Action
Check
Integrated persistent improvement on the security and maintenance of personal information
1. Establishing a mechanism of auditing information security
2. Keeping records of the use, locus information and proof

Diagram 5.2: PDCA (Plan-Do-Check-Act) Cycle

Liability of controllers

Under the CPPDP Law, a controller who violates the protection of personal data against unlawful and unauthorized collection (Art. 18) is only punishable if the controller intends to make profit by doing so and this wrongdoing has caused injury to an individual (Art. 33). The PIP Act increases liability on a controller by providing punishment to a violation of the prohibitions of personal data collection (Art. 15, 19) if this violation may result in injury to an individual regardless of the intention of the controller (Art. 41).[418]

Where personal information has been illegally collected, processed, and used due to the

[418] A violation of the prohibitions of personal data collection (Art. 15, 19) which may result in injury to an individual should be imposed of a sentence or custody of no more than 2 years, or a fine of no more than NTD 200,000 (around US$ 6,666), or both (Art. 41.1). A person who intends to make profit by unlawful or unauthorized collection of personal data which may cause injury to an individual should be imposed of a sentence of no more than 5 years and a fine of no more than NTD 1,000,000 (around US$ 33,333) (Art. 41.2).

non-compliance of the controllers with the PIP Act, the controllers should be liable for compensation for both the property and non-property damage incurred by the said illegal collection, processing and usage of the personal information (Art. 28, 29). A government agency can exempt from damages only if the illegal collection is caused by a natural disaster, incident or other *force majeure* (Art. 28.1). The liability is inapplicable to a non-government agency if it can prove itself to be unintentional or non-negligent (Art. 29.1).

By contrast to the CPPDP Law, the PIP Act increases the total amount of compensation ten-fold with regard to damages caused to multi data subjects by the same cause and fact, which should not exceed NTD 200 million. However, if the interests involved are over NTD 200 million, the amount of compensation should be set according to the interests (Art. 28.4, 29.1).

The increase of liability and huge amount of compensation for damages has led to extreme anxiety among both the government and non-government agencies. The enterprises have been trying to force the MOJ to support their interests by lessening the liability of the controllers and delay the enforcement date of the PIP Act. In a meeting held by the Executive Yuan on 17 February 2012, the MOJ agreed to partially suspend provisions of the PIP Act including those relating to criminal liability of controllers with regard to unauthorized collection, processing or use of personal data (Art. 41).[419] Although Art. 41 was eventually put into force in October 2012, the MOJ has finalized its draft to re-amend to this article by decriminalizing violation committed not for profit (Art. 41.1).

5.3.3.2. The practice of the international data protection principles at the national level in Taiwan

Table 5.1 and 5.2 below indicates how and to what extent the data protection principles[420]

[419] Huang, Yan-Fen (2012), 'The proposed suspension of the controversial provisions of the PIP Act', *iThome*. <http://www.ithome.com.tw/node/72444>, accessed September 7 2014.

[420] Given the theme of this research, I do not intend to examine the principles in detail but rather focus on the

established in the EU Directive and the APEC IPPs have been embodied in the PIP Act, together with the comments of this author.

principles or provisions related to the unauthorized collection of or access to personal data.

Table 5.1: The EU Directive and the PIP Act

EU Directive 1995	The PIP Act	Comments
Prohibition of the Processing of Special Categories of Data 1. The scope of special categories of data (Art. 8.1) a. Racial or ethnic origin b. Political opinions c. Religious or philosophical beliefs d. Trade-union membership e. Data concerning health or sex life 2. Exemptions a. The data subject's explicit consent if there is no prohibition stipulated by law (Art. 8.2a) b. Processing is necessary for carrying out the obligations and specific rights of the controller	Prohibition of the Collection, Processing, and Use of Special Categories of Data 1. The scope of special categories of data (Art. 6) a. Medical treatment b. Genetic information c. Sexual life d. Health examination e. Criminal record 2. Exemption a. It is stipulated by law (Art. 6.1a) b. It is necessary for the government agency to perform its duties or for a non-government agency to fulfill its legal obligation (Art. 6.1b) c. The information has been disclosed by the data	1. While the term 'processing' referred to in the EU Directive means any operation performed upon personal data including their collection and use (Art. 2.b), the PIP Act deals with these three operations, i.e. collection, processing, and use, separately (Art. 2.4-2.6). However, the Act places a limitation on the definition of 'processing' by requiring the purpose of establishing or using a personal data file, which appears redundant and is unhelpful for defining the contents. 2. The five categories of special data listed in the PIP Act are primarily derived from the data concerning body, health or sex life, and no

EU Directive 1995	The PIP Act	Comments
d. Processing is carried out by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and the processing relates solely to the members of the body or to persons who have regular contact with it. (Art. 8.2d) e. Publicly available data disclosed by the data subject (Art. 8.2e) f. Processing is necessary for the establishment, exercise or defence of legal claims (Art. 8.2e) g. Processing is required for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and those data are processed by a health	The rules of the range, procedure and any other items concerning the collection, processing, and use under Art. 6.1d should be set up by the central government authority responsible for the subject sector in conjunction with the Ministry of Justice. (Art. 6.2)	3. The data subject's consent is not included in the exemptions from the prohibition of use, processing and collection of special personal data. The data subject's consent should be the most crucial and requisite requirement that needs to be met before any collection, use or processing can be operated on his/her data based on the right of information privacy. Data subjects can freely decide whether or not and to what extent they disclose their personal information. It is inappropriate to override the data subject's intention especially in the case of the collection, use, and processing of special categories of data where there is lack of explanation concerning this point in the Explanatory

EU Directive 1995	The PIP Act	Comments
Notice of Data Collection 1. Direct collection (data is collected from the data subject) (Art. 10): The controller must provide the data subject with at least the following information – a. The identity of the controller and of his representative; b. The purpose of the processing; c. Any further information such as: ● The recipients or categories of recipients of the data, ● Whether replies to the questions are obligatory or voluntary, and the possible	Notice of Data Collection 1. Direct collection (Art. 8.1): The government and non-government agency should explicitly notify the data subject of the following information – a. The name of the collector; b. The purpose of the collection; c. The categories of information; d. The duration, area, target and method adopted concerning the use of the information; e. The rights of the data subject to his personal information pursuant to Art. 3;[422] and f. The influence on his rights and interests where	1. The EU Directive states that the information enumerated in Art. 10 is only of the minimum standard,[421] while the PIP Act does not indicate such a requirement. 2. The PIP Act only requires the controller to make notice in the case of direct and indirect collection, not covering disclosure to a third-party.

[421] Under Art. 10 of the EU Directive, the controller shall provide further information where "it is necessary with regard to the specific circumstances to guarantee fair processing."

[422] Art. 3 provides data subjects' right of review, duplication, supplement, correction and deletion of their personal information and the right of discontinuing the collection, processing or use of that information.

EU Directive 1995	The PIP Act	Comments
2. Indirect collection or disclosure to a third-party (data are not obtained from the data subject or the disclosure of data to a third party is envisaged) (Art. 11.1): The controller must give the data subject nearly identical information provided under Art. 10 at the time of undertaking the recording of personal data or no later than the time when the data are first disclosed to a third-party. 3. Exemptions: a. Where the data subject already has this information in the cases of direct and indirect collection and disclosure. b. In the case of indirect collection and	2. Indirect collection (Art. 9.1): The agency should notify the data subject of the source of data along with the information listed in Art. 8.1 (a-e, see above) before processing or using the data. 3. Exemptions: In the case of direct collection (Art. 8.2) where a. The data subject has known this information b. It is in accordance with the law c. The collection is necessary for the government agency to perform its official duty or for the non-government agency to fulfill its legal obligation d. The notice will impair the government	3. In the case of indirect collection, the EU Directive obligates the controller to provide information to the data subject at the time of 'undertaking the recording' of the data, whereas the PIP Act requires that notification should be made 'before processing or using the data'. A data subject should be kept informed at or prior to the time of recording rather than at the time of use. The PIP Act causes an inappropriate postponement to the notice time which involves the inadequate protection of the data subjects and demands proper revision. 4. While the PIP Act places an obligation of

[423] This will be further addressed in the next section.

EU Directive 1995	The PIP Act	Comments
● It is for processing for statistical or historical purposes or for scientific research ● The provision of such information proves impossible or would involve a disproportionate effort	e. The information has been disclosed by the data subject or has been publicized legally f. The notification cannot be made to the data subject or his representative g. It is necessary for the public interest for statistics or academic research but only where the information cannot be used to identify an individual The information is collected by mass communicators for reporting purposes based on the public interest.	

Table 5.2: The APEC IPPs and the PIP Act

APEC IPPs	The PIP Act	Comments
Preventing Harm – This recognizes that privacy protection should be designed to prevent harm to individuals through the wrongful collection or misuse of their personal information and that the remedies to privacy invasions are proportionate to the likelihood and severity of the risk of harm.	The collection, processing, and use of personal information should respect the rights and interests of the data subjects and should be performed in an honest, trustworthy manner (Art. 5). The use of personal information by a government agency should only be operated within its statutory duty where necessary and should be consistent with the specific purpose of the collection (Art. 16) The use of personal information by a non-government agency should only be operated where it is necessary for the	This principle is more like a general privacy protection declaration, as it does not create rights in individuals nor imposes obligations on information controllers. It is hence regarded as 'bizarre' to raise it to the status of a privacy principle.[424]

[424] Greenleaf (2005), op. cit.

APEC IPPs	The PIP Act	Comments
Collection Limitation – This provides for the lawful and fair collection of personal information that is relevant to the purposes of collection, and where appropriate, with notice to, or consent of, the individual concerned.	Art. 5 requires that the collection of personal information should be honest and trustworthy and the collection should be fairly and reasonably relevant to the purposes of the collection. Information controllers should provide the data subject with the necessary information regarding the collection (Art. 8.1, 9.1).	Whether the relevance between the collection and the purpose is fair and reasonable should be recognized in a strict manner. The collection should be directly-related to the purpose specified no later than the time of the collection and should be objectively limited where necessary to the function and activities of the agencies which undertake the collection. In addition, a process should be established to enable the data subjects to reject the justification where appropriate.

APEC IPPs	The PIP Act	Comments
Choices – This recognizes that, where appropriate, individuals should be provided with mechanisms for exercising choice in relation to the collection, use and disclosure of their information.	A non-government agency should stop its marketing action using personal information once the data subject refuses this (Art. 20.2) A data subject should be provided with information regarding how to object to the first marketing action and the agency should pay any fees incurred (Art. 20.3).	The PIP Act adopts this principle and offers data subjects a mechanism for exercising choice in relation to the usage of their information for marketing purposes. Art. 14.b of the EU Directive 1995 has also been taken as a precedent.

5.4. Challenges to the Personal Information Protection Act

Having incorporated the data protection principles established at the global and regional levels, Taiwan attempts to provide an overarching law for regulating the operations of personal data in tune with international standards. This section aims to investigate whether the primary data protection law of Taiwan, i.e. the PIP Act, is capable of providing adequate and effective protection for personal information especially in respect of prohibition of unauthorized access or collection, strengthening data controllers' safeguard of database, and enhancement of data subjects' control over their personal data which are particularly important to the regulation of phishing or it may bring reverse-effect on the protection of individuals against phishing.

5.4.1. Obscure orientation of the PIP Act

According to Art. 1, the PIP Act was enacted to regulate the collection, processing and use of personal information in order to prevent the infringement of the right of personality and to enhance the proper utilization of personal information. Therefore, the regulations are expected to accelerate the utilization of personal information and prevent violations of the right of personality at the same time.

The enactment purpose of the PIP Act basically inherits the CPPDP Law with only a slight change of wording. Although the PIP Act was intended to protect personal information, it did not mention any about the protection of right to information privacy. This may be understandable in the CPPDP Law, as the right of privacy remained of uncertain legal status in the 1990s; however, it is questionable why the PIP Act enacted in 2010 bypasses the right of information privacy since such a right has been expressly perceived as a constitutional right by the Justices of the Constitutional

Court since 2003.

The obscure enactment purpose of this Act revealed the intention of the lawmakers to evade creating a balance between two interests – the interests of the data subjects with respect to their information privacy and the interests of the controllers regarding the collection, processing, and use of personal data. While this Act which was supposedly constructed upon a privacy-protection regime should prioritize the protection of information privacy, it actually refused to engage in direct involvement in the right of information privacy. The obscure orientation of this Act makes itself in an awkward regulatory position in the protection of personal information.

5.4.2. The blurred line between identifiable and de-identifiable information

Whereas there is less argument about the distinction between personal, directly identifiable information (PDI information) – e.g. name, I.D. card number, passport number – and personal, indirectly identifiable information (PII information), a fierce debate has been inspired in both the public and private sectors in Taiwan regarding the line between PII information and other de-identifiable information (non-PII information) since the PIP Act was passed. According to Art. 3 of the Enforcement Rules of the PIP Act, PII information refers to information which cannot be used solely to identify an individual, and it can be ascertained only through comparing to, combining with or connecting to other information.

In fact, the distinction between de-identifiable or supposedly anonymous information and identifiable information in either a direct or indirect way has gradually become blurred due to several factors. The widespread availability of publicly available information may contribute to the erosion of this dichotomy. In addition, piecemeal anonymous consumer data can be combined by businesses into profiles that can be linked to a specific person in order to carry out comprehensive data collection.[425] Technological advance may also be an important factor that helps to blur the line between de-identifiable and identifiable information. For example, the utilization of 'browser fingerprinting' technology can gather and combine innocuous data about a consumer's web browser, such as browser plug-ins[426] and fonts and the type of operating system used uniquely to identify and track the consumer.[427]

The increasing ease with which data can be linked to specific individuals has been accompanied by the decreasing significance of distinguishing 'identifiable information' from 'de-identifiable information'. The constraint on the scope of personal information also leaves an unregulated circumstance in which the information is sensitive to a person but may not be linked to him. The context of personal information should be broadly recognized and not subject to discrimination based on whether or not it can be used to identify a person. All sensitive data associated with a person should be appropriately protected.

5.4.3. The unnecessary burden on data subjects of protecting their data quality

Data quality, which requires that personal information should be accurate, complete, and kept up-to-date to the extent necessary for the purpose of use, is one of the fundamental principles set forth in both the OECD Guidelines[428] and the EU Directive 1995.[429] It is also enshrined in the APEC Framework in the Principle of Integrity of Personal Information.[430] The EU Directive further addresses the need for controllers to ensure that personal data which are inaccurate or

[425] Barbaro, Michael, Zeller, Tom, and Hansell, Saul (2006), 'A face is exposed for AOL searcher no. 4417749', *New York Times*.

[426] A plug-in is a set of software components used in web browsers to enhance the functionality of an application. Well-known examples of plug-ins include Adobe Flash Player, QuickTime, and Microsoft Office.

[427] Larkin, Erik (2010), 'Browser Fingerprints: A Big Privacy Threat', *PCWorld*. <http://www.pcworld.com/article/192648/browser_fingerprints_a_big_privacy_threat.html>, accessed September 16 2014.

[428] The OECD Guidelines, Part Two, para.8.

[429] The EU Directive 1995, Art. 6.

[430] APEC Privacy Framework, Part III at para. 21.

incomplete are either erased or rectified (Art. 6.1(d)).

Although the principle of data quality is composed of the elements of accuracy, completeness, and up-to-dateness, the PIP Act only lays special emphasis on the protection of data accuracy. Art. 11 of the PIP Act provides that both government and non-government agencies should ensure the accuracy of personal information, and make corrections to or supplement personal information either ex officio or upon the request of the data subject (Art. 11.1). In principle, the agency should, ex officio or upon the request of the data subject, delete or discontinue the processing or use of personal information when the specific purpose of its collection no longer exists or has expired over time (Art. 11.3).[431]

The Enforcement Rules of the CPPDP Law put an obligation on the data subjects to provide an "explanatory description supported by sufficient proof" when they request correction of or supplementation to their personal information (Art. 25). This is destructive to the legislation system as the Enforcement Rules, which should be supplementary to the Act, are not allowed to exceed the Act and place additional obligations on either the data controllers or the data subjects. More importantly, it reflects the lawmakers' bias in favour of the controllers, as this provision unfairly shifts the responsibility of the data controllers for ensuring the data accuracy to the data subjects by placing an unnecessary burden on the latter. This provision, disappointingly but unsurprisingly, is retained in the Enforcement Rules of the PIP Act. The MOJ only changes the phrase "explanatory description supported by sufficient proof" to "appropriate explanatory description" (Art. 19).

5.4.4. Lack of privacy protection authorities

[431] Art. 11.3 is inapplicable if the processing or use of personal information is necessary for the performance of an official duty or fulfillment of a legal obligation, or it has been agreed by the data subject in writing. See the proviso of Art. 11.3 of the PIP Act.

Where a violation of the PIP Act has resulted in personal information being stolen, disclosed, altered or infringed in other forms, Art. 12 obligates the controller to notify the data subjects in an appropriate way after ascertainment. By using Sec. 42a of the German Federal Data Protection Act (hereinafter, the German FDP Act) as a precedent, the MOJ adds a new article to the enforcement rules (Art. 22) which provides information with respect to the methods and content of the notification.

The data subjects shall be informed in writing, by telephone, text message, email, fax, electronic record, or in other ways that may be able to reach them. Where notifying the data subjects would require a disproportionate cost, such notification may be replaced by the Internet, news items or other effective measures which can make the issue known to the public, if appropriate to the technical feasibility and the privacy protection of the data subjects (Art. 22.1).

In addition to the notification of the data subject regarding the nature of the unlawful disclosure and recommended measures to minimize possible harm, the German FDP Act also requires the private data controller to notify a competent supervisory authority[432] of the nature of the infringement, and recommend measures to minimize the possible harm, the possible harmful consequences and the measures taken as a result (Sec. 42a). By contrast, the PIP Act only requires both the government and non-government agencies to notify the data subject of the nature of the infringement and the responding measures that have been taken by the controller (Art. 22.2).

Under the FDP Act, the supervisory authority shall be authorized to notify the data subjects, and to report the violation to the controller for prosecution or punishment when it finds a violation of this Act or other data protection provisions (Sec. 38(1)). It may also order remedial measures and may

[432] According to Sec. 38(1) of the German FDP Act, the supervisory authority is responsible for monitoring the implementation of this Act and other data protection provisions governing the automated processing of personal data or the processing or use of personal data in or from a non-automated filtering system.

prohibit the collection, processing or use of personal data if these violations are not remedied within a reasonable time (Sec. 38(5)). The need to establish a data protection authority was also recognized by the EU Charter of Fundamental Human Rights (Art. 8) and the EU Directive (Art. 28.1). The EU Directive requires that a supervisory authority should be endowed with appropriate powers in respect of investigation, intervention and engagement in legal proceedings where a violation has occurred (Art. 28.3).

It would be valuable to have one or more independent privacy protection authorities which can represent the interests of individuals. A privacy protection authority should be empowered to supervise the government agencies and corporations and monitor their compliance with the data protection provisions. As an effective option for individuals, the privacy protection authority can also prosecute and sue corporations which fail to comply with the legal requirements and cooperate with and exchange information regarding threats or enhancement measures regarding data protection with different bodies. Such an authority is particularly important in competing against the power of the government agencies and large, wealthy corporations. An independent privacy protection authority is the true demand to the data subjects for helping them protect their personal data but it has been never considered by the lawmakers of the PIP Act.

5.4.5. The overriding interests of the controllers rather than the data subjects

Apart from special categories of information, a government agency can only collect or process personal information where there is a specific purpose and compliance with one of the following conditions (Art. 15):

a. Collection or processing is necessary for the exercise of official authority vested by law;

b. The data subject has given his written consent; or

c. There is no harm to the right and interests of the data subject.

A non-government agency or individual can only collect or process personal data if (Art. 19.1):

a. It is in accordance with law;

b. There is a contract or quasi-contract between the data subject and the agency;

c. The information has been disclosed by the data subject or publicized legally;

d. It is necessary for the public interests and carried out by a research institution for statistical or academic research purposes;

e. The data subject has given his written consent;

f. It concerns the public interests; or

g. The information is obtained from publicly-available resources.

The right of information privacy is a recognized fundamental human right which can only be limited by law under very exceptional circumstances pursuant to Art. 23 of the Constitution.[433] To respect the data subjects' right of informational self-determination and effectively protect their right to privacy with respect to personal data, any collection should be strictly banned unless it is carried out under the data subject's consent or in accordance with the law.

However, the PIP Act, with very little regard to the spirit of information privacy, provides ample scope for exceptions, exemptions and vague concepts such as the 'public interest' and 'major interests' for justifying exemptions. The PIP Act allows the government agencies to legalize their unauthorized collection of personal information once they can prove that such collection is not harmful to the right or interests of the data subject (Art. 15 (c)). This provision obviously mistakes

[433] Art. 23 of the Constitution: All of the freedoms and rights enumerated in the preceding Articles shall not be restricted by law except by such as may be necessary to prevent infringement of the freedoms of other persons, to avert an imminent crisis, to maintain social order or to advance public welfare.

cause for effect, as any collection of personal data without authorization by law or the data subject, is an infringement of the right to information privacy which is also *per se* a harm to the interests of the data subject. If not caused by an insufficient understanding of the right of information privacy, this may be taken as a clear example of the lawmakers' intention to diminish the hindrance of individual privacy protection to efficient governmental operations related to personal data collection.

In addition, the PIP Act provides non-government agencies with a legitimate basis for personal information collection as long as the said information is obtained from publicly-available resources (Art. 19.1(g)).[434] The "publicly-available resources", according to the definition provided by the Enforcement Rules, means "*media, Internet, news, magazine, government gazette and other accesses through which the general public may be aware of or contact, and thus obtain personal information*." (Art. 28) These resources may include social networking websites, chat rooms, news groups or other websites that are open to the public. Nevertheless, the information obtained from the above resources is not necessarily disclosed by the data subjects themselves. It can be made public by a third-party without the awareness or consent of the data subject. Even if the data subject discloses his own personal information, this should not be understood as constituting unconditional permission for any person to obtain or use this information. However, by putting aside the data subject's interests in his personal information, this provision encourages the private sector or even cyber criminals to engage in the large-scale harvesting of personal information through scanning websites, probably by running particular software programs. This, once again, reflects the primacy of the controllers' interests over those of the data subjects.

[434] Non-government agencies should delete or stop processing or using personal information which has been obtained via publicly-available resources, *ex officio* or upon the request of the data subject, where there is an obvious worthiness of the protection of the data subject's major interests (Art. 19.1(g), 19.2). However, it comes to a question of what is the extent of the 'obvious worthiness of major interests'? Also, in what ways can a data subject be expected to request the deletion or discontinuation of use or processing of their information if they have little chance of being aware of the data collection matter? This provision appears to consider the right of information privacy; however, it only provides infeasible, hollow protection to the data subjects.

The continuous intervention of enterprises, as mentioned in the previous subsection (3.3.1), has been a major reason causing the Executive Yuan to delay implementation of the PIP Act for 28 months, exacted in May 2012 and enforced in October 2012. The pressure exerted by the enterprises had successfully propelled the MOJ to initiate the re-amendment of the PIP Act even before it came into effect and eventually stopped the Executive Yuan from bringing Art. 6 and 54 into force.

The Executive Yuan held back the enforcement of these two articles on the grounds of difficulty of administration. The decision of the Executive Yuan not only inspired controversy over the constitutionality[435] but, most importantly, it shows the concession of the executive power of Taiwan to enterprises when facing a conflict between personal information protection and business interests.

As discussed in the previous subsection (5.3.3.2), Art. 6 places a prohibition on collecting, processing, and using special categories of data concerning body, health, sexual life or criminal records; in the meantime, it also provides four exceptional conditions to the prohibition. This provision, however, has been strongly opposed by most Taiwanese enterprises especially those involved in dealing with special types of data, on the grounds of the difficulty of meeting the foregoing four conditions specified. As a result, the Executive Yuan decided to suspend the enforcement of Art. 6 and, for the convenience of the enterprises, proposed the addition of two exceptions which permit the collection, processing and use of the said data when “it is with the

[435] The Constitution of Taiwan states that the Executive Yuan should send an enacted law back to the Legislature for reconsideration within ten days after it has been passed if the Executive Yuan believes that this law is difficult to carry out (Art. 57). The President of the Executive Yuan shall abide or resign from office if the original law is upheld by two-thirds of the Members of the Legislative Yuan. Some argue that the Executive Yuan broke the mechanism established by the Constitution to deal with unenforceable laws and that this suspension of the partial provisions of the PIP Act is unconstitutional. Chen, H. L. (2013), 'Taiwan's PIPA into force, with controversial sections removed', *Privacy Laws & Business International Report*.

consent of the data subject" or when "it is necessary to serve and protect public interests". The abstract legal concept of "public interests" has been repeatedly used by the lawmakers to remove notice duty of data controllers (Art. 9.1(d) (e)) and justify the unauthorized collection, processing, and use of personal information (Art. 16(b) (e), 19.1(d), and 20.1(b) (e)). While the use of an indeterminate legal concept is sometimes necessary to promote administrative efficiency, it can cause chaos in terms of administration due to the inconsistent explanations of the same concept, especially when there is an absence of central government authority in charge of personal information protection tasks, which is precisely the case in Taiwan. This re-amendment to Art. 6 is unfavourable to the protection of special types of sensitive data but only helpful to the data controllers to legitimize their unauthorized collection or use of the foregoing data.

Under Art. 54 of the PIP Act, a controller is obligated to fulfill its notice duty to the data subjects with regard to their personal information that has been indirectly obtained before the amendment within a year from the effective date. Nevertheless, this provision has occasioned strong complaint by the finance, telecommunications, and other industries about the difficulty of implementation within the time limit and the excessive cost of carrying out the notice duty.[436] To respond to the enterprises' disapprobation, the MOJ, with no regard to the right of a data subject of access to his personal information, decided to exclude Art. 54 from the enforcement of the PIP Act and has proposed to amend to this article to loosen the notice duty of a controller by replacing with a requirement of notice only before using the personal information. The continuous compromise of the MOJ with the enterprises is accompanied with the sacrifice of the interests of data subjects. The PIP Act, which is expected to stand with the interests of the data subjects, has unfortunately become a law driven by the economic interests of the controllers.

[436] Council for Economic Planning and Development (2012), 'Personal Information Protection Act being implemented in two stages', *Taiwan New Economic Newsletter*, 141, 24 October 2012, available at: http://www.cepd.gov.tw/encontent/m1.aspx?sNo=0017765. [Accessed 16 April 2013]

5.5. Conclusion

This chapter argued that, in the context of phishing, law can serve not only a corrective measure which deters prohibited behaviour through coercion or punishment, it is also a preventative initiative which functions by ensuring the security of personal information databases and the control of data subjects' over their personal information against unauthorized access, collection and disclosure. Yet, there is a dearth of scholarly work on the subject. The chapter indicated that phishing is a direct infringement of information privacy and is often used as a leading vector for data breach which usually involves exploitation of personal information gathered from social networking sites. Phishing and data breach are complementary to each other. While phishing significantly facilitates the chance of attackers to gain a toehold in a specific target's environment, the great amount of stolen personal data obtained from a data breach also greatly enhances the creation of numerous phishing scams. Social networking service allows individuals to share and update information about their family, work and activities with hundreds of millions of members across the globe instantly; however, this at the same time provides phishers effortless access to a vast volume of personal data which has been increasingly exploited for crafting a personalized phishing message for a specific target, known as spear phishing. The growing threat posed by phishing to information privacy underscores a pressing need of strengthened legal protection of personal information which should particularly maintain the confidentiality of personal data, ensure data controllers' obligation towards database security, and reinforce individuals' control and choice regarding their data.

The first information privacy protection law was passed in West Germany in 1970, which was followed by a succession of data protection enactments in other European countries. However, the inconsistency among regulatory regimes about personal data protection has caused a restraint on trade and inspired a desire for international standards for harmonization of national privacy legislations. Since the 1970s, significant progress has been made in establishing international privacy guidelines since the 1970s. The frameworks set out by the OECD, the EU, and the APEC particularly had profound influence upon Taiwan's enactment of personal data protection laws. The PIP Act of Taiwan especially incorporated the principles set out by the 1995 EU Directive regarding 'prohibition of the processing of special categories of data' and 'notice of data collection' and adopted the APEC IPPs, 'preventing harm', 'collection limitation' and 'notice'.

While Taiwan has made certain efforts to provide an overarching law for personal data protection, there appears to be no clear consensus about what is the central interest that it should endeavor to protect. This chapter put forward arguments to the PIP Act in five points, especially based on the requirements arising from the regulation of phishing. This research argued the significance of discriminating between 'identifiable information' and 'de-identifiable information', as the line between these two kinds of information has become blurred and this discrimination is very likely to leave an unregulated circumstance in which the information is sensitive to a person but may not be linked to him. Therefore, this research suggested that the term 'personal information' should be broadly recognized and not subject to discrimination based on whether or not it can be used to identify a person.

In addition, the public expectation is that the protection provided by the PIP Act should be maximized, whereas the expectation of the government and businesses is that the detrimental effect incurred by the Act should be minimized. It is understandably difficult to achieve a balance between these two values – the value of information privacy and the value of efficiency of data collection, processing, and use; however, the creation of unnecessary burden on the data subjects of protecting the quality of their data along with an ample scope of exemption of controllers from the prohibition of the collection, use and processing of personal data reflected the lawmakers' evident bias in favour the data controllers which has resulted in loose and weak legal protection of personal information.

The difficulty of balancing between two different values highlights the importance of a data protection authority which can effectively represent information privacy interests and has sufficient powers and resources to monitor the controllers' operations in relation to personal data and ensure the proper implementation of the data protection provisions. Unfortunately, plans for an independent data protection authority or agency have never been included in the blueprint of the Taiwanese government.

The continuous battle between the enterprises and the MOJ regarding the elements of liability caused a great delay in the enforcement date of the PIP Act. The primary concern of most enterprises is how they can 'legally' collect and use individuals' personal information to the maximum standard while decreasing their risk of being sued for compensation to the minimum standard. Little consideration has been given to how to reduce unnecessary intervention in information privacy and underpin the safeguarding of personal information against unauthorized access. This is the fundamental difference in the expectations regarding the PIP Act of the controllers and the data subjects. Whether or not the lawmakers can close the gap without sacrifice of specific one-sided interests is the key determining whether the PIP Act can provide substantial protection to information privacy or is a law that exists in name only. This is also crucial to determining whether Taiwan can provide effective legal regulation of phishing in terms of personal information protection.

CHAPTER 6 HARMONIZATION OF LEGAL ENFORCEMENT IN COMBATING PHISHING

Synopsis

This chapter investigates the challenges that phishing has posed to legal enforcement and the solutions required to address weak legal enforcement. It considers the progress that has been made in the development of hard law and soft law, both nationally and internationally, to respond to phishing and the challenge of cybercrime to legal enforcement. This chapter also examines the gaps in criminalization between the existing national and international legal instruments and phishing in terms of the elements of acts and objects and concludes with suggestions for steps to pursue effective legal enforcement.

6.1. Introduction

As we saw in the previous chapters,[437] the transnational dimension of phishing has been a crucial challenge to law enforcement. The borderless nature of cyberspace permits phishing attacks to be operated freely beyond the restriction of geographical frontiers and allows phishers to obscure their location and identity to evade tracing and prosecution. Phishing is frequently a transnational phenomenon, and phishing sites are usually ephemeral and can reappear quickly after they are removed. These all largely increase the difficulties for legal enforcement agencies in investigating and prosecuting phishing perpetrators. The challenges posed by phishing to legal enforcement have

[437] See Chapter 2, section 2.5.1 and Chapter 4, section 4.4.2.5.

raised increasing concerns of legal solutions[438] which usually involve national approaches to criminalizing phishing and international approaches to harmonizing legal standards and cooperation between legal enforcement agencies across countries.

This chapter looks into the legal approaches that have been taken, both nationally and internationally, to respond to phishing and the challenges that cybercrime has posed to legal enforcement, with an aim to contribute towards an examination of their effectiveness in the regulation of phishing. It firstly demonstrates the weaknesses in traditional legal enforcement systems and examines the challenges that phishing, by its transnational and transient elements, has posed upon legal enforcement work and how these can be addressed by an international integrated and harmonized approach to legal standards and cooperation. Thus the chapter explores both national laws, using UK and US as examples and international attempts at harmonization both through hard and soft-law measures as well as international cooperation mechanisms, with a focus on the 24/7 networks that have been established to facilitate contact and coordination of investigative actions against cybercrime between countries.

6.2. Challenges to legal enforcement

While the value of legal regulation lies in effective legal enforcement, phishing, by its nature, has posed crucial challenges to legal enforcement work. Cyberspace provides a playground for cybercriminals to engage in a variety of malicious activities beyond the restriction of geographical frontiers, which makes it an uneasy task to control a particular online behaviour and drastically increases the difficulties of legal enforcement.[439] Lynch[440] and Sullins[441] addressed several

[438] Lynch (2005), op. cit;Menon and Siew (2012), op. cit;Sullins (2006), op. cit.

[439] Broadhurst (2006), op. cit;Lovet (2009), op. cit;Wall (2003), op. cit.

[440] Lynch (2005), op. cit.

[441] Sullins (2006), op. cit.

problems with the legal enforcement of phishing laws. Jurisdictional problems always prevent proper investigation. Another significant problem is that law enforcement agencies, in general, have insufficient technical knowledge and training to deal with phishing.[442] Phishing technology is rapidly evolving; however, it is difficult and costly to increase the technical knowledge of the members of law enforcement agents and keep them continuously updated. On examining the legal enforcement system of USA, Lynch found that the local police were unenthusiastic about spending limited resources investigating a crime that occurred in another jurisdiction whereas the federal investigation agencies may not help the individual victim unless it involved a certain amount of loss.[443]The weakness in traditional law enforcement demonstrates the need for a new approach.[444]

6.2.1. Transnational nature

Phishing frequently involves two or more jurisdictions. The transnational nature of phishing has been recognized as a key challenge to legal enforcement work.[445] Phishing attacks can be carried out by hosting sites or targeting people in different countries, and can be operated by a single person or organized group consisting of members from multiple countries. Cross-border criminal investigations demand the cooperation of law enforcement agencies in all of the countries involved.[446] However, national sovereignty[447] does not allow investigations to be carried out within the territory of different countries without the permission of the local authorities.

[442] Brenner, Susan W and Schwerha IV, Joseph J (2001), 'Transnational evidence gathering and local prosecution of international cybercrime', *J. Marshall J. Computer & Info. L.,* 20, 347;Sullins (2006), op. cit.

[443] Krebs (2004), op. cit.

[444] Lynch (2005), op. cit;Menon and Siew (2012), op. cit;Sullins (2006), op. cit.

[445] Dinna et al. (2007), op. cit;Lynch (2005), op. cit;Stevenson (2005), op. cit;Sullins (2006), op. cit.

[446] Sofaer, Abraham D and Goodman, Seymour E (2001), 'Cyber Crime and Security. The Transnational Dimension', in Abraham D Sofaer and Seymour E Goodman (eds.), *The transnational dimension of cyber crime and terrorism* (Stanford: Hoover Institution Press), 1-34.

[447] Roth, Brad (2005), 'State sovereignty, international legality, and moral disagreement', *The annual meeting of the American Political Science Association* (Washington, DC, USA).

Mutual legal assistance (MLA) is an essential tool in the global fight against transnational crime, even in the absence of a bilateral or multilateral mutual legal assistance treaty or convention. While a country may seek legal assistance from another on the basis of non-treaty letters of request, it is sometimes rather time-consuming. Each country has different laws with regard to the procedures and the authorities which deal with or govern the non-treaty based requests for legal assistance in criminal investigations and enforcement. In some countries, for example, Japan, a non-treaty request is required to be processed via diplomatic channels, while it may be sent to the judicial authorities directly with no need to go through diplomatic procedures in other countries, for example, the UK and the US.[448]

More importantly, although more and more countries are abandoning basing MLA on dual criminality, which requires that the conduct in question is criminalized in the law of both the requested and requesting states, the absence of dual criminality has traditionally been a classic ground for the refusal to provide legal assistance, particularly with regard to measures such as search or seizure. Thus while none of the G8 member states, apart from Japan, base MLA in criminal matters on dual criminality, they make exceptions for requests that involve search, seizure, confiscation of assets or other coercive measures.[449] Yet, investigations into a phishing attack mostly need to search or seize the perpetrator's computer, hardware, log file, or other data or devices related to the offence in order effectively to maintain the integrity of the digital evidence[450] and trace back the methods and routes of how the attack was operated. Dual criminality hence inevitably becomes a requisite when a state seeks legal assistance in investigations of phishing attacks from a foreign jurisdiction.

[448] Commission on Crime Prevention and Criminal Justice (2011), 'Requesting mutual legal assistance in criminal matters from G8 countries: A step-by-step guide, E/CN.15/2011/CPR.6', 20. <http://www.coe.int/t/DGHL/STANDARDSETTING/PC-OC/PCOC_documents/8_MLA%20step-by-step_CN152011_CRP.6_eV1182196.pdf>, accessed September 15 2014.

[449] Ibid.

[450] Digital evidence is defined as "any data stored or transmitted using a computer that support or refuse a theory of how an offense occurred or that address critical elements of the offense such as intent alibi." Casey, Eoghan (2011), *Digital evidence and computer crime: forensic science, computers and the internet* (3 edn.: Academic press).

Given the requirement of dual criminality for MLA, a phishing perpetrator may find safe haven by intentionally including one or more country that lacks or has not fully developed laws in the area of phishing in order to impede investigation. Therefore, the first step to achieve a seamless web of legal enforcement is to ensure the prevalence of the criminalization of phishing among different jurisdictions. The uneven regulation of phishing resulting from the divergence between the phishing laws of different countries is another significant problem that can undermine legal enforcement. This should be addressed by international harmonization of legal standards to promote the consistency and compatibility of the national laws in relation to phishing.

Several researchers studied the phishing laws that have been developed in various countries such as UK,[451] USA,[452] South Africa[453] Saudi Arabia,[454] Malaysia,[455] India,[456] and Taiwan.[457] Instead of introducing a new provision specific to phishing, most countries deal with phishing by either applying their existing cybercrime laws or common laws in relation to spam,[458] impersonation, theft or fraud or developing or updating the law of identity fraud or identity theft. Nevertheless, some studies suggested that the existing legal framework is inadequate to fully cover the conduct of phishing.[459] It is essential to identify the gap in their context in order to make sure every element of phishing has been adequately accommodated. Section 6.3 will looks into the national phishing laws in different domains as well as the international legal instruments that have been developed over the

[451] Bainbridge (2007), op. cit;Mcgowan (2006), op. cit.

[452] Lynch (2005), op. cit;Mcnealy (2008), op. cit.

[453] Granova and Eloff (2005), op. cit.

[454] Almerdas (2014), op. cit.

[455] Dinna et al. (2007), op. cit.

[456] Nappinai (2009), op. cit.

[457] Hsueh (2013), op. cit.

[458] For example, Canadian Anti-Spam Law (CASL) which came into effect on 1 July 2013 regulates phishing by imposing penalties for sending spam or installing spyware on computers without their owner's consent (sec. 8). Bayley, Robin and Bennett, Colin (2014), 'Canada's "anti-spam" law comes into force on 1 July this year', *Privacy Laws & Business International Newsletter,* 129, 19-20;Gannon, James, Morgan, Charles S., and Salzman, Lorne P. (2010), 'Canadian Government's proposed anti-spam and anti-spyware legislation', *World Data Protection Report,* 10 (9), 9-11.

[459] Dinna et al. (2007), op. cit;Granova and Eloff (2005), op. cit;Nappinai (2009), op. cit.

past decade to respond to cybercrime and examine whether they can adequately cover phishing.

6.2.2. Transient nature

Apart from the challenges that the transnational element poses on investigation and prosecution work, the short lifetime of phishing sites[460] and the speed at which phishers can move to another server or reappear after the counterfeit sites have been taken down places the legal enforcement agencies under heavy time pressure to identify and trace them.[461] Tracking and tracing an attack may not only interrupt the attack in progress but the process of tracing may also be helpful in uncovering the route and relevant details of the attack techniques to facilitate the development of defensive measures that could prevent similar attacks in the future.[462] Importantly, it is a prerequisite for bringing the attacker to justice.

However, the characteristics of cyberspace, in particular anonymity, invisibility and remoteness, enable phishing perpetrators to be at lower physical risk of being caught and prosecuted.[463] In addition, a vast majority of phishing perpetrators deliver scam messages via botnets[464] and tend to host phishing sites on free web space or compromised machines rather than on their own machines.[465] These all drastically increase the difficulties for investigators to identify real phishers.

[460] Apwg (2008a), op. cit.

[461] Varghese (2008), op. cit.

[462] Lipson, Howard F (2002), 'Tracking and tracing cyber-attacks: Technical challenges and global policy issues', (DTIC Document).

[463] Brenner, Susan W (2004), 'Toward a criminal law for cyberspace: A new model of law enforcement', *Rutgers Computer & Tech. LJ,* 30, 1;Katyal, Neal Kumar (2001), 'Criminal law in cyberspace', *University of Pennsylvania Law Review*, 1003-114.

[464] Bacher et al. (2005), op. cit;Feily, Shahrestani, and Ramadass (2009), op. cit;Ianelli and Hackworth (2005), op. cit;Milletary (2005), op. cit.

[465] Mcgrath and Gupta (2008), op. cit;Moore and Clayton (2009), op. cit.

Several forensic protocols have been introduced by researchers for tracing phishing, such as hosting a honeynet[466] that was attacked by phishers,[467] using web bugs and honeytokens[468] on the fake web site to trace the unauthorized access by phishers,[469] and feeding phishers fingerprinted credentials (*phoneytokens* or phishing honeytokens) which look like a valid credential to the phisher but can be identified and traced.[470] Nevertheless, the honeynet project was more interested in collecting information regarding the technical means used by phishers rather than in tracing phishers. In addition, a honeytoken is useful only when it can guarantee that the only access to that token would be by unauthorized parties, which means that the token's tracking ability is likely to be compromised if the token could be viewed in normal interaction with a system.[471] It seems that whether these methods can track down phishers and how far they are able to trace still need to be further proved and verified. Granted there is a tool that is able to accurately identify the location or even the identity of phishers, phishing perpetrators still have great chance to flee from arrest if the investigative authorities fail to react in a timely manner.

[466] A honeynet is a network set up with intentional vulnerability, aimed to attract and trap attackers in order to gather information about their activities and study their motives and methods which can be subsequently used to increase network security. It usually contains one or more honeypot. According to the definition given by Lance Spitzner, a honeypot is "*an information system resource whose value lies in unauthorized or illicit use of that resource*." A honeypot can be a computer or merely a resource which is deployed intentionally for attackers to interact with. Rouse, Margaret (2007), 'Honeynet', *TechTarget*. <http://searchsecurity.techtarget.com/definition/honeynet>, accessed September 17 2014;Spitzner, Lance (2010), 'Honeytokens: The Other Honeypot', *Symantec* <http://www.symantec.com/connect/articles/honeytokens-other-honeypot>, accessed September 20 2014.

[467] Watson, David, Holz, Thorsten, and Mueller, Sven (2008), 'Know your Enemy: Phishing', *The Honeynet Project*. <http://www.honeynet.org/papers/phishing/>, accessed September 15 2014.

[468] A honeytoken is a honeypot that can only come in the form of digital or information system resource. It can be a credit card number, Excel spreadsheet, PowerPoint presentation, a database entry, or a bogus login. As a honeytoken has no authorized use, no one should be using or accessing it. Therefore, any interaction with a honeytoken is very likely to be unauthorized or malicious activity. Spitzner (2010), op. cit.

[469] McRae, Craig M and Vaughn, Rayford B (2007), 'Phighting the phisher: Using web bugs and honeytokens to investigate the source of phishing attacks', in Jr. Ralph H. Sprague (ed.), *40th Annual Hawaii International Conference on System Sciences 2007 (HICSS 2007)* (Big Island, Hawaii: IEEE), 270c-70c.

[470] Birk, Dominik, et al. (2007), 'A forensic framework for tracing phishers', *IFIP Summer School on The Future of Identity in the Information Society, Karlstad, Sweden*;Gajek, Sebastian and Sadeghi, Ahmad-Reza (2008), 'A forensic framework for tracing phishers', in Simone Fischer-Hübner, et al. (eds.), *The Future of Identity in the Information Society* (Springer), 23-35.

[471] Birk et al. (2007), op. cit.

A quick response is crucial for a successful investigation, which can only be made by cooperation, both at domestic and international levels. As Sullins emphasized, the solution to phishing or other non-traditional crimes lies in cooperation in three areas: law enforcement, legislation and the private sector.[472] Similarly, Lynch also manifested the necessity of coordination between potential victims, law enforcement agencies, and other organizations that have the means to control information and Internet security.[473] Section 6.4 will look at the global and regional frameworks that have been developed to promote coordination and cooperation between legal enforcement agencies and private sectors involved against cybercrime.

6.3. Legislative response to the threat of phishing

The introduction of computer and Internet technologies has given rise to new forms of crime which pose crucial challenges to the national and international legal systems. To respond to the emergence of new offences, lawmakers must make necessary amendments to the existing criminal laws. Offences that have been criminalized under national criminal law need to be reviewed and updated to integrate new forms of cybercrime. For example, electromagnetic records or digital information need to be given equivalent status to traditional written documents.[474]

The legislative adjustment may generally start with the identification of gaps in the criminal code. To ensure an effective legal foundation for combating cybercrime, it is essential to identify the gaps between the status of the criminal legal provisions in the existing national laws and the requirements arising from criminal offences which abuse the new technology. In many cases,

[472] Sullins (2006), op. cit.

[473] Lynch (2005), op. cit.

[474] An example of the integration of digital sources is Section 11.3 of the German Criminal Code: “Audiovisual media, data storage media, illustrations and other depictions shall be equivalent to written material in the provisions which refer to this subsection.” Similar provision can also be found in the Criminal Code of Taiwan which provides the same status as document to “audio records, visual records, electromagnetic records or the voices, images or symbols that are illustrated through the computer process” (Art. 220.2).

cyber-related crimes are not new crimes but ones committed using information communication technologies which may be covered by existing offences. For example, the laws that address forgery may also apply to the treatment electromagnetic records. In this case, the legislative amendment needs to focus solely on those offences that are insufficiently covered by the national law.

However, if the actions performed cannot be addressed by the existing laws, the drafting of new legislation is considered a necessity. One example is computer-related fraud. In the past, some countries had adequate provisions for regular fraud but were unable to deal with offences whereby a computer system was influenced, rather than a human. For these countries, the adoption of new laws which criminalize computer-related fraud has hence become indispensable.[475]

The effective investigation and prosecution of phishing attackers is grounded on the universal criminalization of phishing. Several countries have undertaken legislative measures to respond to the increasing threat of phishing. First, this section provides an examination of the national laws, as illustrated by the example of UK and US laws on criminalizing phishing. This is followed by an overview of the international legal instruments that play a key role in the development of the criminal law provisions and cross-border legal enforcement cooperation addressing cybercrime, particularly identity or fraud-related crime.

6.3.1. National laws on phishing-related crime

The reason why I use the term ‘phishing-related crime’ is because there has been no specific law passed against the offence of phishing. A clear definition is the basis for the development of legal solutions. However, phishing is in general not a stand-alone crime, as it is considered as synonym of

[475] As example of new legislation on computer-related fraud is Art. 339-3 of the Taiwanese Criminal Code, passed in 1997, which makes it a crime to “obtain another person’s property or to cause another person to obtain unlawful profit of property by inputting false data or giving an unauthorized command to a computer or related equipment to create a false electromagnetic record relating to acquisition, loss, or alteration of property rights”.

identity theft in some countries[476] and is usually covered by the concept of identity theft or identity fraud. The term ‘phishing’ can be used to describe a combination of acts. It contains two key elements: object (sensitive information belonging to another) and two acts. The first act is using the identity of a person or a corporation, for example, their name, email address, logo, or trademark, and the second act is obtaining data. The object ‘data’ can include identity-related information and other confidential information related to a person, enterprise, or country. Therefore, the identity can be either a tool or a target in some phishing cases whereby a phisher uses the identity of a person to acquire identity information from another person.

The criminalization of phishing is usually covered by the offence of ‘identity theft’ or ‘identity fraud’, under an umbrella term ‘identity-related crime’. Identity-related crime concerns “*all punishable activities that have identity as a target or a principal tool*”,[477] which may include identity fraud, identity theft or other related offences, such as the possession, distribution, and manufacture of relevant items, devices, etc. Although a commonly accepted definition of identity theft is still lacking,[478] one of the general definitions is “the theft or assumption of a pre-existing identity (or significant part of it), with or without consent, and regardless of whether the person is dead or alive”.[479] This definition contains the object (identity) and the act (assumption), which overlaps with the elements of phishing but cannot fully cover them. The object in this definition is only specified for identity-related information and the act focuses on obtaining the identity. Thus, the obtainment of information other than identity and the use of identity are not covered by this definition.

[476] Acoca, B (2008), 'Scoping paper on online identity theft (Ministerial Background Report DSTI/CP (2007) 3/FINAL. Retrieved May 27, 2009'.

[477] Koops, Bert-Jaap and Leenes, Ronald (2006), 'Identity theft, identity fraud and/or identity-related crime', *Datenschutz und Datensicherheit-DuD,* 30 (9), 553-56.

[478] Koops and Leenes (2006), op. cit.

[479] Paget, François (2007), 'Identity theft', *McAfee Avert Labs technical white paper*. <http://www.pubblicaamministrazione.net/file/whitepaper/000042.pdf>, accessed September 17 2014.

‘Identity fraud’ arises “*when a person pretends to be someone else through the taking over of a false identity or the adoption of a real person’s name with or without their permission to obtain goods and services*”.[480] This definition contains two acts – using (taking over/adoption) identity (fictitious or real identity) and obtaining monetary gain (goods and services). An overlap of these elements can be seen between phishing and identity fraud, as both use a false identity to defraud someone. However, identity fraud concentrates on monetary or property gain, while phishing targets a variety of sensitive information which may bring financial gain but not on every occasion. As a consequence, the definition of identity fraud may cover phishing, but only partially.

The definition of identity theft or identity fraud varies in different publications and legislations. Some use the term ‘identity theft’ to describe any act of obtaining an identity, while others only use it to describe the use of another person’s identity in relation to other offences.[481] While most US laws and publications use the term ‘identity theft’, the term ‘identity fraud’ is widely preferred in the UK laws.

Nevertheless, the inconsistent use of the terms and gap between phishing and identity theft and identity fraud cause the main difficulty in the criminalization of phishing. This subsection studies and reviews the laws of the UK and US (including the failed Anti-Phishing Bill of 2005) as examples of national legislations in relation to Internet-related identity theft and fraud, and analyses the above statutes to evaluate the extent to which they already cover phishing.

6.3.1.1. The UK Fraud Act 2006

[480] United Kingdom Cabinet Office (2002), 'Identity Fraud: A Study'. <http://www.statewatch.org/news/2004/may/id-fraud-report.pdf>, accessed September 17 2014.

[481] Gercke, Marco (2007), 'Internet-Related Identity Theft', *Economic Crime Division, Directorate General of Human Rights and Legal Affairs, Strasbourg, France*.

The provisions involved in regulating phishing

The UK Fraud Act 2006 has been the most significant law which strengthens the ability of the criminal law to deal with phishing and the possession, making or supplying of phishing kits.[482] There had been no single fraud legislation in English law until the Fraud Act 2006.[483] The Fraud Act 2006 aims to close the loopholes existing in the old regime by tackling modern fraudulent activity and keeping pace with the rapid technological developments. This Act replaced a complicated array of deception offences[484] by introducing three specific forms of fraud: fraud by false representation (section 2), fraud by failing to disclose information (section 3) and fraud by abuse of position (section 4).

> Section 2(1) outlaws conduct whereby a person:
>
> (a) Dishonestly makes a false representation, and
>
> (b) Intends, by making the representation to –
>
> (i) make a gain for himself or another, or
>
> (ii) cause loss to another or to expose another to a risk of loss

In *R v. Ghost,*[485] Lord Lane CJ established a two-stage test to determine whether the defendant was acting dishonestly:[486]

[482] Phishing kits refer to computer programs or data designed or used to launch phishing attacks.

[483] The Fraud Act 2006 received Royal Assent on 8 November 2006 and came fully into force on 15 January 2007.

[484] These deception offences include 'obtaining property by deception' (section 15 of the Theft Act 1968), 'obtaining a money transfer by deception' (section 15A of the Theft Act 1968), 'obtaining pecuniary advantage by deception' (section 16 of the Theft Act 1968), 'procuring the execution of a valuable security by deception' (section 20(2) of the Theft Act 1968), 'obtaining services by deception' (section 1 of the Theft Act 1978) and 'evasion of liability by deception' (section 2 of the Theft Act 1978). See the Explanatory Notes of the Fraud Act, para. 7.

[485] [1982] QB 1053.

[486] See the Explanatory Notes of the Fraud Act, para. 10.

> […], a jury must first of all decide whether according to the ordinary standards of reasonable and honest people what was done was dishonest. If it was not dishonest by those standards, that is the end of the matter and the prosecution fails.

If it was dishonest by those standards, then the jury must consider whether the defendant himself must have realized that what he was doing was by those standards dishonest.

A representation is 'false' if it is untrue or misleading and the person making it knows that it is, or might be, untrue or misleading (section 2(2)). No limitation is placed on the way in which the representation must be expressed. A representation may be express or implied (section 2(4)), which can be stated in words or communicated by conduct. It could also be written, spoken or posted on a website.[487] A representation may be regarded as 'made' if it is submitted in any form to any system or device designed to receive, convey or respond to communication (with or without human intervention) (section 2(5)). Accordingly, representation made by email is also included.

In the Explanatory Notes of the Fraud Act 2006, the lawmakers particularly address that the section 2 offence, which carries a maximum sentence of 10 years' imprisonment (section 1 (3)(b)), would be committed by a person who engages in phishing when he disseminates an email to groups of people falsely representing that the email has been sent from a legitimate entity to prompt the recipients to provide information such as credit card and bank account numbers so that the phisher can gain access to the victims' other assets.[488]

In addition, this Act makes it a crime if a person has in his possession or under his control any article for use in the course of or in connection with any fraud (section 6(1)). Under section 7 (1),

[487] See the Explanatory Notes of the Fraud Act, para. 14.
[488] See the Explanatory Notes of the Fraud Act, para. 16.

this offence occurs when a person makes, adapts, supplies or offers to supply any article. The above statutes require the specific knowledge or intention of the accused. The accused needs to know that this article is designed or adapted for use in the course of or in connection with fraud, or intends this article to be used to commit, or assist in the commissions of fraud. ‘Article’ includes any program or data held in electronic form (section 8 (1)). Accordingly, a person who writes a program aimed at producing counterfeit websites or emails for the use of phishing, supplies it to another or simply possesses it, intending to commit phishing or facilitate the commission of phishing, constitutes a breach of sections 6 and 7.

Gaps in application

While the Fraud Act 2006 demonstrates an attempt to make phishing an offence of fraud by false representation (section 2), it fails to give comprehensive consideration to the discrepancy of the elements between fraud and phishing. The section 2 offence requires that the person must make representation; it nevertheless does not address certain malware attacks, where no such representation has been made.[489] Spyware, for example a Trojan or keylogger program, is usually installed on individuals’ computers to collect the stored data or intercept their keystrokes once they visit a malicious website or a legitimate website which is nevertheless embedded with malware. This type of attack is performed without the users’ knowledge and is not necessarily based on an untrue or misleading representation

The nature of the offence of fraud is that it is an economic crime. Although this section does not require that a gain or loss actually occurs,[490] it requires that the person must intend to make a gain

[489] Bainbridge (2007), op. cit.

[490] See the Explanatory Notes of the Fraud Act, para. 11.

or cause a loss or risk of loss to another. Section 5(2) defines 'gain' and 'loss'[491] as extending only to money or other property which refers to any property whether real or personal (including things in action and other intangible property). Accordingly, the section 2 offence can only cover the prosecution of a person who performs phishing intending to make monetary gain or cause a loss to the property of another person; it cannot be used to prosecute phishers with other intents.

Unlike the offence of fraud, phishing is malicious conduct which endangers the integrity and confidentiality of computer system and data privacy. The type of data that a phishing perpetrator targets varies. The data targeted include financial information, such as credit card details or other banking information, which may yield monetary gain or cause a loss to another person's property and other sensitive information which may not result in monetary gain or loss to that person whose information has been acquired. For example, a phisher who obtains the password of another person that enables access to non-financial accounts such as an email account may take over the account and use it for other illegal purposes. This causes an infringement of information privacy of that account owner but does not necessarily bring monetary loss to that person. Although the motive behind a significant number of phishing attacks may involve financial profit, the intent of monetary gain should not be considered as a prerequisite element when deciding whether an offence of phishing has been committed.

6.3.1.2. The US Federal Legislation

[491] 'Gain' includes a gain by keeping what one has as well as a gain by getting what one does not have (section 5(3)) and 'loss' includes a loss by not getting what one might get as well as a loss by parting with what one has (section 5(4)).

Identity theft statutes

The Identity Theft Assumption Deterrence Act of 1998 was the first law to make identity theft a crime[492] at the federal level. This act provided penalties for individuals who had either committed or attempted to commit identity theft. It also empowered the Federal Trade Commission (FTC) to record the complaints of identity theft and refer them to the appropriate consumer reporting and law enforcement agencies.

Identity theft is defined as a federal crime when someone:

> Knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

Based on the above definition of identity theft, law enforcement agencies can prosecute an offender once he 'transfers', 'possesses', or 'uses' identity-related information with the intention to commit, aid or abet an offence even if he either obtains or uses such information for criminal purposes.

The Identity Theft Penalty Enhancement Act, which came into force in July 2004, amended to the federal criminal code to establish a new federal crime, aggravated identity theft (18 U.S.C. §1028A). This act further reinforced the federal government's ability to prosecute identity theft by adding two years to prison sentences for identity theft committed in relation to specified felony violations.

The Identity Theft Enforcement and Restitution Act of 2008 made it the perpetrator's responsibility

[492] Identity Theft is codified at 18 U.S.C. §1028.

to make restitution to a victim of identity theft. Section 202 of this act authorized restitution to identity theft victims through compensation of an amount equal to the value of the time that the victim spent remedying the harm caused by the identity theft. This does not include any incidental losses that a victim may have incurred, for example, denial of credit or increased interest rates caused by identity theft.

However, two gaps exist in the above statutes. The statutes only criminalize the transfer process initiated by the offender, which means that these provisions are inapplicable if the transfer process is initiated by the victim rather than the offender. This is especially relevant in the case of phishing.[493] Phishing perpetrators usually tempt their victims into disclosing and transferring their information by themselves through the manipulation of social-engineering techniques. Due to the lack of a transfer process initiated by the offender, the above identity theft provisions cannot be used to prosecute phishing perpetrators.

Second, as 18 U.S.C. §1028 and §1028A are limited to the illegal use of a means of identification of “a person”, it is unclear whether the federal government can prosecute an identity thief who misuses the identification of a corporation or organization, such as the logo or trademark of a legitimate business.[494] In order to create a convincing website or email, a phishing attacker usually takes the name, logo and trademark of a trustworthy organization. This gap means that the law enforcement agencies cannot use those statutes to charge identity thieves who engage in phishing schemes by illegally using an organization’s name.

[493] Gercke (2007), op. cit.

[494] The US President's Identity Theft Task Force (2007), 'Combating Identity Theft: A Strategic Plan'. <http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/downloadabledocuments/combating_identity_theft_a_strategic_plan.pdf>, accessed September 17 2014.This task force was created in May 2006 by Executive Order 13402 to coordinate federal agencies against identity theft and was charged with creating a strategic plan to combat identity theft. It made a legislative recommendation to the Congress to amend the identity theft statutes so that thieves who misappropriate the identities of corporations and organizations can be prosecuted. However, this recommendation has not yet been addressed by Congress. For more details, see Finklea, Kristin M (2014), 'Identity theft: Trends and issues', *CRS report*. <http://fas.org/sgp/crs/misc/R40599.pdf>, accessed September 10 2014.

The Federal Trade Commission Act and the Gramm-Leach-Bliley Act

In July 2003, the FTC filed a lawsuit against a 17-year-old boy who sent emails purporting to be from America Online to scam the credit card numbers of the recipients.[495] This is the first legal action of the FTC against a suspected phisher. As no specific law existed against phishing, charges were brought under the FTC Act,[496] which prohibits unfair and deceptive practices (15 U.S.C. §45), and the Gramm-Leach-Bliley Act (hereinafter, GLB Act),[497] which outlaws the obtainment of customers' financial information under false pretenses.[498] It constitutes a violation of the GLB Act, which relates to any person who obtains or attempts to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, customer information of a financial institution relating to another person by making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial institution or to a customer of a financial institution (15 U.S.C. Subchapter II, §6821 (a)).

However, two problems arise when applying the GLB Act to phishing cases. This act only covers fraudulent access to customers' financial information, while phishing attackers target a variety of information which may include financial information, personally identifying data as well as other sensitive information such as trade or military secrets. Second, this act creates a significant number of exceptions of applicability for law enforcement agencies, financial institutions, insurance

[495] Legon, Jeordan (2004), 'Phishing'scams reel in your identity', *CNN*. <http://edition.cnn.com/2003/TECH/internet/07/21/phishing.scam/>, accessed September 16 2014.

[496] Federal Trade Commission Act (15 U.S.C. §§41-58) empowers the FTC to prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce. See http://www.ftc.gov/ogc/stat1.shtm.

[497] The Gramm-Leach-Bliley Act was enacted in November, 1999. It prohibits fraudulent access to customer's financial information and encourages the institutions covered by the Act to implement safeguarding measures against such access (15 U.S.C. Subchapter II, §§6821-6827). See http://www.ftc.gov/privacy/glbact/glbsub2.htm.

[498] Moynahan, Moynahan (2005), 'Three ways to fight back against phishing', *COMPUTERWORLD*. <http://www.computerworld.com/article/2568318/security0/three-ways-to-fight-back-against-phishing.html>, accessed September 16 2014.

institutions, and private investigators under certain circumstances (§6821 (c)-(g)). However, it is also very likely to create loopholes in the legal protection against phishing due to the ample exceptions of the prosecution of phishing attackers in accordance with their positions.

The Anti-Phishing Bill of 2005

In February 2005, Senator Patrick Leahy introduced a bill to criminalize Internet scams involving fraudulently obtaining personal information, commonly known as the Anti-Phishing Bill 2005 (s. 472), to combat the weakness of the current laws. According to the statement made by Leahy,[499] the threat of phishing attacks undermines the confidence and trust of Internet users in the Internet and online transactions, which has resulted in a profoundly negative influence on the viability of e-commerce. Leahy also indicated that the prosecutions of phishers, under the current wire fraud or identity theft statutes, can take place only after someone has been defrauded. A law enforcement official is unable to prosecute attackers when the official receives a report from a recipient of a phishing email unless the recipient actually suffers harm by disclosing his information.

To address the inadequacy of the current laws, the Anti-Phishing Bill 2005 attempted to add two new offences to the U.S. code. First, it prohibited the creation or procurement of a website or domain name that represents itself as a legitimate business by which to induce the victim to divulge personal information with the intent to commit a crime of fraud or identity theft (section 1351(a)).[500] Second, it prohibited the creation or procurement of an email that represents itself as

[499] Gross, Grant (2005), 'Proposed Law Aims to Fight Phishing', *PCWorld*. <http://www.pcworld.com/article/119912/article.html>, accessed September 11 2014.

[500] Section 1351(a): whoever knowingly, with the intent to carry on any activity which would be a Federal or State crime of fraud or identity theft – (1) creates or procures the creation of a website or domain name that represents itself as a legitimate online business, without the authority or approval of the registered owner of the actual website or domain name of the legitimate online business; and (2) uses that website or domain name to induce, request, ask, or solicit any person to transmit, submit, or provide any means of identification to another; shall be fined under this

being sent by a legitimate business for the same purpose with the same intent as above (section 1351(b)).[501]

Although this Bill was not passed and its effectiveness was doubted as a delayed response to a problem that has spread rampantly,[502] it was regarded as a step in the right direction and legislation that at least demonstrates a greater awareness of the phishing problem.[503] The Bill criminalized the act of creating a phishing website or a phishing email regardless of whether fraud was committed. While it made an individual criminalization of phishing apart from the offence of fraud or identity theft, it still required that the person who creates a phishing website or email must intend to commit fraud or identity theft.

This Bill was *sui generis* in nature in making it a crime to create or procure the creation of a counterfeit website or scam email for solicitation purposes; however, it did not provide a comprehensive understanding of phishing attacking models. Under the Bill, a counterfeit website was an indispensable element for phishers to induce individuals to reveal their identification information. Directing individuals to visit a fictitious website is a common tactic adopted in phishing schemes, but is not the only way to carry out phishing attacks. In the absence of a phishing website, phishers can still gain the data directly from the recipients' computers through malware installation once the recipients open or execute the spyware in the attachment. A phishing email could be an email that includes a phishing URL and also an email that contains malicious codes or

title or imprisoned up to 5 years, or both.

[501] Section 1351(b): whoever knowingly, with the intent to carry on any activity would be a Federal or State crime of fraud or identity theft sends any electronic mail message that – (1) falsely represents itself as being sent by a legitimate online business; (2) includes an Internet information location tool that refers or links users to an online location on the World Wide Web that falsely purports to belong to or be associated with such legitimate online business; and (3) induces, requests, asks, or solicits a recipient of the electronic mail message directly or indirectly to provide, submit, or relate any means of identification to another; shall be fined under this title or imprisoned up to 5 years, or both.

[502] Germain, Jack M. (2004), 'Will Antiphishing Legislation Be Effective?', *E-Commerce Times*. <http://www.ecommercetimes.com/story/38006.html>, accessed September 11 2014.

[503] Wilson and Argles (2011), op. cit.

malware; for example, a Trojan. Yet, the Bill only addressed one model of phishing attack with no regard to the technical-subterfuge scheme, thus reflecting an inadequate knowledge of the lawmakers.

6.3.1.3. Summary

The lack of a precise definition may not hinder the development of legislation on identity theft or identity fraud in several countries; however, the incomprehensive understanding of the difference between the context of phishing and identity theft or fraud has resulted in gaps in the prosecution of phishing attackers. The diverse definitions of phishing make is difficult to identify the true extent of the problem, which also makes it more difficult to come up with an international approach and coordinate an international investigation, including trans-border evidence sharing, the extradition of offenders and mutual legal assistance. How to pursue a common and converged definition of phishing in both the national and international legal systems is a fundamental question that demands considerable attention in order to close the gaps existing in the criminal legal provisions to ensure the universal criminalization of phishing in the national laws and effective international cooperation over legal enforcement in the fight against phishing.

6.3.2. International laws in combating phishing

In order to eliminate safe havens for phishers and to improve the effective cooperation between the legal enforcement agencies in different countries, it is vital to promote the consistency and compatibility of the phishing laws between different jurisdictions and ensure that there is close cooperation between the countries involved in phishing investigations. Over the past decade, considerable progress has been made to develop a transnational legal instrument to respond to the threat of cybercrimes. This subsection studies two international treaty instruments which provide a fundamental basis for the harmonization of the legal standards in the fight against cybercrime and particularly examines the effectiveness of these two treaties in regulating phishing.

6.3.2.1. United Nations Convention against Transnational Organized Crime

The United Nations has been actively involved in addressing computer-related crime since the eighth UN Congress on the Prevention of Crime and the Treatment of Offenders held in Havana in 1990. In December 2000, a United Nations symposium, themed 'The Challenge of Borderless Cyber-Crime', was held in conjunction with the Palermo signing conference of the Convention against Transnational Organized Crime.[504]

The United Nations Convention against Transnational Organized Crime (the TOC Convention),[505] adopted by General Assembly[506] resolution 55/25 in November 2000, was opened for signature by the Member States in Palermo, Italy, in December 2000 and entered into force on 29 September 2003. The TOC Convention, supplemented by three Protocols, including the Protocol to Prevent, Suppress and Punish Trafficking in Persons; the Protocol against the Smuggling of Migrants; and the Protocol against the Illicit Manufacturing and Trafficking in Firearms, is the leading international instrument in combating transnational organized crime. It has been signed by 147 states and has 166 parties (to date of 29 April, 2012).[507]

[504] Challenge of Borderless 'Cyber-Crime' to International Efforts to Combat Transnational Organized Crime Discussed at Symposium, see http://www.unis.unvienna.org/unis/pressrels/2000/LPMO10.html.

[505] Full text of the TOC Convention and its Protocols, see http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.

[506] The General Assembly (GA) is the main deliberative, policymaking and representative organ of the United Nations. It comprises all 193 members of the United Nations and gives all member nations equal representation. The GA meets in regular session from September to December each year, and votes on the resolutions brought forth by the member states. GA resolutions are generally non-binding on member states. See: http://www.un.org/en/ga/.

[507] On the signature and ratification status of the TOC Convention, see http://www.unodc.org/unodc/en/treaties/CTOC/signatures.html. [Accessed 29 April 2012]

The TOC Convention enables MLA between countries and signifies the need to foster close law enforcement cooperation and promote training and technical assistance. Under the provision of the TOC Convention, the signatories shall develop or improve training for law enforcement personnel to deal with the methods for combating the misuse of computers or telecommunication networks (Art. 29.1 (h)). The TOC Convention also expressly requires capable states to provide assistance for developing countries in planning and training work for dealing with cybercrimes (Art. 29.2).

Detailed and comprehensive provisions with respect to MLA can be found in Art. 18, which provides that states may seek assistance related to: taking evidence or statements from persons; executing searches and seizures; examining objects and sites; providing evidentiary items and documents; and identifying or tracing the proceeds of crime (Art. 18.3). Art. 27 deals with law enforcement cooperation which asks the member states to establish channels of communication between the legal enforcement authorities, to provide necessary items for analytical or investigative purposes, and to assist in identifying the suspected person and moving the equipment used for committing the offences covered by this Convention. Additionally, the Convention requires its member states to promote the exchange of personnel and other experts, including liaison officers and the exchange of information with regard to the methods used by organized criminal groups and measures for the early identification of the offences. States are encouraged to establish bilateral or multilateral agreements or arrangements based on the TOC Convention or to make full use of the existing agreements or arrangements to enhance the cooperation between their law enforcement agencies (Art. 27.2).

The states that ratify this instrument commit themselves to creating several domestic offences, including participation in an organized criminal group (Art. 5), money laundering (Art. 6), corruption (Art. 8) and the obstruction of justice (Art. 23)[508] as well as serious crimes. 'Serious

[508] See: http://www.unodc.org/unodc/en/treaties/CTOC/.

crime' is broadly defined in the TOC Convention as conduct which is transnational in nature, involves an organized criminal group (Art. 3.1. (b)) and attracts a penalty of four or more years' imprisonment (Art. 2 (b)). An 'organized criminal group' means a group which consists of three or more persons and exists for a period of time in an attempt to commit serious crime in order to obtain financial or other material benefits (Art. 2 (a)). An offence is transnational in nature if it is (a) committed in more than one State; (b) committed in one State but prepared, directed or controlled in another State; (c) committed in one State but involving an organized group that engages in cross-border criminal activities; or (d) committed in one State but has substantial effects in another State (Art. 3.2).

Although the TOC Convention is not specially designed for the regulation of cybercrime, it is a highly relevant global instrument which addresses the cybercrimes carried out by criminal networks in relation to serious crime.[509] Most cybercrime qualifies as serious crime, as such offences usually involve at least three or more actors, affect more than one country, and are committed in an attempt to obtain financial or material benefits. INTERPOL (ICPO-INTERPOL, International Criminal Police Organization) has also indicated an emerging trend of organized syndicates comprising criminally minded technology professionals who work together and pool their resources and expertise.[510]

The TOC Convention can be applicable in cases of phishing that are operated by organized rings and involve different jurisdictions. In most cases, a phishing group is formed by members from multiple countries, as it does not require much physical contact and can rely solely on Internet communication, for example, chat rooms or instant messages, to frame the plans and co-ordinate their activities. Following the development of anti-phishing techniques, the attacking tactics of

[509] Broadhurst (2006), op. cit.

[510] See: http://www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp.

phishing have been continually refined and sophisticated. A phishing attack may be operated by a single person, but is now more likely to be exercised by a group of people who may largely promote the effectiveness of the attack through sharing the workload. A phishing organized group may include a person who creates a fake website, a spammer who sends scam emails, and another person who moves money from the victim's bank account or abuses the victim's identification information for subsequent criminal purposes. It may include only a few people or a large number of actors. For example, on 17 October, 2009, the FBI arrested nearly 100 people in the U.S. and Egypt as part of Operation Phish Phry, which targeted U.S. banks and stole online banking information from hundreds and possibly thousands of account holders. According to the FBI's statement, this was the largest phishing group that has been uncovered to date and its members contained American residents from three states as well as Egyptian citizens.[511]

Although the TOC Convention provides a comprehensive framework for MLA, it gives a requested state discretion to decline to render MLA on the ground of the absence of dual criminality (Art. 18.9). However, as the legislation has not been fully developed in many countries in the area of phishing, the above provision may be used by states to refuse the request for legal assistance, which might enable organized phishing groups to abuse the legislation inconsistency existing in certain countries in order to impede cross-border cooperation over legal enforcement.

6.3.2.2. Council of Europe Convention on Cybercrime

[511] FBI (2009), 'Operation Phish Phry - Major Cyber Fraud Takedown', *FBI*. <http://www.fbi.gov/news/stories/2009/october/phishphry_100709>, accessed September 10 2014.

Overview

The Council of Europe (the CoE) first examined the issue of computer-related crime in 1985, with the establishment of an expert committee. This committee introduced a guideline on national legislation, which was later endorsed in a Recommendation by the Council of Ministers in 1989,[512] containing a "minimum list of offences necessary for a uniform criminal policy",[513] which outlined eight offences seen as critical computer misuse requiring criminalization, including gaining unauthorized access to a computer system or network by infringing security measures. In addition, this Recommendation included an "optional list" of four offences,[514] which did not reach a consensus among the member states but were thought worthy of consideration, including computer espionage which acquires commercial secrets without right or any other legal justification by improper means with the intent either to cause economic loss to another person or to gain an unlawful economic profit.

However, CoE Recommendations are not legally binding and can only have a limited effect. Based on the recognition of the need for a harmonized response between different countries to combating cybercrime and the belief that an effective fight against cybercrime requires rapid, well-functioning international cooperation over criminal matters,[515] the CoE European Committee on Crime Problems set up a committee of experts in 1996 to draft the Convention on Cybercrime, signed in Budapest late in 2001 and coming into force in July 2004. As of August 2014, the CoE Convention

[512] Recommendation No. R. (89) 9.

[513] It includes computer fraud, computer forgery, damage to computer data or computer programs, computer sabotage, unauthorized access, unauthorized interception, unauthorized reproduction of a protected computer program and unauthorized reproduction of a topography.

[514] The optional list included the alteration of computer data or computer programs, computer espionage, unauthorized use of a computer and unauthorized use of a protected computer program.

[515] See the Preamble of the Council of Europe Convention on Cybercrime, http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

on Cybercrime has been signed by fifty-three countries and ratified by forty-two.[516]

The Convention is the first and the only binding international instrument to deal with crimes committed via the Internet and other computer networks. It presents a significant step forward in fighting cybercrime as it commits the ratifying countries to prosecute computer-related crime more vigorously. The Convention is not a regional treaty, as it is open for signature by non-member countries which participated in the development of the Convention. It currently has four non-member signatories, including the United States, Canada, Japan and South Africa, but has only been ratified by the United States and Japan. The fact that it only has two non-European ratifying nations suggests that it cannot at present be described as a global convention, but it nevertheless has global significance and provides a fundamental guide for many countries outside Europe in formulating their national laws on cybercrime. However, critics also argue that the countries that participate in the Convention and abide by its mandates are not the countries where legal enforcement is in greatest demand.[517]

Objective and Structure

The main objective of the CoE Convention on Cybercrime (hereinafter, the Convention), as set out in the preamble, is to pursue a common criminal policy to protect society against cybercrime by harmonizing the relevant legislation at the national level and fostering effective international cooperation. To achieve this, the CoE adopts the approach of: laying down certain criminal offences to harmonize the national laws in order to eliminate problems of dual criminality; defining a common set of procedural powers in order effectively to investigate and prosecute cybercrime

[516] See the status of signature and ratification to the Convention, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG.

[517] Archick, Kristin (2005), 'Cybercrime: The council of Europe convention', *Congressional Research Service Report (CRS Report for Congress)*. <http://mail.iwar.org.uk/news-archive/crs/10088.pdf>, accessed September 19 2014.

offences; and providing arrangements for fast and reliable international cooperation.

The Convention consists of four chapters. Chapter I defines the terms used by this treaty. Chapter II includes a list of crimes – nine are mentioned in the Convention – that each signatory must incorporate into their domestic laws. The Convention also sets out certain procedural mechanisms which the signatories are required to implement within their laws, including granting the power to the law enforcement authorities to compel an Internet Service Provider to monitor a person's online activities. Chapter III establishes a framework of cooperation and calls upon the signatories to provide international cooperation to the widest extent possible in the investigation and prosecution of cybercrime offences or the collection of evidence. The law enforcement agencies of each signatory are obligated to assist the police from other participating countries to respond to their mutual assistance requests. The final chapter includes miscellaneous provisions common to most CoE treaties.

Offences

The Convention obligates the signatories to criminalize nine offences in four categories. The first category addresses an "offence against the confidentiality, integrity and availability of computer data and systems", including illegal access to a computer system (Art. 2), the illegal interception of non-public transmissions of computer data to, from or within a computer system (Art. 3), interference with computer data (Art. 4), interference with a computer system (Art. 5), and the misuse of devices or computer passwords to access a computer system, including the production, sale, procurement for use, import, distribution or possession of such devices or passwords (Art. 6). The second category, "computer-related offences", covers the traditional offences of forgery and fraud when committed through the input, alteration, deletion, or suppression of computer data or through interference with a computer system (Art. 7 and 8). “Content-related offences” calls for the criminalization of offences related to child pornography (Art. 9). This is supplemented by an additional protocol[518] adopted in November 2002, making it a criminal offence to disseminate racist and xenophobic material through computer systems. The fourth category criminalizes offences related to the infringement of copyright and related rights.

Jurisdiction and Procedural Powers

The Convention addresses the question of jurisdiction in relation to cybercrime offences, including the case of multiple jurisdictions and the way to solve jurisdictional conflicts. Art. 22 establishes criteria based on the principles of territoriality (Art. 22.1 (a)-(c)) and nationality (Art. 22.1 (d)), under which the contracting parties are obligated to establish jurisdiction over the criminal offences in the Convention. Each Party is required to punish the commission of the criminal offences enumerated in Art. 2-11 that are committed in its territory. This allows a participating state to assert jurisdiction regarding a computer crime involving a computer system within its territory, even if the perpetrator committed the offence outside the territory of the state.[519] The provision also grants a state jurisdiction over a national of that state who committed the offences laid out in the Convention outside the state boundaries, provided that the said conduct also constitutes an offence under the domestic law of the state where it was committed or the conduct occurred outside the territorial jurisdiction of any contracting state.[520] In cases when more than one state has jurisdiction over an offence, the states involved shall consult with each other to determine the proper avenue for prosecution (Art. 22.5).

[518] For the full text of the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist or xenophobic nature committed through computer systems, see: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

[519] See the Explanatory Report to the Convention on Cybercrime, http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm, para. 233.

[520] Ibid, para. 236.

For procedural legal issues, the Convention requires the participating states to establish a minimum set of procedural tools whereby the legal enforcement agencies have procedural powers to conduct certain investigative measures specific to cybercrime offences. The procedural powers provided by the Convention include: common procedural rules (Art. 14 and 15), traditional measures such as the search and seizure of computer data (Art. 19) and new measures such as the expedited preservation of computer data (Art. 16) and expedited preservation and partial disclosure of traffic data (Art. 17). Additional evidence collection measures such as the real-time collection of traffic data (Art. 20) and interception of content data (Art. 21) are also adapted by the Convention to include the collection of electronic data in the process of communication.

International Cooperation and Mutual Assistance

The Convention establishes three general principles of international cooperation (Art. 23). First, it requires that international cooperation is to be provided among contracting states "to the widest extent possible". Thus, the states are required to provide extensive cooperation to each other and to minimize any obstacles to the rapid flow of information and evidence.[521] Second, the scope of the obligation to cooperation extends not only to the crimes set forth in this Convention, but also to all criminal offences related to computer systems and data, as well as to offences involving the collection of electronic evidence. Accordingly, provisions for international cooperation are applicable, whereby a crime is committed by using a computer system or where an ordinary crime is not committed by using a computer system but involves electronic evidence.[522] Finally, the international cooperation provisions do not supersede the preexisting provisions of international

[521] Ibid, para. 242.
[522] Ibid, para. 243.

agreements on these issues.[523]

The Convention establishes general principles for mutual assistance (Art. 25) and also makes it possible for a state to request mutual assistance at the international level regarding the expedited preservation of stored computer data (Art. 29), the expedited disclosure of preserved traffic data (Art. 30), the accessing of stored computer data (Art. 31), the real time collection of traffic data (Art. 33), and the interception of content data (Art. 34). Although the Convention permits trans-border access to stored computer data without the authorization of another state, such investigations are only allowed when accessing publicly available data or when the state obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data (Art. 32). It is worth nothing that the Convention does not see dual criminality as a prerequisite condition for the purpose of preserving computer data. Preservation, as foreseen by the drafters of the treaty, is not particularly intrusive and should be undertaken rapidly without unnecessary bureaucracy because electronic evidence is easily deleted, removed or altered within a very short time.[524]

Application to the case of phishing

All of the ratifying countries are required to criminalize certain computer-related offences (Art. 2-8), if they have not already done so. The following provisions are especially relevant to the case of phishing.

> Illegal Access (Art. 2):
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its criminal law, when committed

[523] Ibid, para. 244.

[524] Ibid, para. 285.

> internationally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

This provision adopts a broad approach of the criminalization of the offence of an attack against the security of computer systems and data, such as hacking, cracking or computer trespass. It aims to protect the interests of organizations and individuals to manage and control their system without unauthorized disturbance and intrusion. The term 'access' does not depend on a specific method[525] and includes the entering of the whole or part of a computer system which contains hardware or stored data. This provision is applicable when a phishing perpetrator invades computer systems to acquire data directly through the infection of a computer or related devices with malware.

> Illegal Interception (Art. 3):
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its criminal law, when committed internationally, the interception without right, made by technical means, of non-public transmission of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intention, or in relation to a computer system that is connected to another computer system.

This provision criminalizes the violation of the right of privacy in respect of data communication, as the traditional taping and recording of oral conversations between persons. The Explanatory Report points out that the provision covers the communication process taking place within a computer system[526] and applies to all forms of electronic data transfer, such as transfer by telephone, fax,

[525] But the mere sending of an email or file to that system does not constitute 'access'. See the Explanatory Report to the Convention on Cybercrime, http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm, para. 46.

[526] "The communication in the form of the transmission of computer data can take place inside a single computer

email or file transfer. To avoid over-criminalization, this provision requires that the interception needs to be carried out by 'technical means' in relation to the listening to, monitoring or surveillance of the content of communication, either through accessing the computer system or through employing electronic eavesdropping or tapping devices.[527] Technical means may include the use of software, passwords and codes. It hence does not cover acts of social engineering in the absence of the use of technical means. Under this provision, the offence of illegal interception would be committed where a phishing attacker intercepts the keystroke activities of an individual by technically installing a keylogger program onto the victim's computer.

> Computer-related forgery (Art. 7):
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its criminal law, when committed internationally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it was authentic, regardless whether or not the data is directly readable or intangible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

In order to protect the security and reliability of electronic data, this Convention provides a parallel offence to the forgery of tangible documents. It aims to fill the gaps in the criminal law relating to the traditional forgery provisions that might be inapplicable to electronically stored data.[528] The 'input' of data corresponds to the production of a false tangible document[529] and the subsequent acts enumerated in Art. 7 correspond to the falsification of an authentic document. This provision is especially relevant to email-based phishing scams and can be used to prosecute the creation of

system (flowing from CPU to screen or printer, for example), between two computer systems belonging to the same person, two computers communicating with one another, or a computer and a person (e.g. through the keyboard)" Ibid, para. 55.

[527] Ibid, para. 53.

[528] Ibid, para. 81.

[529] Ibid, para. 84.

fraudulent emails designed to perpetrate phishing attacks.

> Computer-related fraud (Art. 8):
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its criminal law, when committed internationally and without right, the causing of a loss of property to another person by:
>
> a. any input, alteration, deletion or suppression of computer data;
>
> b. any interference with the functioning of a computer system,
>
> with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Financial gain has been the priority target in most phishing attacks. This can be achieved by money transfer or credit card fraud after phishing perpetrators obtain credit card details or banking information from their victims. The Convention makes it an offence to manipulate computer data or a computer system in the course of data processing which results in a loss of property to another person, with the intent to procure economic benefits for oneself or for another person fraudulently or dishonestly (Art. 8). The manipulation of data includes 'input', 'alteration', 'deletion' or 'suppression'. The offence of computer fraud is only constituted if the manipulation of data produces a loss of property to another person. The term 'loss of property' is broadly defined as any loss of money, tangibles and intangibles, with an economic value.[530]

However, given the various possibilities of how phishing perpetrators can obtain sensitive data, it is necessary to point out that not all possible acts of phishing are covered by the Convention. The Convention deals with the preparatory phase of phishing – the falsification of scam emails (Art.7), access to a computer system which is usually accompanied by a malware attack (Art.2), the

[530] Ibid, para. 88.

acquirement of information by intercepting communication through technical means, a keylogger program for example (Art.3), and the possible fraudulent use subsequent to obtaining the information (Art.8). Nevertheless, it does not cover the act which is most closely related to phishing – a social engineering attack. Phishing is usually performed by a social-engineering scheme by masquerading as a trustworthy person or entity through a seemingly electronic communication in order to lure the victim to a counterfeit website or to use software tools to automate an attack. The nature of a social engineering attack is the key element which makes phishing perpetrators different from other cyber criminals, such as hackers or crackers. To ensure the elimination of safe havens for phishing and coordinate the cross-border prosecution and investigation of phishing attackers, a review to close the gaps in the Convention on the criminalization of phishing should be given careful, favourable consideration.

6.4. Global and regional approaches to combating identity-related crime

In order to tackle the rise in the new forms of offences which abuse information technology, significant efforts have been made by several international organizations to coordinate actions against cybercrime. This section examines the work of the United Nations, OECD, G8 and APEC that has been developed to combat cybercrime, with a particular focus on identity-related crime and phishing, where appropriate.

6.4.1. United Nations

The General Assembly adopted Resolution 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on combating the criminal misuse of information technologies. In Resolution 55/63,[531] the General Assembly noted a number of similar values in the G8 10-Point Action Plan of 1997 and

[531] Full text of the Resolution 55/63, see: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

invited the States to take into account the measures identified in the resolution in their efforts to combat the criminal misuse of information technologies. This Resolution emphasized that "legal systems should protect data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized". It also stressed that the development of solutions against the criminal misuse of information technologies needs to "take into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse".

The Bangkok Declaration on "Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice",[532] endorsed by General Assembly resolution 60/177 of 16 December 2005, underlines the crucial importance of tackling document and identity fraud in order to curb organized crime and terrorism. This Declaration called on States to "*improve international cooperation to combat document and identity fraud, in particular the fraudulent use of travel document, through improved security measures, and encourage the adoption of appropriate national legislation*".

Given the increasing problems related to fraud and other illicit activities caused by taking and misusing personal identifying information, the United Nations Economic and Social Council (ECOSOC)[533] adopted a resolution (2004/26)[534] on international cooperation over the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes in 2004. In order to facilitate legal enforcement against fraud, the misuse and falsification of identity, the ECOSOC encouraged States to adopt the following measures:

[532] UN (2005), 'Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice', (Bangkok, Tailand: The 11th UN Congress on Crime Preventation and Criminal Justice).

[533] The United Nations Economic and Social Council (ECOSOC) is a principal organ for coordinating economic, social and related work, and serves as a central forum for discussing international economic and social issues. For more details, see: http://www.un.org/en/ecosoc/.

[534] For the full text of the Resolution 2004/26, see: http://www.un.org/en/ecosoc/docs/2004/resolution%202004-26.pdf.

- To facilitate the identification, tracing, freezing, seizure and confiscation of the proceeds of fraud and the misuse and falsification of identity; and
- To cooperate with one another in an effort to prevent and combat fraud and the misuse and falsification of identity.

In addition, this Resolution requested the Secretary-General to convene an intergovernmental expert group to prepare a study on fraud and the criminal misuse and falsification of identity. States were invited to cooperate with and assist the intergovernmental expert group in its work and make voluntary contributions to support the intergovernmental expert group and facilitate the participation of experts from developing countries.

Pursuant to the above ECOSOC resolution, UNODC commissioned a study on "International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crime" which was released in 2007.[535] This study suggested that only six States reported that they had criminalized, in whole or part, the transfer, possession or use of another person's identification or identity information or of a false identity in connection with another crime. It is worth noting that this study also pointed out the application gap between the existing criminal provisions and certain identity-related crimes, including phishing. It indicated that the existing theft offences may not always be applicable where intangible information may not be seen as property and where such information is taken from open sources. In addition, the existing offences of economic fraud may only be applicable in the case of phishing if the identity information that has been taken by deception has value.

In ECOSOC resolution 2007/20,[536] States were encouraged to establish or update criminal offences

[535] The UNODC's study contained the result of the study on identity-related crime, which was submitted to the Commission on Crime Prevention and Criminal Justice at its sixteenth session (E/CN.15/2007).
[536] For the full text of the Resolution 2007/20, see:

related to the illicit taking, copying, fabrication and misuse of identification documents and identification information. This resolution requested the UNODC to provide legal expertise or other forms of technical assistance to Member States in reviewing or updating their laws dealing with transnational fraud and identity-related crime. It also encouraged the promotion of mutual understanding and cooperation between public and private sector entities to bring the various stakeholders together and facilitate the exchange of views and information among them.

6.4.2. OECD

In 1998, the OECD Committee on Consumer Policy started to develop a set of general guidelines to protect electronic commerce which was approved by the OECD Council in 1999. The *1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* (the 1999 Guidelines)[537] represented a recommendation to governments, businesses, and consumers about effective consumer protection for electronic commerce. In 2003, the OECD developed another guideline in respect of cross-border fraud (the 2003 Guidelines).[538] These two Guidelines do not explicitly deal with an approach to how to criminalize identity theft but they set out the principles and serve as a solid basis for establishing a framework and strategies for effectively investigating and prosecuting online identity theft and other fraud.

In 2008, the OECD published the 'Scoping Paper on Online Identity Theft'[539] which provides a detailed analysis of the characteristics of identity theft and different online identity theft scams, as well as dealing with aspects of victims and law enforcement schemes. The term 'identity theft' is

http://www.unodc.org/documents/organized-crime/ECOSOC_resolution_2007_20.pdf.

[537] OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, available at: http://www.oecd.org/dataoecd/18/13/34023235.pdf.

[538] OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, available at: http://www.oecd.org/document/56/0,3343,en_2649_34267_2515000_1_1_1_1,00.html.

[539] Scoping Paper on Online Identity, Ministerial Background Report, DSTI/CP(2007)3/FINAL, available at: http://www.oecd.org/dataoecd/35/24/40644196.pdf.

defined in this paper as:

> ID theft occurs when a party acquires, transfers, possesses, or uses the personal information of a natural or legal person in an unauthorized manner, with the intent to commit, or in connection with, fraud or other crimes.

This definition applied to both individuals and legal entities, but was limited to identity that affects consumers. Phishing is regarded as the dominant method which enables the commission of ID theft.[540] In section II 'Online ID Theft Toolkit', this paper makes specific address to phishing techniques and phishing's evolution and trends. In the same year, the OECD also released the 'Policy Guidance on Online Identity Theft'.[541] This guidance provides an overview about responding to the initiatives regarding online identity theft, particularly focusing on the ways of enhancing the awareness of consumers, businesses and governments and improving data security through the use of education.

6.4.3. The Group of Eight (G8)

The Group of Eight (G8) is a forum for the governments of eight of the world's largest industrialized economies, comprising Canada, Germany, France, Italy, Japan the United Kingdom, the United States and Russia. It originated with a 1975 summit hosted by France and was originally established to co-ordinate economic policy; it nevertheless has also developed initiatives for dealing with international crime. At the Halifax Summit in 1995, the G7 established a senior experts group (the 'Lyon Group') to address measures for combating transnational organized crime. At the following summit held in Lyon in 1996, the Lyon Group released 40 recommendations (also known

[540] OECD (2006), *OECD Anti-Spam Toolkit of Recommended Policies and Measures* (OECD Publishing).

[541] OECD Policy Guidance on Online Identity Theft, 2008, available at: http://www.oecd.org/dataoecd/49/39/40879136.pdf.

as the 'Lyon Recommendations')[542] which aimed at promoting the efficiency of collective action against transnational organized crime by strengthening the investigation and prosecution powers for high-tech crime and enhancing a cross-border cooperation regime in related criminal matters.[543]

To improve the implementation of the 40 Recommendations, the Lyon Group's 'High-Tech Crime Subgroup' was set up in 1997. During the meeting in Washington D.C. in that year, the G8 Justice and Home Affairs Ministers adopted a set of principles and a 10-point Action Plan which was endorsed by the G8 Birmingham summit in May 1998 to ensure there were no "safe havens" for criminals who abuse information technologies. These principles included:

- The investigation and prosecution of international high-tech crimes must be coordinated among all concerned States.
- The legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.
- To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.

One of the practical achievements of the work done by the experts group has been the creation of the G8 24/7 High Tech Crime Network (G8 24/7 Network) in 1997 which requires the participating countries to establish contact points permitting the sharing of information on ongoing investigations against cyber criminals. This idea of a 24/7 Network has been picked up by a number of international approaches in the fight against cybercrime. One example is the CoE's Convention on Cybercrime (Art. 35).[544]

[542] For the full text of the Senior Experts Group Recommendations, see: http://www.g8.utoronto.ca/crime/40pts.htm.
[543] Broadhurst (2006), op. cit.
[544] Further discussion of the 24/7 Network features in the subsequent section.

At the Ministerial Conference in Moscow in 1999, the G8 specified their plans regarding the fight against high-tech crimes which called for the development of a dialogue and effective cooperation between the government and industry and a comprehensive response, including crime prevention, investigation, and prosecution relating to Internet Fraud.[545] A mass of G8 discussions which were undertaken on the ministerial levels in the later 1990s served as a bridge between the summits and the experts and incorporated expert recommendations into statements that were then adopted by the G8 countries.[546]

In May 2004, the G8 Ministers issued a joint communiqué at a meeting in Washington stating that, "all countries must continue to improve laws that criminalize misuses of computer networks and that allow for faster cooperation of Internet-related investigations". The communiqué also emphasized that, with the activation of the CoE's Convention on Cybercrime, the states should take steps to "encourage the adoption of the legal standards it contains on a broad basis".[547] During the 2006 Moscow Meeting, the G8 Justice and Home Affairs Ministers discussed issues related to the effective countermeasures against IT terrorism and terrorists who act in the sphere of high technologies, which encompassed the work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs.[548]

At the Deauville summit in 2011, the heads of the G8, for the first time, discussed the issue of the Internet. The G8 leaders acknowledged the importance of the Internet especially in prompting freedom, democracy and human rights, and also recognized the role of governments, the private

[545] The Communiqué of the Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, held in Moscow, October 19-20, 1999, see: http://www.g8.utoronto.ca/adhoc/crime99.htm.

[546] Gstöhl, Sieglinde (2007), 'Governance through government networks: The G8 and international organizations', *The Review of International Organizations,* 2 (1), 1-37.

[547] The Communiqué of the Meeting of G8 Justice and Home Affairs Ministers, held in Washington, May 11, 2004, see: http://www.g7.utoronto.ca/justice/G8justice2004.pdf.

[548] Press Conference on the Result of the G8 Justice and Home Affairs Ministerial, held in Moscow, 16 June, 2006, see: http://www.g7.utoronto.ca/justice/justice2006.htm.

sector, users, and other stakeholders in creating an environment for underpinning the development of a flourishing Internet in a balanced manner.[549] During the summit, the G8 agreed on a number of key principles including "*freedom, respect for privacy, multi-stakeholder governance, cyber-security, and protection from crime*".[550]

The E-G8 Forum (the eG8) was held in Paris on 24-25 May, 2011, two days prior to the Deauville summit, to discuss and propose a series of initiatives on the Internet within the context of global policy. The eG8, convened by the former French President Nicolas Sarkozy, invited the G8 leaders and the executives of global technology industries, including Google, Facebook, Amazon and eBay, to debate a wide range of key themes involving the Internet, including support for innovation, the future development of the Internet, the freedom of networks, the protection of personal data from cybercrime, the protection of minors, and the impact on a variety of fields such as economic growth, job creation, democracy, government administration, education, news and health.[551]

This was the first time that the issue of the Internet had been included on the agenda of a meeting at such a high political level. The eG8 provided an opportunity for the policymakers and figures from the technology industries to converse about certain important issues relating to the Internet. However, due to their different positions, the two-day discussion manifested a tension between the technologists and policymakers and created a vivid debate between the more traditional content industry and new businesses that develop new services on the basis of the Internet, particularly over the protection of intellectual property rights.[552] In general, while the G8 leaders tended to wish to

[549] G8 Declaration: Renewed Commitment for Freedom and Democracy, released on May 27, 2011, see http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html.

[550] G8 Declaration: Renewed Commitment for Freedom and Democracy, released on May 27, 2011, see http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html.

[551] E-G8 Forum, Press Release, Paris, 30 May, 2011, see: http://www.g8.utoronto.ca/summit/2011deauville/eg8/eg8-closing.pdf.

[552] Blanco, Carlos L. (2011), 'The eG8 Summit in Paris – a step forward for global Internet and broadband policy', *Telefonica*. <http://www.publicpolicy.telefonica.com/blogs/blog/2011/06/07/the-eg8-summit-in-paris-%E2%80%93-a-step-forward-for-global-internet-and-broadband-policy/>, accessed September 8 2014.

step up the governance and strengthen the regulation of the Internet to deal with the problem of digital piracy, the representatives of the technology industries preferred a technological solution; for example, placing a limitation on the capacity of video traffic and bandwidth-heavy content passing through the telecommunications networks, rather than regulatory solutions.[553] The communiqué of the first eG8 outlined the key notions of the discussion which were: "*protect, without constraining; regulate, without adulterating the fundamental liberty on which the Internet has been built*".[554]

6.4.4. APEC

Although founded for the purpose of promoting economic growth and trade among the member economies, how to effectively protect economic development against the threat of cybercrime has also become an urgent issue in the discussions of the APEC over the past decade. After the 9/11 attack on the U.S. in 2001, the APEC leaders issued a Statement on Counter-terrorism which condemned the terrorist attack and considered it imperative to reinforce collaboration in different respects to combat terrorism.[555]

At a meeting held in Los Cabos, Mexico, in October 2002, APEC's leaders, addressing the threat of terrorism and the importance of enhancing the cyber security infrastructure, collectively committed to:[556]

a. Enact a comprehensive set of laws relating to cyber security and cybercrime which imitates

[553] Pfanner, Eric (2011), 'G-8 Leaders to Call for Tighter Internet Regulation', *New York Times*. <http://www.nytimes.com/2011/05/25/technology/25tech.html?_r=2&>, accessed September 17 2014.

[554] Press release of eG8, 30 May, 2011, see: http://www.g8.utoronto.ca/summit/2011deauville/eg8/eg8-closing.pdf.

[555] APEC Leaders Statement on Counter-terrorism, APEC Economic Leaders' Meeting, held in Shanghai, 21 October, 2001. See: http://www.apec.org/About-Us/About-APEC/~/~/media/Files/LeadersDeclarations/2001/01_ldrs_counterterror.ashx.

[556] The full text of the APEC Leaders' Statement on Fighting Terrorism and Promoting Growth in Los Cabos, Mexico, on 26 October, 2002 is available at: http://www.apec.org/Meeting-Papers/Leaders-Declarations/2002/2002_aelm/statement_on_fighting.aspx.

UN GA Resolution 55/63 and the CoE's Convention on Cybercrime;

b. Identify national cybercrime units and international high-technology assistance contact points; and

c. Establish institutions that exchange threat and vulnerability assessment, such as Computer Emergency Response Teams (CERTs).

APEC's Telecommunications and Information Working Group (TEL),[557] established in 1990, has been actively participating in APEC's projects to strengthen the capacity of the APEC member economies for dealing effectively with cybercrime. In 2002, the APEC Ministers endorsed the APEC Cybersecurity Strategy[558] which was developed by the TEL as a response to the call from the leaders to combat cybercrime and strengthen the critical infrastructure protection. The APEC Cybersecurity Strategy stressed the importance of a legal framework on cybercrime and encouraged APEC economies to adopt, develop and report on their comprehensive, substantive, procedural and mutual assistance laws and policies. It also highlighted the work of information sharing and cooperation, security and technical guidelines, public awareness, training and education and wireless security as the basis for APEC's efforts with regard to cybercrime.

To respond to the increasing misuse of the online environment through spam, identity theft, and fake websites which undermine the potential economic and social benefits by eroding the trust and confidence in the security of the online environment, the TEL adopted the APEC Strategy to Ensure A Trusted, Secure and Sustainable Online Environment[559] in 2005, which expanded APEC's work

[557] The TEL is one of the APEC working groups which aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing telecommunications and information policies. The work of the TEL is conducted through three steering groups: Liberalization Steering Group, ICT Development Steering Group and Security and Prosperity Steering Group. See: http://www.apec.org/Home/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.

[558] For the full text of APEC Cybersecurity Strategy, see: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf.

[559] For the full text of APEC Strategy to Ensure A Trusted, Secure and Sustainable Online Environment, see: http://www.apec.org/Home/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Gro

on combating cybercrime, promoting information and network security and harmonizing frameworks for securing transactions and communication, and identified seven action item areas for promoting online security. The Strategy recognized the important roles of government, industry, academics and others in ensuring a trusted and secure online environment and emphasized the need to raise users' awareness of online security. In addition, it encouraged its member economies to ensure their legal and policy frameworks by addressing the threat posed by the misuse of the online environment.

The U.S. proposed a project in the APEC e-Security Task Group of the TEL and organized a conference on 21-25 July, 2003 in Bangkok, Thailand. Attended by over 120 delegated from 17 economies, this conference had three main objectives: to assist economies to develop the necessary legal frameworks for combating computer crime; to promote the development of the investigative capacity of the law enforcement units; and to enhance cooperation between the private and public sectors in addressing the threat of computer crime.[560] This conference primarily focused on the issue of how to build a comprehensive legal framework to combat cybercrime in terms of establishing: substantive laws that criminalize conduct such as unauthorized access to a computer system; procedural laws for the collection of electronic evidence; and laws and policies that allow the cooperation of the member economies in the investigation and prosecution of cybercrime. In addition, the expert present agreed that the CoE Convention on Cybercrime serves as a valuable model for improving the domestic law on cybercrime.

In 2005, the sixth APEC Ministerial Meeting on the Telecommunications and Information Industry passed the Lima Declaration, which encouraged "*all economies to study the Convention on Cybercrime and to endeavor to enact a comprehensive set of laws relating to cybersecurity and*

ups/~/media/Files/Groups/TEL/05_TEL_APECStrategy.ashx.

[560] APEC, Conference on the Strengthening International Law Enforcement Cooperation to Prosecute Cyber Criminals, Hackers, and Virus Authors, News Release, Bangkok, 25 July, 2003. See: http://apec.org/Press/News-Releases/2003/0725_tha_strengthening_law.aspx.

cybercrime that are consistent with international legal instruments, including UN General Assembly Resolution 55/63 and the Convention on Cybercrime"[561] In September of that year, APEC TEL organized a Conference on Cybercrime Legislation, stating that the TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project would support the member economies to implement new cybersecurity laws.

Although APEC has endeavoured to enable its Member economies to adopt a set of unified legal standards against cybercrime on the basis on the Convention on Cybercrime and UN Resolution, the progress has not been very satisfactory due to the huge inconsistencies among its members. While some economies within the APEC have claimed that their laws have been or will be consistent with the Convention on Cybercrime, many other countries have quite different legal systems or even no cybercrime laws at all.[562] Taiwan, for example, took the CoE's Convention on Cybercrime as an important referral model for drafting a specific chapter of computer-related offences which was added to their Criminal Code in 2003. While nearly every article of the substantive laws set forth in the Convention was adopted in the Taiwanese Criminal Code, the procedural laws of the Convention were overlooked and have not been incorporated into the Taiwanese legislation to date.

6.5. 24/7 network

Cybercrime investigations are often time-sensitive, as traffic data are often deleted within a rather short period of time and related evidence can disappear quickly.[563] Nevertheless, traditional legal methods for obtaining cross-border evidence often cannot keep up with the need for rapid

[561] Art. 32 of Lima Declaration, the 6th APEC Ministerial Meeting on the Telecommunications and Information Industry, 1-3 June, 2005, Lima, Peru. See: http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2005_tel.aspx.

[562] Li, Xingan (2007), 'International actions against cybercrime: Networking legal systems in the networked crime scene', *Webology,* 4 (3), 1-45.

[563] Brenner and Schwerha Iv (2001), op. cit.

cybercrime investigations. To this end, the establishment of 24/7 contact points has been the consensus reached in most international approaches against cybercrime to enable countries to network with authorities in other countries and request immediate reaction and assistance in cybercrime investigation and evidence collection.

As aforementioned, the G8 created a new mechanism to expedite contacts between countries in 1997. The G8 24/7 High Tech Crime Network (HTCN) is an network which provides around-the-clock, high-tech expert contact points, which permits the sharing of information on ongoing investigations against cyber criminals.[564] The CoE Convention, based on experience gained from the existing network created by the G8, also creates the legal basis for an international cybercrime assistance network – the 24/7 network – which supplements the existing channels of police cooperation and mutual assistance to address the challenges of the computer age effectively. Under Art. 35, states are obligated to designate a point of contact available 24 hours per day, 7 days per week, in order to ensure a rapid response and immediate assistance with regard to investigations within the scope of the Convention. Each national 24/7 point is either to facilitate or directly carry out technical advice, the preservation of data, the collection of evidence, and the locating of suspects. The establishment of a 24/7 network is regarded as one of the most important means provided by the Convention of ensuring the states' effective response to the law enforcement challenges posed by computer crime.

The installation of the contact points has two main functions regarding to cybercrime investigation, including: speeding up a. the communication by providing a single point of contact; and b. investigations by authorizing the contact point to carry out certain investigations right away.[565]

[564] The overview of G8 24/7 High Tech Crime Network, see http://itlaw.wikia.com/wiki/G8_24/7_High_Tech_Crime_Network.

[565] ITU (2009), 'Understanding Cybercrime: A Guide for Developing Countries', *International Telecommunication Union Cybercrime Legislation Resources*. <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>, accessed September 7

In addition, Interpol has developed a global police communication system, known as I-24/7 to connect law enforcement officers in all member countries. I-24/7 enables authorized users to share sensitive police information and enables investigators to access INTERPOL’s criminal databases with regard to suspected criminals, stolen and lost travel documents, stolen motor vehicles, fingerprints, DNA profiles, stolen administrative documents and stolen works of arts. To ensure the information reaches the specialized police units as fast as possible, the INTERPOL compiled a list of National Central Reference Points (NCRPs) to facilitate the prevention, investigation and prosecution of cybercrime.

6.6. Conclusion

The value of legal regulation is largely dependent upon effective legal enforcement, therefore phishing, especially because of its transnational and transient nature, has posed acute difficulties in investigating and prosecuting perpetrators and resulting in weak legal enforcement. This chapter has highlighted the need for universal criminalization of phishing, international harmonization of legal standards, and integrated efforts and cooperation between legal enforcement agencies across countries for a seamless web of legal enforcement and the problems of achieving these.

Phishing, as a conduct which comprises multiple phases of acts, usually is not regarded as a stand-alone crime but is sometimes accommodated by traditional criminal actions such as spam, impersonation, theft or fraud or covered by new offences of identity theft or identity fraud. However, while some countries have undertaken legislation to develop or update the laws in relation to identity theft or identity fraud to respond to the rise of phishing, they appeared to have overlooked the distinction between phishing and these two offences in terms of the elements of acts and objects.

2014.

Phishing is similar to identity theft in the sense that they both usually involve unauthorised use of another person's identity. However, the object of identity theft is only specified for identity-related information while the object of phishing can include a variety of confidential information concerning a person, corporation or even a country. Phishing is also similar to identity fraud in the sense that they both use a false identity to defraud someone. Nevertheless, identity fraud concentrates on monetary or financial gain whereas phishing may target various sensitive information which may not necessarily have monetary value or bring financial gain. Phishing is similar to these two offences but is not equivalent to them.

International law has similar problems. The CoE Convention on Cybercrime is the first and the only binding international instrument to deal with cybercrimes. While the Convention deals with the falsification of scam emails, access to a computer system through malware, the acquisition of information by technical interception means, and the possible fraudulent use subsequent to obtaining the information, this chapter pointed out that the Convention failed to cover some social-engineering phishing conduct. The gaps in the application of the existing legislation to phishing at both national and international levels resulting from failure to identify the true context of phishing have caused loopholes in the legal protection against phishing which are likely to be exploited by phishing attackers to create safe havens. How to pursue a clear understanding and converged definition of phishing in the legal context is a fundamental question that demands substantial consideration to promote consistency and compatibility of national laws and enable effective legal enforcement.

In addition to cooperation between legal enforcement, the international frameworks against cybercrime that have been addressed in this chapter all underline the importance of cooperation and information sharing between the governments, private sectors and other stakeholders involved to effectively tackle cybercrime and ensure a secure online environment. While there has been significant progress in the development of co-operation, there is much room for improvement. A key question is whether it is adequate to rely on legislators and prosecutors to plan and implement solutions in an area highly related to social-engineering and technical subterfuge schemes in which technology, Internet service providers, and even the potential victims have critical roles. What possible solutions do we have beyond law and who are the stakeholders involved in the regulation of phishing? This is the question that will be explored in the next chapter.

CHAPTER 7 MULTI-DIMENSIONAL REGULATIONS AND TAIWAN’S ANTI-PHISHING APPROACH

Synopsis

This chapter considers a broad form of regulation over laws that have been developed in multiple dimensions, including technology, education, and institutional network through an examination of the function as well as issues raised by each category of countermeasures in combating phishing. It also looks into the development of anti-phishing framework in Taiwan, with a particular focus on the progress over the past five years. To better understand the capacity of Taiwan’s multi-regulatory scheme for phishing and how different stakeholders contribute to the anti-phishing work, the chapter provides an analysis which is primarily based on existing documentary resources and literature but supplemented by the information obtained from interviews with the key persons from various regulatory interfaces.

7.1. Introduction

A successful phishing attack, as suggested by Chapter 2, not only exposes the weakness in legal protection but also unveils the vulnerabilities existing in technical infrastructure, inadequate awareness and knowledge of information security, and weak administration of domain and websites. Chapters 4-6 have demonstrated the challenges to the effectiveness of law in the context of legal provisions and law enforcement in combating phishing. Legal solutions may be part of the answer but are not capable of adequately addressing the problem of phishing. This makes it necessary to look for a broader form of regulation covering multi-dimensional phishing countermeasures that have been developed.

The previous chapters focused on the role of legal regulation, and while this chapter also considers issues involved in the practical implementation of legal regulation, its focus is on the examination of technology, education, and institutional networking. The chapter provides an overview of the phishing countermeasures along the general process of a phishing attack and aims to investigate how each form of regulation functions as well as the problems they may experience in combating phishing.

Prior to 2010, as indicated in Chapter 3, phishing has been an issue which was discussed mostly in the technological research arena in Taiwan. The introduction of the Taiwan Anti-Phishing Working Group (APWG) and Anti-Phishing Notification Window (APNOW) in 2010 not only established a landmark in the progress of Taiwan's anti-phishing work but also manifested the ambition of Taiwan to combat phishing through joint efforts of different stakeholders across sectors. Nevertheless, this movement did not spur further research over the role of different stakeholders in current anti-phishing work. This chapter aims to shed a light on the roles of the major stakeholders in the anti-phishing community by examining their work in responding to phishing attacks and the additional efforts they can devote or are expected to devote to the fight against phishing. This is assisted by a qualitative empirical study involving in-depth interviews with key persons from various regulatory bodies, including law enforcement, NCC, ISPs, CERTs, online merchants, and information security industry to explore their work and opinions on the effectiveness of current efforts and suggestions for future work. This is a small-scale field work, but, to the best of my knowledge, it is the first study conducted in Taiwan that synthesizes the opinions of experts from different fields, and examines the anti-phishing efforts of the stakeholders.

7.2. Limitations of legal regulations relating to phishing

Legal regulations are generally regarded as a slow countermeasure in responding to computer technology crimes which usually involve swift change of tactics by increasing the sophistication and complexity of attacks, as legislation is usually created passively to respond to known cyber misconduct which may have been practised for quite a long time, by making it an offence. The criminalization of phishing conduct is always a requisite for making phishing perpetrators accountable for their conduct; however, it does not necessarily lead to the successful prosecution of phishers. Taking the example of the Taiwanese Criminal Code, prosecutors cannot indict a person who obtains confidential information performed in electronic format without authorization from the other person unless the victim makes a complaint (Art. 359, 364).[566] While the absence of the victim's compliant is probably a factor leading to the failure to prosecute, the previous chapters have demonstrated that the difficulties of identifying genuine phishing perpetrators is the main determinant of a successful prosecution.[567]

Legal regulations, as a corrective measure to deter phishing through coercion and punishment, are only made possible if they can successfully increase the risk of conviction experienced by phishing perpetrators. Nevertheless, Chapter 6 has demonstrated the huge challenges that the transnational and transient elements of phishing have posed to legal enforcement agents to track and identify real phishers.[568] The fact that only a few phishing perpetrators are arrested and prosecuted represents a major problem of the effectiveness of law and the investigative and prosecutorial agencies.[569]

[566] See Chapter 4, section 4.4.2.2.

[567] See Chapter 4, section 4.4.2.5 and Chapter 6, section 6.2.

[568] See Chapter 6, section 6.2.

[569] Sofaer and Goodman suggest that it may, on the contrary, be a mistake to give the investigative and prosecutorial agencies the main responsibility to deal with cybercrime, as the above agencies are most concerned with using information to track down and arrest criminals rather than warning users of an attack in progress or developing technological countermeasures to deter future attacks. Sofaer and Goodman (2001), op. cit.

Therefore, phishing demands a broad approach to regulation that goes beyond law, and a combined approach, as suggested by several researchers, may be the only solution to phishing.[570] It is not an option but a necessity to develop a multi-dimensional regulatory framework in order to effectively diminish phishing problem.

7.3. Multi-Dimensional Regulations for Combating Phishing

This section firstly identifies the context and coverage of the regulation of phishing and then provides an overview of the general process of a phishing attack combined with the countermeasures that have been proposed in relation to technology, education and institutional framework against each step in the process.

7.3.1. Scope of the regulations

Although law has typically served as an essential tool to constrain certain behavior in both real and virtual world, it alone is incapable of adequately addressing phishing. Lessig[571] argued that the 'Code', i.e. software and hardware, which constitute the architecture of cyberspace is a key regulator in virtual space. Reidenberg[572] also argued that law is not the only source of rule-making and put forward a notion 'Lex Informatica' which suggested that network technology itself impose rules regarding the access and use of information. A good example of regulation through technical rules is the use of cryptography to prevent unauthorized access to data. Instead of Lessig's statement

[570] Lynch (2005), op. cit;Mcnealy (2008), op. cit;Sullins (2006), op. cit;Wilson and Argles (2011), op. cit.

[571] Lessig (2006), op. cit.

[572] Reidenberg, Joel R (1997), 'Lex informatica: The formulation of information policy rules through technology', *Tex. L. Rev.,* 76, 553.

"code is law," there was another approach based on "code meets law,"[573] which suggested that law and software together determine the overall regulatory environment.[574]

Yet, a phishing attack exploits not only the vulnerability in law or technical infrastructure but also the weakness in administration of domain or websites and user's awareness of information security. Therefore this chapter argues that phishing demands a broader form of regulation which is not limited to law or technology but refers to any force which makes it possible to prevent or interrupt a phishing attack or which helps to control or mitigate the potential risk which is likely to be caused by phishing. A regulation of phishing, in this sense, can be understood as a countermeasure or a solution against phishing. It can be a piece of legislation, a software or hardware, a management system or even an educational or training programme. Appropriate regulation therefore involves not only consideration of these various forms but also their interaction.

Phishing can be constrained by increasing the costs or difficulties of performing phishing or by decreasing the probabilities of success. The costs may include time, money, or even freedom. For example, if legal rules can raise the cost of criminal activity, such as increase of penalty or jail time, to a would-be perpetrator, it may promote deterrence of that wrongdoing in the first place.[575] Technology makes it more costly and difficult to phishers to succeed by interrupting phishing attacks through detection, interference with navigation, prevention of transmission of information or rendering the stolen information useless. A close connection between victims, CERTs, and ISPs to prompt takedown of phishing sites is important to diminish potential victims and losses which in turn makes phishing less productive. Education can also deter phishing in the way that promoting users' knowledge about phishing and fostering users' awareness of information security by which not only helps them stay away from ongoing phishing attacks but also enables them to engage in

[573] Wagner, R Polk (2005), 'On software regulation', *U of Penn. Law School, Public Law Working Paper,* 57.
[574] Wagner (2005), op. cit.
[575] Katyal (2001), op. cit.

more secure online behaviours to prevent potential exploitations by phishers.

7.3.2. Overview of countermeasures against phishing

Significant research has been undertaken to develop phishing countermeasures in various areas, most of which focuses on proactive measures for detection of phishing. Several researchers provided a general overview of the different methods that have been developed against phishing.[576] Purkait[577] generated a comprehensive literature review of the available anti-phishing solutions in 2012, to determine how research has evolved in terms of quantity, content and publication outlets. Emigh[578] provided a detailed analysis of the technology employed by phishers as well as the countermeasures that can be applied along with the information flow of phishing attacks. It is considered to be very helpful to obtain a quick understanding of various phishing countermeasures by outlining the general process of a phishing attack and identifying the applicable countermeasures at each step in the process of controlling phishing. As we saw in Chapter 2, a phishing attack usually involves at least the following steps:

STEP1 Preparation: the phisher registers domain names or hacks into a legitimate website and creates a phishing website.

STEP 2 Delivery of the lure: the phisher sends scam emails to the user to tempt him/her into clicking the URL link which directs him/her to the phishing website.

STEP3 Biting the bait: the unsuspecting user follows the path set forth by the phisher to visit the phishing site.

STEP 4 Request for information: the user is prompted to enter his/her confidential information to

[576] Bose and Leung (2007), op. cit;Emigh (2005), op. cit;Hong (2012), op. cit;Huang, Tan, and Liu (2009), op. cit;Purkait (2012), op. cit.

[577] Purkait (2012), op. cit.

[578] Emigh (2005), op. cit. --- (2007), 'Phishing attacks: Information flow and chokepoints', in Markus Jakobsson and Steven Myers (eds.), *Phishing and countermeasures: understanding the increasing problem of electronic identity theft* (John Wiley & Sons), 31-64.

respond to the request of the spoof website.

STEP 5 Submission of information: the user renders the information.

STEP 6 Collection of data: the phisher assembles the target data which may be sold to a third party or personally used for subsequent fraudulent purposes.

Step 1 can be interrupted by suspending the abusive domains[579] or by forbidding the creation, transferal or possession of phishing tools for the creation of phishing websites and ensuring website security against hacking.[580] Phishing email filters[581] can help to defend against Steps 2 and 3 by preventing phishing emails from reaching users and deterring them from connecting to phishing websites. An anti-phishing toolbar[582] can hinder the process at Step 4 by warning users of the potential hazards associated with the fraudulent website that he/she is visiting. In addition, taking down phishing websites is an important countermeasure that has been largely adopted to break the chain of attack at Step 4.[583] The education of the end users[584] is a key defence to protect users against Steps 3 – 5. Proper training and education about phishing can teach users to spot phishing emails (Step 3) and identify faux websites (Step 4-5), and hence helps users to make better decisions to avoid suspicious phishing links and not reveal any confidential information. A phishing attack can be frustrated at Step 6 by the countermeasure of a component or an extension to a web browser which hides the genuine information submitted by users among bogus credentials to

[579] APWG (2008b), 'Best Practices Recommendations for Registrars'. <http://docs.apwg.org/reports/APWG_RegistrarBestPractices.pdf>, accessed September 15 2014;Konings, Marika (2009), 'Final report of the GNSO Fast Flux Hosting Working Group'. <http://gnso.icann.org/files/gnso/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf>, accessed September 20 2014;Rodenbaugh, Mike (2009), 'ICANN policy developments on abusive domain name registrations', *The IP Litigator: Devoted to Intellectual Property Litigation and Enforcement,* 15, 9-15.

[580] See Chapter 2, section 2.5.2.

[581] Abu-Nimeh et al. (2007), op. cit;Basnet, Mukkamala, and Sung (2008), op. cit;Bergholz et al. (2010), op. cit;Ceesay (2008), op. cit;Chandrasekaran, Narayanan, and Upadhyaya (2006), op. cit;Fette, Sadeh, and Tomasic (2007), op. cit;Fette, Sadeh, and Tomasic (2007), op. cit;Islam and Abawajy (2013), op. cit.

[582] Apple op. cit;Chou et al. (2004), op. cit;Google op. cit;Kirda and Kruegel (2005), op. cit;Microsoft op. cit;Netcraft op. cit.

[583] Moore and Clayton (2007), op. cit;Moore and Clayton (2008), op. cit;Moore and Clayton (2009), op. cit;Nero et al. (2011), op. cit;Netcraft op. cit.

[584] Kumaraguru et al. (2008), op. cit;Kumaraguru (2009), op. cit;Kumaraguru et al. (2009), op. cit;Kumaraguru et al. (2010), op. cit;Robila and Ragucci (2006), op. cit;Sheng et al. (2007), op. cit;Sheng et al. (2010), op. cit;Von Solms (2013), op. cit;Yang et al. (2012), op. cit.

prevent them from being accessed by phishers.[585]

The forgoing countermeasures against phishing can be generally categorized into three groups: technology, institutional network which is exampled by notice-and takedown scheme, and education. The following sections will continue to examine both the strengths and weaknesses of each category of countermeasures in combating phishing.

7.4. Technology[586]

A phishing attack is typically carried out using an email in an attempt to lure recipients to visit a bogus website in order to deceive them into disclosing their personal credentials or tempt them into executing malware designed to steal their confidential data in storage. Technology functions in the regulation of phishing by physically constraining phishing attackers from engaging in or successfully performing certain behaviours, for example, preventing phishing emails from reaching intended recipients or preventing access to phishing sites. Significant work has been conducted to develop various technical methods to detect or filter phishing, which can be implemented at the phishing email level and the phishing website level.

7.4.1. Phishing email level

Spam filters

At first, spam-filter techniques such as Bayes filters[587] were prevalently employed to tackle

[585] Yue, Chuan and Wang, Haining (2008), 'Anti-phishing in offense and defense', *Annual Computer Security Applications Conference, 2008 (ACSAC 2008)* (Anaheim, California, USA: IEEE), 345-54;Yue and Wang (2010), op. cit.

[586] A brief overview of the available technical means has been provided in Chapter 2, section 2.5.3. This section looks into the different technical approaches in more details, with a particular focus on the examination of their effectiveness and ineffectiveness in tackling phishing.

phishing emails; however, it appeared inadequately effective to intercept phishing messages as soon as phishing strategy became more sophisticated and targeted. Spam is generally known as unsolicited bulk email which is sent in large quantities indiscriminately for commercial purpose. Similarly, both spam and phishing emails are undesirable messages which contain no useful information for the intended recipients. However, the purpose of spam is to sell products or services, while a phishing message is delivered in a malicious attempt to dupe the recipients into believing that it is from a legitimate source and so revealing their confidential information.

A typical phishing attack is broad-based, which usually involves a high volume of scam emails to non-specified recipients. Nevertheless, the past few years have witnessed a changing trend of phishing tactics, which are now much more targeted, with low volumes of messages being sent to a specific group of people or even a specific person.[588] In a further effort to bypass spam filters based on the naïve Bayes methodology, phishing messages are increasingly being crafted to imitate legitimate emails by duplicating the look, feel, and structure as well as the logos of legitimate organizations. While text-based classification may do well with regard to identifying spam, it appears inadequately effective to stop phishing messages, especially those designed to look almost identical to real emails. This suggests that the development of a filter specific to the features of a phishing message is critical to effectively stop phishing emails.

Phishing email classifiers

[587] Bayesian spam filtering is a statistical technique of email filtering based on the naïve Bayes classifier which works by correlating words with spam and non-spam emails and calculating the probability of an email being spam or not. Bayesian spam filters assume that an email message is an unordered collection of words selected from one of two bags: one bag is filled with words found in spam messages, such as “Viagra”, “stock” or “buy”, while the other, which is usually called ‘ham’, is filled with words found in legitimate messages; for example, words related to the recipient’s acquaintances or work. It classifies an email message according to which bag it is more likely to be by using Bayesian probability based on the text of the message. For more information about Bayesian spam filtering, see http://en.wikipedia.org/wiki/Bayesian_spam_filtering. Bag-of- words model, see http://en.wikipedia.org/wiki/Bag-of-words_model.

[588] See Chapter 2, section 2.4.1 and Chapter 5, section 5.2.2.2.

A popular approach is content-based classification centered on machine learning techniques which is capable of distinguishing phishing and legitimate messages automatically. A classifier, in the case of phishing classification, will classify an email either as phishing or legitimate by learning specific features in the email. There are several different phishing filtering techniques such as Logistic regression, Support Vector Machines (SVM),[589] Random Forests,[590] and Bayesian classification.[591] Some researchers also proposed a multi-tier phishing classifier that combines multiple classification techniques.[592] Abu-Nimeh et al.[593] compared the performance of different machine learning techniques in terms of the predictive accuracy on a phishing data set. They concluded that the inclusion of additional features might be helpful to improve the predictive accuracy of classifiers.

Chandrasekaran et al.[594] proposed a technique to detect phishing emails based on their structural properties. The authors used a total of 25 features consisting of a mixture of style markers, such as the words suspended, account, and security and structural attributes, such as the structure of the subject line and the greeting in the body. By employing SVM as the classification technique, the authors tested 400 emails (200 phishing emails and the rest were normal), and the results claim a detection rate of 95% of phishing emails with minimum errors. However, as pointed out by the authors themselves, it is difficult to draw a broader conclusion given the small size of the email collection.

Fette et al.[595] presented a classifier, *PILFER*, which identifies phishing emails by using ten features

[589] Bergholz et al. (2010), op. cit;Chandrasekaran, Narayanan, and Upadhyaya (2006), op. cit.
[590] Fette, Sadeh, and Tomasic (2007), op. cit.
[591] Cao, Han, and Le (2008), op. cit;Chen, Chia-Mei, Guan, DJ, and Su, Qun-Kai (2014), 'Feature set identification for detecting suspicious urls using bayesian classification in social networks', *Information Sciences*;Zhang et al. (2011), op. cit.
[592] Abawajy, Jemal and Kelarev, Andrei (2012), 'A multi-tier ensemble construction of classifiers for phishing email detection and filtering', in Xiang Yang, et al. (eds.), *Cyberspace Safety and Security, 4th International Symposium, CSS 2012,* (Melbourne, Australia: Springer), 48-56;Islam and Abawajy (2013), op. cit.
[593] Abu-Nimeh et al. (2007), op. cit.
[594] Chandrasekaran, Narayanan, and Upadhyaya (2006), op. cit.
[595] Fette, Sadeh, and Tomasic (2007), op. cit.

handpicked - nine of these features can be extracted from the email itself,[596] the tenth feature, i.e. the age of the linked-to domain name, has to be obtained by performing a WHOIS query at the time when the email is received.[597] The authors tested the proposed method on 860 phishing emails and 6,950 legitimate emails, and correctly identified over 96% of the phishing emails with a false positive rate of 0.1%. The proposed method can also be used in detection of phishing webpages.

Bergholz et al.[598] proposed a more sophisticated classification using a number of novel features which include statistical models of email topics, sequential analysis of email text and external links, the detection of embedded logos and indicators for hidden salting. The authors tested a dataset of 20,000 ham and phishing emails and successfully identified 99.46% of the phishing emails.

However, while researchers are trying to achieve high accuracy, none of the current research claims zero false positive. The false positive is always a problem to phishing filters. One false positive alarm can potentially cause serious problems for the user. As indicated by Islam and Abawajy,[599] "user can often live with some false negative instead of losing even one legitimate email." In addition, since the content of phishing emails is continually evolving, it is necessary for the filters to keep updated through active and dynamic learning. The foremost drawback of content-based classifiers is their weakness in detecting spear phishing or other targeted phishing messages which are highly personalized and crafted for a particular group or person, in which no specific features can be identified.

[596] These nine features include: IP-based URLs, nonmatching URLs, 'here' links to non-modal domain, HTML emails, number of links, number of domains, number of dots, contains javascript, untrained SpamAssassin Output. Fette, Sadeh, and Tomasic (2007), op. cit.SpamAssassin is a freely-available computer program which has been widely deployed for spam filtering based on content-matching rules. See: http://spamassassin.apache.org/.

[597] WHOIS is a query and response protocol that is used for querying databases, such as domain names and IP addresses. When the phishing website's URL is entered into the WHOIS search field, the directory information reveals when the websites was registered and by whom. In order to deceive users, it is a common tactic that the phishers register a domain name which looks similar to the legitimate one, e.g. yaho0.com or yahooo.com. Given the short lifespan of phishing domains, phishers tend to use these domains shortly after registration. The age of the domain hence becomes a distinctive indicator of phishing websites.

[598] Bergholz et al. (2010), op. cit.

[599] Islam and Abawajy (2013), op. cit.

Email authentication

The key to the success of a phishing attack is convincing the recipient that the source of the communication is an entity that he/she trusts. The higher perceived reputation of the sender can increase the percentage of recipients who comply with the request for personal information. The spoofing of email senders has thus been a common tactic used by phishers. Email authentication hence may serve as an effective means to reduce phishing by detecting spoofed emails.[600]

Some methods have been proposed to validate senders particularly against phishing emails, such as digitally signed mails[601] and identity-based digital signatures.[602] The three main approaches to sender authentication are Sender Policy Framework (SPF), Sender ID Framework (SIDF) and DomainKeys Identified Mail (DKIM),[603] which differ with regard to the specific part of an email that each checks.

The Simple Mail Transfer Protocol (SMTP) - an Internet standard for email transmission across IP networks - permits any computer to send email claiming to be from any source address. This security flaw of the SMTP is often exploited by phishers to forge sender addresses in order to hide their true identity. The Sender Policy Framework (SPF), as an extension of SMTP, is an email validation system designed to prevent email spoofing by verifying envelope sender addresses.[604] SPF allows the owner of an Internet domain to specify their mail sending policy in an SPF record, e.g. which mail severs are authorized to send mail from their domain. The receiving server can

[600] Watson (2004), op. cit.

[601] Garfinkel et al. (2005), op. cit.

[602] Adida, Hohenberger, and Rivest (2005), op. cit.

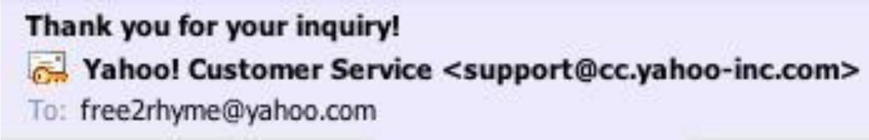
[603] Herzberg (2009b), op. cit;Lininger and Vines (2005), op. cit.

[604] Like conventional mail, email messages have at least two sender addresses – one on the envelope and one on the letterhead. The envelope sender's address, which is usually not displayed to the recipients, is used for the delivery of a message during its transit from one mail server to another. The header's sender address is contained in the "From" or "Sender" header and is displayed to the recipients by mail programmes.

check and may reject a message if it comes from an unauthorized server which does not comply with the SPF records before receiving the body of the message.

Sender ID provides another anti-spoofing method which consists of two parts: SPF classic and Purported Responsive Address (PRA). In addition to the information in the envelope, Sender ID also checks sender-related information in the header to identify if the message actually came from the domain that it appears to be from by comparing it with the information published by the domain owners.

DomainKeys is a Yahoo!-proposed technology used to combat email forgery by verifying both the domain of the email sender and the message's integrity. It verifies that an email is really from the domain it claims to be through the use of public key encryption technology at the domain level. Yahoo! Mail users can find a DomainKeys icon, i.e. a small icon showing an envelope and key, in the email header if this message has been verified (see figure 7.1).[605]



Thank you for your inquiry!
Yahoo! Customer Service <support@cc.yahoo-inc.com>
To: free2rhyme@yahoo.com

Figure 7.1: Example of the DomainKeys icon

A study[606] of the adoption of SPF in Sweden published in 2007 pointed out that the adoption-ratio of SPF as an anti-phishing mechanism is extremely low, only 1.63% among all Swedish domains have a published SPF policy. The low adoption-ratio could be down to several causes: limited knowledge about SPF, lack of visual indicators in software that the policy is absent, and failure to

[605] Information and example icon of DomainKeys, see: http://antispam.yahoo.com/phishing.

[606] Görling (2007), op. cit.

recognize the danger of un-validated sender addresses.

Both SPF and DomainKeys aim to validate whether an email message comes from a legitimate domain; however, they are unable to verify if this message is really from the person from whom it appears to be. A phishing email can easily bypass SPF and DomainKeys checks as long as it does not involve domain spoofing. Email authentication is helpful in detecting one aspect of phishing attacks, but cannot stop phishing messages sent from a legitimate source, for example a bot-infected or a compromised computer, but by the wrong person.

7.4.2. Phishing website level

Keeping users away from phishing sites is another promising approach to disrupting phishing attacks. Phishing do not necessarily, but usually, involves the use of a bogus website which mimics the genuine one in order to trick visitors into entering their personal or financial information. As users' confidential data is exposed to immediate risk of being compromised once they access a spoofed site, it is very important to spot the danger to protect users. Considerable researches have been conducted for detection of phishing at the website level, which generally fall into two main categories: blacklisting and heuristic-based approach.

Blacklisting

Blacklisting is a common approach that concentrates on combating phishing websites and protecting users from accessing them. It functions by checking the website against a list of reported phishing URLs when a web address is rendered in a browser and is typically built into web browsers[607] and available as a web browser toolbars.[608] The SmartScreen Filter,[609] for instance, is

[607] Apple op. cit;Google op. cit;Microsoft op. cit;Mozilla op. cit.

a feature in Windows Internet Explorer that helps to detect phishing websites. The web address of the site that a user is visiting will be sent to the SmartScreen service for comparison with a dynamic list of known phishing sites. Internet Explorer will display a warning notifying the user that the site has been blocked once the SmartScreen Filter finds a match on the blacklist and advises the user not continue to the unsafe website. In the Mozilla Firefox browser,[610] each web page requested by a user of the browser is checked against a blacklist of reported phishing and malware sites which is automatically downloaded and updated every 30 minutes. Wherever there is a match on the blacklist, Firefox will block the page from loading and display a Reported Web Forgery warning.

Several software developers have also proposed web browser toolbars which help to detect phishing websites based on the blacklisting model. McAfee SiteAdvisor,[611] for example, is a browser plug-in that gives safety advice about websites before a user clicks on them. SiteAdvisor works by adding site rating icons, i.e. red, yellow and green, to users' search results and a browser button to alert users about potentially risky sites. With SiteAdvisor software installed, phishing websites are automatically rated red and a user is automatically re-directed to a warning page whenever he/she tries to browse a phishing website.

Blacklists of phishing URLs can be produced in different ways, including automatic categorization using a set of classification rules based on previous phishing patterns, manual classification by administrators or crowd sourcing by users.[612] The above methods can be used individually or alongside each other. PhishTank is a typical example which uses crowd sourcing. It provides a community-based system whereby anyone can submit suspected phishes while other users can verify whether a submission is a phishing website or not. However, while the manually-verified

[608] Mcafee op. cit;Netcraft op. cit.

[609] Microsoft op. cit.

[610] Google op. cit;Mozilla op. cit.

[611] Mcafee op. cit.

[612] Wilson and Argles (2011), op. cit.

phishing URLs list has a high level of accuracy, it is a rather time-consuming process. The automatic categorization process may classify a high volume of phishing URLs, those are nevertheless more likely to be false positive.

More importantly, the time gap between the appearance of phishing sites and the updating of the blacklist is always a problem with the effectiveness of this approach, which in turn produces advantages to the phishers. New phishing sites appear frequently and are ephemeral in nature. For example, an average of more than 1,960 unique phishing sites was detected per day in February 2012,[613] which usually existed for only few days, and many of them disappeared within hours. In addition, phishing sites are ephemeral in nature, usually existing for only few days, and many of them disappear within hours. Nevertheless, it always takes some time before a new phishing site is reported and added to the blacklist. A study[614] indicated that over half of stolen data is harvested within the first hour of a phishing email being received, which makes it a pressing task to block a phishing site within the first 60 minutes of its existence. Sheng et al.[615] tested eight anti-phishing toolbars with 191 fresh phish that were less than 30 minutes old and they found blacklists were ineffective at hour zero and could only identify 47% - 83% of phishing even after 12 hours. The time-lag in updating the blacklist has become the major challenge to the effectiveness of blacklisting.

To change the reactive nature of blacklists, some researchers proposed predictive blacklisting which is capable of detecting phishing based on known bad domains[616], features of known phishing sites[617] or URLs,[618] or a relevance ranking scheme borrowed from the link-analysis community.[619]

[613] APWG (2012), 'Phishing Activity Trends Report - 1st Quarter (January -March) 2012'. <http://www.antiphishing.org/reports/apwg_trends_report_q1_2012.pdf>, accessed September 9 2014.
[614] Klein (2010), op. cit.
[615] Sheng et al. (2009b), op. cit.
[616] Felegyhazi, Kreibich, and Paxson (2010), op. cit.
[617] Prakash et al. (2010), op. cit.
[618] Ma et al. (2009), op. cit.

Felegyhazi et al. inferred an average 3.5 to 15 new domains from a given known-bad domain grounded on registration and name serve information. The authors attempted to demonstrate the potential of a domain-based proactive blacklisting, and their analysis showed that 93% of these interfered domains subsequently appear suspect and nearly 73% eventually appear on a reactive blacklist about 2 days after. However, as indicated by the authors themselves, a significant variable of gain exists in different domains. In addition, there apparently exists a problem of false positive that needs to be overcome.

Heuristic-based approaches

Heuristic-based technique functions by estimating whether a given page has certain phishing characteristics. Most of heuristic-based researchers identify phishing sites by looking into URL features[620] or/and website content,[621] including textual and visual content such as words, titles, or images in the website.

For example, Garera et al.[622] extracted a set of features from phishing URLs alone to tell whether a URL is a phishing or benign one. Ludl et al.[623] discovered a list of 18 properties of a phishing site, two of which are derived from the page's URL and the remaining features are extracted from the HTML source of a page. CANTINA (Carnegie Mellon Anti-Phishing and Network Analysis Tool) is another content-based approach developed by Zhang et al.[624] to determine the legitimacy of a website. It works by calculating a lexical signature using TF-IDF by taking five terms from the

[619] Zhang, Porras, and Ullrich (2008), op. cit.

[620] Alsalman (2012), op. cit;Garera et al. (2007), op. cit;Hsu, Wang, and Pu (2011), op. cit.

[621] Chen et al. (2009), op. cit;Chen, Dick, and Miller (2010), op. cit;Liu et al. (2006), op. cit;Ludl et al. (2007), op. cit;Medvet, Kirda, and Kruegel (2008), op. cit;Nirmal, Ewards, and Geetha (2010), op. cit;Pan and Ding (2006), op. cit;Wenyin et al. (2005), op. cit;Xiang and Hong (2009), op. cit;Zhang, Hong, and Cranor (2007a), op. cit;Zhang et al. (2011), op. cit.

[622] Garera et al. (2007), op. cit.

[623] Ludl et al. (2007), op. cit.

[624] Zhang, Hong, and Cranor (2007a), op. cit.

phishing-suspicious page and feeding them into a search engine. If the domain name of the given web page matches the domain name in the top 30 results, then it is considered legitimate. There was also a proposal of content-based framework which takes into account both textual and visual contents to measure the similarity between the legitimate and suspicious web pages by using a Bayesian approach.[625]

While nearly all the above methods claimed to have reached a very high accuracy rate in spotting phishing sites, researchers suggested that the performance largely depended on the source of phishing URLs and the freshness of the URLs tested and found many of the anti-phishing tools were vulnerable to simple exploits.[626] The advantage of the heuristics approach is that it can detect phishing sites as soon as they are launched without the need to wait for blacklists to be updated. However, due to the high similarity between phishing and legitimate pages, the heuristic technique is likely to mislabel a legitimate site as phish and is hence rarely used in a web browser given its high false positive rate. Another problem is that attackers may be able to design their attacks to circumvent heuristic-based detection as long as long as they know the current strategies being used.[627]

Technology features largely in the fight against phishing, although each approach has its advantages and disadvantages. While undoubtedly there is much that can be done technically to detect phishing attacks, there is unlikely to be a perfect solution that can completely prevent them. It was suggested that a combination of these techniques is probably a way to optimize the ability to detect phishing accurately while achieving the least false positive rate.[628]

However, several researchers argued the effectiveness of both server-side security indicators and

[625] Zhang et al. (2011), op. cit.

[626] Zhang et al. (2007b), op. cit.

[627] Bin, Qiaoyan, and Xiaoying (2010), op. cit;Sheng et al. (2009b), op. cit.

[628] Wilson and Argles (2011), op. cit.

client-side toolbars and warnings in helping users avoid phishing attacks.[629] Most users frequently ignore the warning stated on the toolbar[630] or the cues such as HTTPS indicators[631] that tell them that the websites are very likely to be malicious. Wu et al.[632] tested three security toolbars and other browser security indicators on 30 subjects with previous experience in online shopping and found they were all ineffective in preventing users from phishing attacks. Their analysis indicated that many of the subjects failed to continuously check the browser security indicators and the others disregarded or explained away the toolbars' warning even when they had noticed suspicious signs coming from the indicators. Schechter et al.[633] examined the effect of security indicators (HTTPS indicators and site authentication images) by asking 67 customers of a single bank to login to that bank's website. The result revealed that all the participants entered their passwords even when HTTPS indicators were absent and 92% of the participants who used their own accounts entered their passwords even after their site authentication images were removed. The authors concluded that the security indicators have rather limited effectiveness as users hardly pay attention to the alarming clues that their connections are insecure.

Researchers suggested that most users do not see maintaining security as their primary goal[634] and they are generally lacking a baseline level of security awareness.[635] Users are often not clear about how to interpret a warning sign and what they are expected to respond to warnings.[636] Many users even do not understand phishing attacks and what to look for in phishing messages.[637] Although various technical solutions have been developed to defend against phishing, the above usability

[629] Aburrous et al. (2010), op. cit;Dhamija, Tygar, and Hearst (2006), op. cit;Downs, Holbrook, and Cranor (2006), op. cit;Egelman, Cranor, and Hong (2008), op. cit;Herzberg (2009a), op. cit;Schechter et al. (2007), op. cit;Wu, Miller, and Garfinkel (2006b), op. cit;Zhang et al. (2007b), op. cit.

[630] Wu, Miller, and Garfinkel (2006b), op. cit.

[631] Schechter et al. (2007), op. cit.

[632] Wu, Miller, and Garfinkel (2006b), op. cit.

[633] Schechter et al. (2007), op. cit.

[634] Kumaraguru et al. (2010), op. cit;Wu, Miller, and Garfinkel (2006b), op. cit.

[635] Bakhshi, Papadaki, and Furnell (2009), op. cit;Furnell (2007), op. cit.

[636] Furnell (2009), op. cit.

[637] Furnell (2007), op. cit.

studies of anti-phishing tools prove that technology alone is not enough to combat phishing.

More importantly, phishing tactics are constantly being modified and refined in order to take continual advantage of the weakness of computer systems. A flawless technical solution is almost impossible, as the development of the anti-phishing technology is always a few steps behind creation of new phishing techniques. Provided there is a perfect anti-phishing technique which could spot all phishing, it is still likely to be bypassed by users if they fail to realize how dangerous and sophisticated phishing attacks can be and what they are expected to do in responding to phishing.

7.5. Education of users

While considerable effort has been devoted to solving the phishing problem through the prevention and detection of spoofed emails and websites, comparatively little research has been done in the area of education and training of users to recognize phishing attacks. Technical solutions can be used as the front line of defence against phishing; however, these solutions are unlikely to perform flawlessly and cannot eradicate phishing by themselves but should be complemented with a key component – user education.

Phishing relies on social engineering which largely exploits the weakness of humans rather than technical vulnerabilities. A successful phishing attack not only abuses the weakness in human nature but also takes advantage of a user’s inability to discern phishing emails or websites from legitimate ones. A study[638] found that, when users were asked to determine whether a website was valid or not, the incorrect choice was made 40% of the time. This study also revealed that a well-crafted phishing site was able to fool more than 90% of the participants, including even the most

[638] Dhamija, Tygar, and Hearst (2006), op. cit.

sophisticated users. This result demonstrated that users generally experience difficulties in distinguishing fraudulent sites from legitimate ones, which highlights the need for the education of users to spot phishing and actively protect themselves from phishing attacks.

Education and training is another dominant countermeasure against phishing by enabling users to engage in secure online behaviours.[639] Many financial and commercial institutions have invested in an education campaign to teach their users to interact safely with emails and websites and not to engage in potentially risky activities that may lead them to being victimized. Anti-phishing education for customers is usually performed by providing advice in the form of guidelines on or tips about recognizing phishing. For example, eBay provides tutorial advice to users about how to spot spoof emails and fake websites as well as how to report suspicious emails. It also includes behavioral tips regarding the protection of users' information from being stolen, such as "never click on a link in an email if you are unsure of its origins" or "never provide sensitive personal information in an email".[640]

A variety of anti-phishing educational materials is also available online. For example, APWG provides a set of public education initiatives which include the Phishing Education Landing Page Program that functions by redirecting users towards instructional materials instead of an error page at the "most teachable moment" – when these users have just clicked on a link in a phishing communication (email or otherwise).[641]

Nevertheless, a study[642] indicated that users rarely look for anti-phishing educational materials and tend to ignore emails that direct them towards theses. An interactive approach, which is mostly

[639] Ademaj and Schuck (2009), op. cit;Arachchilage and Love (2013), op. cit;Davinson and Sillence (2010), op. cit;Jerram et al. (2012), op. cit;Liang and Xue (2010), op. cit;Von Solms (2013), op. cit.

[640] eBay 'Recognizing spoof (fake) eBay websites'. <http://pages.ebay.com/help/account/recognizing-spoof.html>, accessed September 8 2014.

[641] APWG Public Education Initiatives (PEI), http://phish-education.apwg.org/.

[642] Kumaraguru et al. (2010), op. cit.

designed in the format of games or web-based tests, is generally considered to be more helpful to improve users' resistance to phishing by allowing them to assess their likely vulnerability to phishing or teach them how to identify phishing in a natural and interactive environment for learning by doing. Several proposals for anti-phishing education or training programs have been put forward in both academics and industry.[643] SonicWALL, for instance, has set up a website containing a Phishing IQ test,[644] which takes the form of a sequence of phishing email screen shots and scores based on how well the participants can identify potential phishing emails.

Anti-Phishing Phil,[645] an online game proposed by Sheng et al. that enhances users' ability to avoid phishing by teaching them how to spot phishing URLs, where to seek out cues in web browsers, and how safely to use search engines to find legitimate websites. The authors compared the effectiveness of their proposed method with the existing online training materials and security tutorials and found that the participants who played the game were better at spotting phishing sites.[646] Another well-known example is *PhishGuru*,[647] an email-based education system using embedded training methodology and learning science principles that delivers training messages to users at the moment users actually fall for phishing attacks. The authors also demonstrated the effectiveness of their proposed education tools to help users to better recognize phishing by the results of both lab and real-world experiments.[648]

However, some researchers argued that user education "puts the burden on the wrong shoulder"[649]

[643] Kumaraguru et al. (2008), op. cit;Kumaraguru (2009), op. cit;Kumaraguru et al. (2009), op. cit;Kumaraguru et al. (2010), op. cit;Robila and Ragucci (2006), op. cit;Sheng et al. (2007), op. cit;Sheng et al. (2010), op. cit;Von Solms (2013), op. cit;Yang et al. (2012), op. cit.

[644] SonicWALL Phishing IQ Test, http://www.sonicwall.com/furl/phishing/.

[645] Anti-Phishing Phil, http://cups.cs.cmu.edu/antiphishing_phil/; Sheng et al. (2007), op. cit.

[646] Kumaraguru et al. (2010), op. cit;Sheng et al. (2007), op. cit.

[647] Kumaraguru (2009), op. cit.

[648] Kumaraguru et al. (2008), op. cit;Kumaraguru (2009), op. cit;Kumaraguru et al. (2009), op. cit.

[649] Nielsen, Jakob (2004), 'User education is not the answer to security problems', *Nielsen Norman Group*. <http://www.nngroup.com/articles/security-and-user-education/>, accessed September 17 2014.

and indicated that user security education was a “myth”.[650] Anandpara et al.[651] indicated that the only measurable effect of phishing tests is to increase the participants’ suspicion about phishing rather than to improve their ability to recognize phishing attempts. Davison and Sillence[652] also questioned the effects of Anti-Phishing Phil on promoting secure behaviour beyond the specific points it trained on. Whether the knowledge provided by training materials can be transferred to secure online behaviour in a real world setting and how long the knowledge can be retained is an important problem needing to be addressed when developing education frameworks.

Another important reason which makes educational measures ineffective is a general shortage of motivation among the end users to learn about security, as most users only consider security to be a secondary goal and tend to disregard the signs of risk.[653] End users can be security conscious, as long as they perceive the danger of phishing and the need to adopt secure behaviour in order to avoid being phished.[654] Arachchilage et al.[655] proposed a game-based education framework to enhance user avoidance behaviour through intensifying avoidance motivation, which is, according to Liang and Xue,[656] determined by the elements of perceived susceptibility, perceived severity, safeguard effectiveness, safeguard cost, and self-efficacy. Users develop a threat perception when they believe that the threat is real (perceived susceptibility) and could be severe (perceived severity). When threatened, users are more motivated to avoid the threat if they believe the recommended measure is effective (safeguard effectiveness) and the cost is reasonable (safeguard cost) and they can successfully perform it (self-efficacy). Similar opinion was also held by Comesongsri.[657]

[650] Görling, Stefan (2006), 'The myth of user education', *Virus Bulletin Conference* (11; Montreal, Canada), 13.
[651] Anandpara et al. (2007), op. cit.
[652] Davinson and Sillence (2010), op. cit.
[653] Anandpara et al. (2007), op. cit.
[654] Adams, Anne and Sasse, Martina Angela (1999), 'Users are not the enemy', *Communications of the ACM,* 42 (12), 40-46.
[655] Arachchilage and Love (2013), op. cit.
[656] Liang and Xue (2010), op. cit.
[657] Comesongsri (2010), op. cit.

The cost of education and training is also a problem.[658] It is hard to expect that the user training program can get instant results. To educate the users and employees to prevent phishing attacks which are constantly updated and reformed, the businesses need to maintain periodical training programs with ongoing cost but without immediate benefit. This may negatively influence the eagerness of the business to spend on training and education.

A successful phishing attack largely relies on exploitation of human vulnerability, which is almost impossible to control and manage. Although it is difficult to see an immediate effect of education and expect all users have adequate knowledge to spot phishing or act like educated users when responding to the warnings, education is always an essential baseline of defense by helping users protect themselves from falling for phish even if there is no any technical defense. However, how educational materials can be effectively transferred to users' secure online behaviours is an important question that needs to be taken into account when developing education or training programs. To encourage users to engage in secure online behaviours and intensify their motivation of pursuing information security education and training, it is necessary to strengthen their awareness of the correlation between their behaviours, e.g. misjudging threats as non-threats or bypassing warning sign and security indicators, and the enormous damage that could cause to themselves and a great number of other users.

7.6. Institutional network – an example of the notice-and-takedown scheme

According to Castells,[659] 'networks' are the unit of a network society; and the social power in a network society is primarily exercised through networks. 'Institutional network', which refers to an

[658] Purkait (2012), op. cit.
[659] Castells (2011), op. cit.

organized cooperation and connection between institutions in different interfaces, can serve as a powerful measure to control certain behaviour which is against laws or social order. Institutional network can be operated nationally or internationally; and the institutions can be public or private institutions. The best example of the regulation of phishing in institutional network fashion is the notice-and-takedown strategy.

'Notice-and-takedown' is a promising scheme used for removing undesirable content from the Internet. Moore Clayton undertook a study of the removal times and the number of visitors based on a sample of 144 phishing sites and found each site attracted around 18 visitors if it is removed within one day of being reported, rising by 8 victims for each successive day.[660] Their study illustrated an important fact: the longer a phishing site exists, the more users are victimized. This highlights the significance of an immediate reaction consisting of taking down phishing sites in order to minimize the potential damage as well as protect more users from falling victims.

The removal of phishing websites is another countermeasure that has been prevalently employed especially among banks or financial organizations that are likely to be spoofed to combat phishing. Many financial institutions contract takedown companies to remove spoofed sites as soon as they are detected. The takedown process generally starts when a takedown company is altered to existence of a phishing site and that company then contacts the domain registrars, the hosting companies or the system administrators (sysadmin), or ISPs to bring that phishing site down. The process usually takes a few hours but could take several days or even longer when the server is geographically operated outside national boundaries. Netcraft, a well-known phishing takedown company, pointed out that a savvy phishing attacker often host the spoofed site in countries with inadequate legal enforcement resources, to ensure that the process is as difficult and

[660] Moore and Clayton (2007), op. cit.

time-consuming as possible.[661]

There are different actors responsible for phishing takedown according to the types of phishing attack.

7.6.1. Web-hosting companies, system administrators, and ISPs

In order to evade being traced, most phishing attackers host websites in free hosting environment or on compromised machines such as a residential machine or a server in a data center rather than on their own machines.[662] To get a phishing site removed from free web space, a takedown company needs to contact the free web-hosting companies to ask them to remove the bogus site and cancel the hosting account. When the phishing website is hosted on a compromised machine, a takedown request will be sent to the relevant ISP who will temporarily take the website in question offline or disable connection to the offending web pages and approach the administrator to ask him to remove the website and fix the machine. The message to administrators usually has to be delivered through ISPs as the information about them mostly is not made public.

A research[663] which was conducted by Moore and Clayton over a large set of phishing sites hosted on free web space and compromised machines indicated that the phishing sites were removed fairly promptly once the hosting companies and the administrators of compromised machines received the takedown request, but, they could remain up considerably longer if they are missed by the brand owners. The authors concluded that how quickly the phishing sites are removed largely depends on whether the brand owners are aware of the existence of these websites. It was also suggested that

[661] Netcraft op. cit.

[662] Mcgrath and Gupta (2008), op. cit;Moore and Clayton (2009), op. cit.

[663] Moore and Clayton (2009), op. cit.

responses from ISPs often vary largely depending on company, country, and the competence and language skills of the requesting organization.[664]

7.6.2. Domain registrars and registries

In the case that a domain name has be registered especially for phishing use or in some complex cases involving rock-phish or fast-flux phishing networks,[665] it is necessary to contact the domain name registrars and registries to ask for suspension of the domain name in question. Phishers exploit the DNS by registering domains and use them to send scam and host fraudulent sites. Recent statistics[666] revealed that 27% of the 82,163 domains used for phishing were registered maliciously by phishing attackers in the second half of 2013. McGrath et al.[667] conducted an analysis of registration of phishing domains and the machines used to host the phishing sites and found most domains registered for the purpose of phishing become active almost immediately upon registration. When a fraudulent site has been taken down, it can be moved to a different host or ISP, and the domain point to the new site. To suspend the resolution of the phishing domain is the only way to stop this cycle.

Rock-phish and fast-flux phishing sites have become a huge challenge to the effectiveness of takedown strategies and they were found to be able to survive much longer than ordinary phishing sites by obfuscating phishing behaviours to complicate takedown procedures.[668] Rock-phish gangs operate by making a network of compromised machines as proxies to relay request. Taking down a proxy cannot really remove phishing sites, as rock-phish sites automatically switch to another

[664] Moore and Clayton (2007), op. cit.

[665] The discussion about rock phish and fast-flux technology, see Chapter 2, section 2.4.1.

[666] APWG (2014), 'Global Phishing Survey: Trends and Domain Name Use in 2H2013'. <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf>, accessed September 9 2014.

[667] Mcgrath and Gupta (2008), op. cit.

[668] Mcgrath, Kalafut, and Gupta (2009), op. cit;Moore and Clayton (2007), op. cit;Moore and Clayton (2009), op. cit.

machine which is still working. Fast-flux network works by changing IP addresses in seconds and rapidly moving the phishing sites around to make it almost impossible to take them down.

The only practical way to remove rock-phish and fast-flux sites is to have the domain name suspended. Nevertheless, it becomes very difficult if the domain registrar requested fails to recognize that the domain name in question is an impersonated one.[669] The person who requests the suspension of a particular domain name might be required to present evidence which can prove its fraudulent nature. For example, the Austrian domain registrar nic.at initially refused to remove rock-phish domains and asked the reporter, Spamhaus - an email-blacklist operator, to prove that these domains had been registered by non-existent persons.[670] This may cause additional difficulty to the takedown procedure which, in turn, extends the lifetime of phishing websites. While the average lifetime of ordinary phishing websites was found to be less than 60 hours, the rock-phish domains could remain alive for more than 90 hours and the lifetime of the fast-flux domains even reached up to nearly 19 days on average.[671]

Domain registrars and registries are one of the key actors responsible for phishing takedown; however, their reaction to phishing incidents was described rather "lagging",[672] even though they are very often the victims involved in phishing attacks too.[673] APWG produced a set of recommendations for domain registrars and registries which particularly focused on the assistance

[669] Moore and Clayton (2007), op. cit;Rodenbaugh (2009), op. cit.

[670] Warrner (2007), op. cit.

[671] Moore and Clayton (2007), op. cit.

[672] Sheng et al. (2009a), op. cit.

[673] A report released by the Security and Stability Advisory Committee of ICANN indicated that domain names have become a popular target of phishing attackers. Increasing number of phishers impersonate a registrar to obtain the account credentials of the registrar's customers by which they can modify the customer's domain registration for malicious purpose or use the credit card or other forms of payment on file to purchase more domains for subsequent illegal use. ICANN, Security and Stability Advisory Committee (SSAC) (2008), 'SAC 028: SSAC Advisory on Registrar Impersonation Phishing Attacks '. <https://www.icann.org/en/system/files/files/sac-028-en.pdf>, accessed September 15 2014.
In addition, criminals register new domains mostly by using stolen credit or debit cards. The registrars are the ones that eventually take the charge back for these fraudulent domain registrations. Apwg (2008b), op. cit;Rodenbaugh (2009), op. cit. Sheng et al. (2009a), op. cit.

that they are able to provide in law enforcement, screening of fraudulent domain registrations, and takedown of phishing domains.[674] Registrars were encouraged to share fraudulent domain registration information such as registrant IP addresses or registrant's personal information with law enforcement authorities to assist in investigation. APWG also suggested registrars to periodically check against the blacklists of phishing URLs from different sources to identify malicious domains before they take effect. Registrars and registries should make timely response to domain takedown requests by suspending or terminating phishing domains as quickly as they are notified. While domain registrars and registries were regarded to stand in an excellent position in combating phishing, a study of the anti-phishing efforts of the domain registrar community indicated that some registrars and registries will act upon complaints but the others, including their downstream resellers, will not take any action or investigation because domain registrars generally are low margin businesses owning very limited manpower and resources and many of them are also unwilling to take the cost of customer service to address domain abuse.[675]

The Internet Corporation for Assigned Names and Numbers (ICANN)[676] funded in 1998 is a nonprofit organization responsible for managing global domain name system (DNS) and IP addressing functions to ensure the network's stable and secure operation. ICANN coordinates the Internet Assigned Numbers Authority (IANA) functions, including management of Top-Level Domains (TLDs),[677] operation of root name servers,[678] assignment of IP address blocks to regional domain registries, and allocation of Internet numbering resources.[679] Although ICANN does not take phishing complaints directly, it has key influence over the response of domain registrar community to phishing by developing policies and setting and negotiating contractual standards for

[674] Apwg (2008b), op. cit.

[675] Rodenbaugh (2009), op. cit.

[676] ICANN, https://www.icann.org/.

[677] TLDs are the domains at the highest level in the hierarchical DNS. A TLD is the last segment immediately following the final dot in a web address. For example, *www.google.com*, com is the TLD.

[678] Root name servers are resolvers that translate host name to IP address to find TLDs.

[679] The work of ICANN, https://www.icann.org/resources/pages/welcome-2012-02-25-en.

registrars and registries. Experts suggested that ICANN should establish a set of minimum standards of domain abuse and enforce compliance through accreditation mechanism, and encourage adoption of anti-abuse policies by regularly publishing data on registries' performance on phishing takedown and taking anti-abuse metrics as part of evaluation criteria for registry application.[680]

In May 2008, ICANN's GNSO (Generic Names Supporting Organization)[681] Council formed a working group on fast flux to consider the problem of fast-flux hosting and how it can be mitigated by ICANN contracting parties. The final report of this Working Group was released in August 2009.[682] This report demonstrated that some proposals are taking in place that help to mitigate malicious domain registrations, recommended the adoption of a *Fast Flux Data Reporting System* for ICANN members to submit potential fast flux domains to better monitor illegal activity, and considered ICANN as the facilitator to set policy and ensure the implementation of best practices among its contracted parties.

The SSAC of ICANN issued an advisory which encouraged each registrar to provide an effective and responsive contact point of abuse matters that is capable of responding quickly to domain abuse complaints.[683] In 2009, Rodenbaugh produced a document addressing the state of ICANN effort and policy development on abusive domain name registrations.[684] This document indicated that the APWG have been working with the registry representatives on developing a suspension process for phishing domains with a hope that can effectively cut down the up-times of phishing domains while reduce false positive complaints. The registry will suspend a domain in question if the registrar or registrant fail to address the suspension request within a certain timeframe. This suspension process

[680] Sheng et al. (2009a), op. cit.

[681] ICANN GNSO, http://gnso.icann.org/en/index.htm.

[682] Konings (2009), op. cit.

[683] ICANN, Security and Stability Advisory Committee (SSAC) (2009), 'SAC 038: Registrar Abuse Point of Contact'. <https://www.icann.org/en/system/files/files/sac-038-en.pdf>, accessed September 15 2014.

[684] Rodenbaugh (2009), op. cit.

nevertheless is only applicable to the domains that are used solely for phishing and only admits the suspension requests filed by accredited anti-phishing teams. This suspension process can be adopted by other registries on a voluntary basis if it proves effective.

This section demonstrates how phishing attacks can be controlled by systematic connection and organized cooperation between different organizations, exampled by notice-and-takedown strategy. However, the effectiveness of this strategy has been questioned, as the phishing sites, especially those on compromised machines, may continue to reappear shortly after they are first taken down. Taking down a phishing site only hastens the phisher's movement from one host to another, and many users continue to fall for phish. This is like a cat and mouse game, with takedown companies always being a few steps behind the fraudsters, as fraudsters operate in real time but takedown solutions can only be reactive in nature.[685]

Although the removal of phishing websites is often perceived as an endless task, it does help to lower the damage that a phishing site may cause and prevent potential victims by removing the site as soon as it is known by the brand owners, takedown companies or other anti-phishing organizations.[686] An effective takedown strategy relies on the joint effort of different institutions involved, including the organizations that are impersonated, takedown companies, web-hosting companies, ISPs, system administrators, and domain registrars and registries. The effectiveness can be improved by coordinating the action of the actors responsible for takedown to removal requests and enhancing information sharing between different takedown companies.[687]

While takedown companies only focus on removing those phishing sites that directly attack their client, it is considered to be very important to set up a publicly available notice-and-takedown

[685] Varghese (2008), op. cit.

[686] Moore and Clayton (2007), op. cit.

[687] Moore and Clayton (2008), op. cit.

mechanism which allows every user to report phishing sites or emails with all types of contents. The next section (7.7) looks into the anti-phishing work that has been undertaken in Taiwan, with a particular focus on the establishment and operation of the Taiwan anti-phishing working group and the phishing reporting system established in late 2010.

7.7. The Taiwan Information Security Strategic Alliance

7.7.1. Background

The Computer Emergency Response Team / Coordination Center (CERT/CC) was first founded by the Defense Advanced Research Projects Agency (DARPA, now ARPA) in 1988 as a result of the first automated network security incident encountered by ARPANET,[688] usually referred to as the "Morris Worm".[689] The initiative of CERT/CC sprang up quickly worldwide and these incident response teams created an informal organization known as the Forum of Incident Response and Security Teams (FIRST) in 1990.[690] The computer centre of National Sun Yat-Sen University has been in charge of the operation of TWCERT/CC since its establishment in September, 1998.[691]

[688] ARPANET (The Advanced Research Projects Agency Network), founded by DARPA of the U.S. Department of Defense in 1969, was the world's first operational packet switching network and served as the beginning of the Internet. See: http://en.wikipedia.org/wiki/ARPANET.

[689] A student at Cornell University, Robert T. Morris, wrote a program that would connect to another computer to find and use one of several vulnerabilities to copy itself to that second computer and continue to repeat these actions at the new location on ARPANET. An explosion of copies caused by this self-replicating, automated network attack tool consumed a great volume of system resources which significantly influenced the function of the attacked computers. In consequence, 10% of the U.S. computers connected to ARPANET stopped at about the same time. The Morris Worm prompted DARPA to establish a computer emergency response team to coordinate responses to network emergencies. Regarding the history of the Morris Worm, see: Longstaff, Thomas A, et al. (1997), 'Security of the Internet', *The Froehlich/Kent Encyclopedia of Telecommunications,* 15, 231-55.

[690] The idea of FIRST can be traced back to 1989. While the number of incident response teams continued to grow, the interaction between these experienced difficulties due to the different languages, timezones, and standards employed. This highlighted the need for better communication and coordination between teams and prompted the creation of FIRST which brings together a wide variety of security and incident response teams, including teams from the government, commercial, and academic sectors. FIRST is a recognized global leader which enables incident response teams to respond to security incidents more effectively by providing access to best practices, tools and trusted communication with team members. See: http://www.first.org/.

[691] In addition to coordinating the responses to computer security incidents, the main tasks of TWCERT/CC also involve uniting the system and network related resources to assist sites that detect potential vulnerabilities and to improve the

TWCERT/CC joined FIRST in October 2001 and, since then, has acted as the international contact window of Taiwan in respect of computer security incidents as well as a bridge between different CERTs.

However, the operator of TWCERT/CC - an academic team which is subordinate to a university – has been restricted by its limited manpower and resources, which has posed a crucial challenge to TWCERT/CC in effectively implementing communication and coordination work among CERTs at either the domestic or transnational level.[692] As a result, in 2009, the Taiwan Network Information Center (TWNIC)[693] was commissioned by the National Information and Communication Security Taskforce (NICST)[694] to administer the operation of TWCERT/CC on behalf of the computer centre of National Sun Yat-Sen University for a three-year period between 2009 and 2012 to enhance the transformation of TWCERT/CC and, above all, to strengthen its role in coordinating the different CERTs to handle computer security incidents.[695] No single organization alone has all of capability or information needed to deal with information security incidents. Given the importance of collaboration over different computer security teams across different sectors in responding to arising security breaches, TWCERT/CC called on the stakeholders involved, including government agencies, ISPs, academic units, computer security industries, and business

security of sites, and educate network users about computer security. See: http://www.cert.org.tw/eng/index.htm.

[692] Lin, Yi-Long (2010), 'The Relay Position of the TWNIC to Enable the TWCERT/CC to Transform and Restart', *TWCERT/CC Newsletter,* 1.

[693] The Taiwan Network Information Center (TWNIC), established at the end of 1999 and supervised by the Ministry of Transportation and Communication, is a unique neutral, non-profit organization that oversees domain name registration and IP address allocation in Taiwan. In addition to providing specialized Internet services, TWNIC is also committed to coordinating and facilitating the activities and cooperation between national and international Internet-related organizations such as ICANN (Internet Corporation for Assigned Names and Numbers) and APNIC (Asia Pacific Network Information Center) as well as the equivalent national Internet organization in other countries, including JPNIC (Japan), CNNIC (China) and KRNIC (Korea). See Background and Mission of TWNIC, http://www.twnic.net.tw/english/about/about_01.htm.

[694] NICST was established in 2001, following the passing of the Executive Yuan's 'National Information and Communication Infrastructure Security Mechanism Plan' (2001-2004). The main task of NICST is to promote the tasks of building the information security foundation of Taiwan. In 2009, NICST gave impetus to the 'National Information & Communication Security Development Plan' (2009-2012), aiming at achieving the goal of "Safe and Trustworthy Intelligence Taiwan, Safe and Quality Digital Life." See http://www.icst.org.tw/Intro.aspx?lang=en.

[695] Liu, Jin-Han (2010), 'The Activation of the Taiwan Information Security Strategic Alliance', *TWCERT/CC Newsletter - Special Periodical for the Taiwan Information Security Strategic Alliance*. <http://www.myhome.net.tw/cert01/cont04.htm>, accessed September 16 2014.

corporations, collectively to build up a joint defensive alliance to remove sectoral barriers and reinforce the cooperation among different teams regarding tackling issues relating to information security.

7.7.2. Structure and cooperation model

The Taiwan Information Security Strategic Alliance (hereinafter, the Alliance), which was formally established on 23 September, 2010, aims at "establishing a collectively defensive mechanism and reinforcing information security systems". The Alliance currently has two working groups: the anti-phishing working group and honeynet[696] working group (Cyber Clean Center). The Advisory Committee - the main body of the Alliance comprising all of the members - meets twice a year to consider the suggestions or reports submitted by the working groups, make the rules and decide the direction for the work. The Alliance also holds meetings every three months to discuss and share information and experiences regarding Internet security techniques.

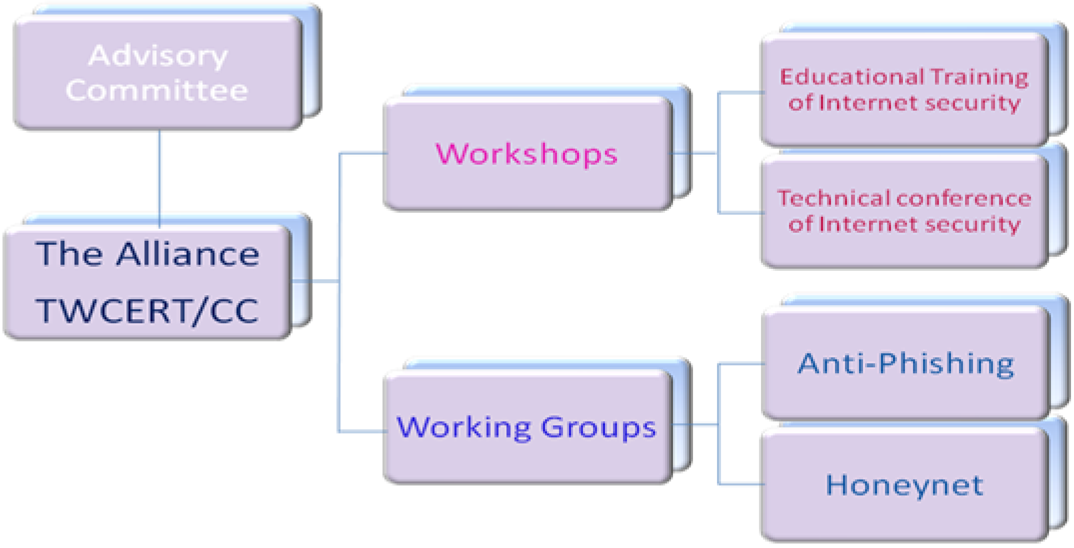


Diagram 7.1: Organizational Structure of the Alliance

Source: TWNIC

[696] A honeynet is a network set up with intentional vulnerability, aimed to attract and trap attackers in order to gather information about their activities and study their motives and methods which can be subsequently used to increase network security. It usually contains one or more honeypot, which are computer systems on the Internet designed purposely to trap people who attempt to penetrate other computer systems. For a definition of honeynets, see: http://searchsecurity.techtarget.com/definition/honeynet.

The Alliance is primarily constructed based on three existing CERTs, including TWNCERT (Taiwan National CERT), the TANet CERT (Taiwan Academic Network CERT), and the NCC CERT (National Communication Commission CERT). The above three are the teams responsible for responding to the computer security incidents occurring on governmental, academic, and commercial networks, respectively. The Alliance, under the supervision provided by the Science and Technology Advisory Group of the Executive Yuan (the STAG, now the OBOST),[697] currently embraces the members of government agencies –the Ministry of Transportation and Communications, the Ministry of Education, the NCC, the Research, Development and Evaluation Commission of the Executive Yuan (the RDEC),[698] the Information and Communication Security Technology Center (the ICST),[699] the Ministry of Education; the Taiwan Internet Association (the TWIA);[700] and the five leading Taiwanese telecom enterprises in terms of revenue and customer numbers that provide Internet access services (IASPs) - HiNet by Chunghwa Telecom, Far Eastone Telecom, Taiwan Fixed Network, So-net Taiwan, and Asia Pacific Telecom.

[697] STAG, which was established in December 1979, turned into the Office of the Board of Science and Technology of Executive Yuan (OBOST) on 01 January 2012 as a result of organizational reform. It is responsible for making administrative policies with regard to science and technology at the level of central government and also in charge of execution of the policies. See: http://www.bost.ey.gov.tw/Default.aspx.

[698] The RDEC, established in 1969, is responsible for "policy research and development, policy planning, policy supervision and evaluation, government's IT management, circulation of government publications, archives and other tasks assigned". It was dissolved in January 2014 and the superseding agency is the National Development Council. See: http://www.ndc.gov.tw/.

[699] The ICST belongs to one of the seven groups of the NICST – the Government Information and Communication Security Working Group, which is in charge by the RDEC. The ICST is responsible for helping the RDEC to carry out the related work of the above group and provides pre-incident protection, during-incident handling, and post-incident forensics and recoveries to all government agencies. In order to detect information security incidents early, the ICST establishes the Government Security Operation Center (G-SOC) to execute information security monitoring services for government agencies. The ICST also operates the Government Information Sharing and Analysis Center (G-ISAC) whereby the ICST gives counsels, provides technical services, and publishes messages related to information security to government agencies. The G-ISAC also organizes, integrates and distributes the information related to computer security through the system automation and information standardization of the information sharing process. See: http://www.icst.org.tw/index_e.aspx.

[700] TWIA, formed in late 1999, is a non-governmental organization, aimed at providing a communication and cooperation platform for domestic industries in related to Internet services in order to facilitate innovation and the free development of Internet-related industries. TWIA welcomes domestic ISPs (Internet service providers), ICPs (Internet content providers), operators of portal sites or electric commerce or individuals who would be interested in this issue as members. See: http://www.twia.org.tw/.

The Alliance aims at building trusted relationship among its members to enable them to carry out collective defence against information security threats horizontally. Thereby, they can expand the safeguard scope and improve the reactive speed to information security incidents. The cooperation model of the Alliance is shown in Diagram 7.2.

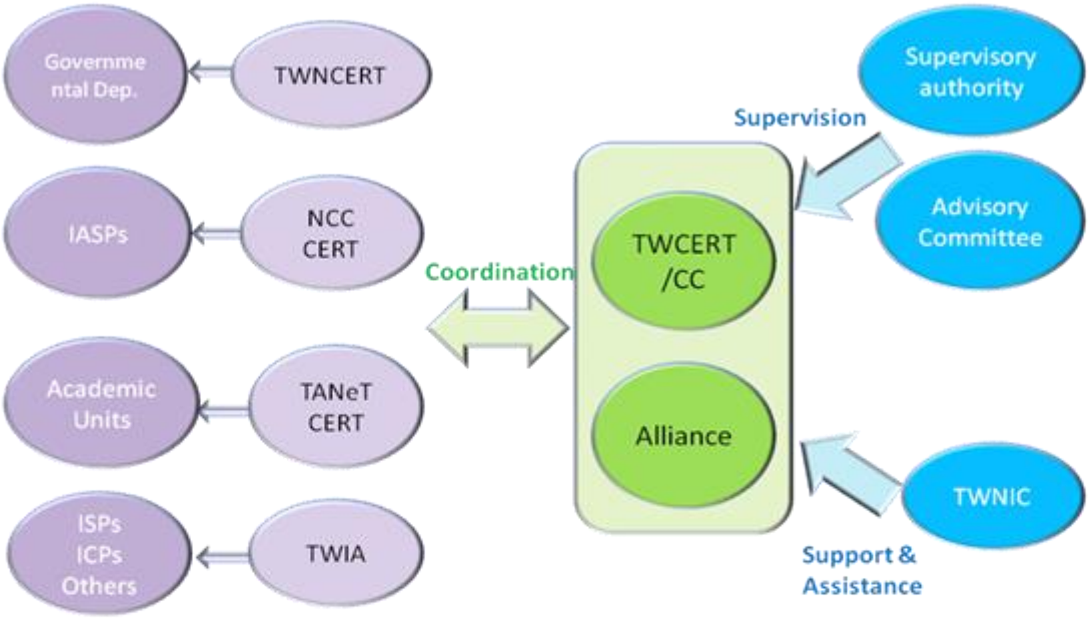


Diagram 7.2: Cooperation Model of the Alliance
Source: TWNIC

7.7.3. Taiwan Anti-Phishing Working Group (TAPWG) and Anti-Phishing Notification Window (APNOW)

Given the increasing threat of phishing attacks in Taiwan, the Alliance members reached a consensus that anti-phishing work should be prioritized by first organizing an anti-phishing working group and establishing an ‘anti-phishing notification window’ to streamline the reporting procedure for phishing incidents. TWCERT/CC first introduced the Taiwan Anti-Phishing Working Group (TAPWG) in July 2010. TAPWG, which includes the members of TWNCERT, TANet CERT, NCC CERT, ISPs and academic departments, attempts to combine the knowledge and ability of the public and private sectors as well as research units to produce responding measures through undertaking joint deliberation for tackling the potential risk of phishing and dealing with phishing incidents that have been detected.[701]

Following TAPWG, TWCERT/CC activated a phishing reporting mechanism known as the Anti-Phishing Notification Window (APNOW) in October 2010. APNOW serves as both an internal and external window to receive reporting regarding phishing attacks. Reporting may come from a variety sources; for example, individual users, domestic and foreign CERTs or other entities.

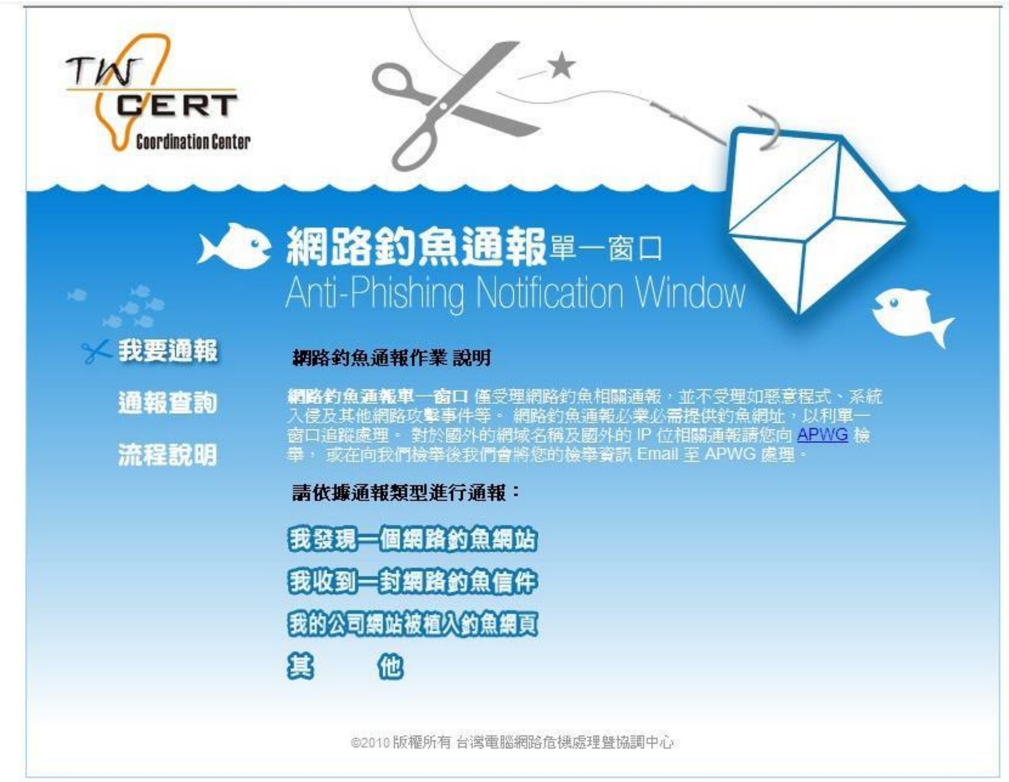
7.7.3.1. APNOW reporting procedure

APNOW provides an exclusive platform for reporting suspected phishing incidents, which do not include other cyber-attacks, such as malware attacks or computer system intrusion. It is worth noting that APNOW is only involved in the reporting of suspected phishing websites hosted in Taiwan. For phishing notification in relation to foreign domain names or IP address, APNOW forward them to relevant foreign CERTs in conjunction with notifying the Anti-Phishing Working Group (APWG), PhishTank, and browser industries, such as Microsoft, Firefox or Google. In this case, users are also encouraged to notify APWG of suspected phishing emails or websites directly.

Through visiting the website of APNOW (www.apnow.tw), users can not only make reports but are also able to trace the progress of reports that have been previously submitted. On the front page of

[701] Lin, Shun-Jie (2011a), 'The Introduction of the Taiwan Anti-Phishing Reporting Mechanism and Platform', *TWCERT/CC Newsletter,* 6.

APNOW, users are provided with three options regarding submitting reports in accordance with the types of phishing incident, which include phishing emails, phishing websites, and phishing webpage injection. If users are uncertain about the reporting type, they can go to 'Others' and the personnel of the back-end system will help them to categorize them (see Figure 7.2).



網路釣魚通報作業 說明

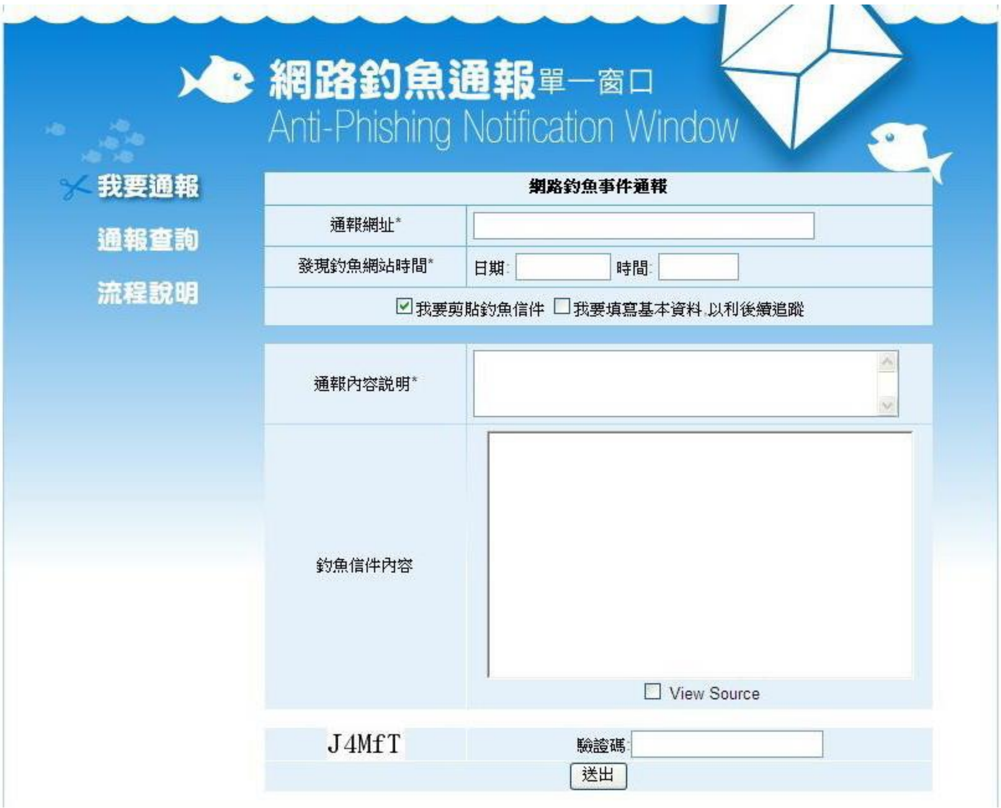
網路釣魚通報單一窗口 僅受理網路釣魚相關通報，並不受理如惡意程式、系統入侵及其他網路攻擊事件等。 網路釣魚通報必業必需提供釣魚網址，以利單一窗口追蹤處理。 對於國外的網域名稱及國外的 IP 位相關通報請您向 APWG 檢舉， 或在向我們檢舉後我們會將您的檢舉資訊 Email 至 APWG 處理。

請依據通報類型進行通報：

©2010 版權所有 台灣電腦網路危機處理暨協調中心

Figure 7.2: Front page of APNOW website
Source: http://www.apnow.tw/

The more information that users provide, the more efficient the back-end system of APNOW processes submission. At a minimum, APNOW asks users to provide the URL of the suspected website and indicate the date and time on which they detected it. Users can copy the phishing message contents into the text box and identify the concrete contents of reports, if they wish. However, users need additionally to submit their personal information, including their name, email address and telephone number, if they intend to track the progress of their submissions afterwards.



網路釣魚事件通報

通報網址*

發現釣魚網站時間* 日期: 時間:

☑我要剪貼釣魚信件 □我要填寫基本資料,以利後續追蹤

通報內容說明*

釣魚信件內容

□ View Source

J4MfT 驗證碼:

Figure 7.3: APNOW Reporting Format
Source: http://www.apnow.tw/index2.cgi?s=2

7.7.3.2. APNOW processing procedures

The APNOW processing procedures of phishing reports are primarily operated via an automated system. First, the APNOW system provides the reporter with an individual reference number for his submission, for tracking use. Second, the system roughly verifies the report to determine whether or not it is a real phishing case, finds the IP address of the suspected website and passes the case, along with the relevant evidence collected from the website in question, to the corresponding CERT. Following further verification of the factuality of the phishing website in question, the CERT, at the third step, asks the operators or sysadmins of the website or hosting companies to take the necessary measures, including repairing, shutting down or blocking access to the website. However, in most cases, the APNOW system notifies the ISPs directly, thereby bypassing the NCC-CERT once the IP of the suspected website has been identified to be a commercial net to produce a more effective outcome.

On the other hand, the APNOW system continues tracking the handling of phishing sites. Each phishing site is checked hourly to confirm its availability till it is declared to be down. The corresponding CERT or ISP is required to complete the response measures to the phishing site within a specific time frame or else its office director needs to assist if the phishing site is still active after 16 hours and its supervisory authority needs to intervene after 24 hours.

Finally, to end the case, the CERT or ISP is required to report back to APNOW by logging on the system to record the handling result of the phishing site; for example, if the site has been taken down or its access has been blocked. The reporter is also kept informed about the eventual result via APNOW. Diagram 7.3 shows the flow of the APNOW processing procedures.

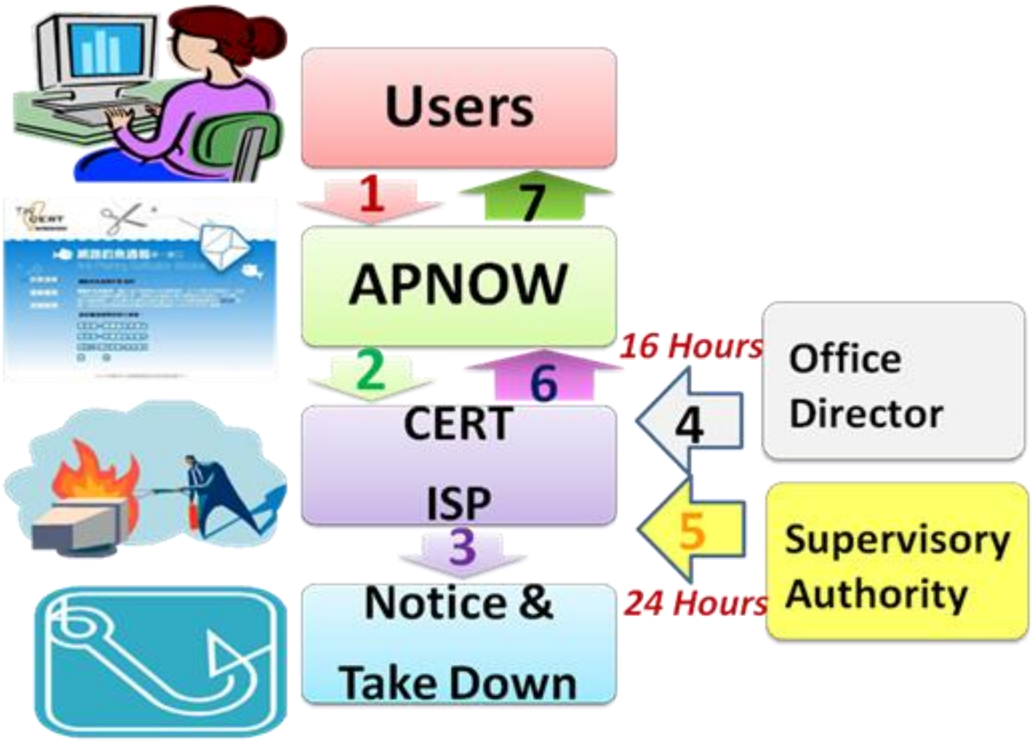


Diagram 7.3: APNOW processing procedures

7.7.3.3. Requirement of processing time

The longer a phishing site remains alive, the more risk is posed to potential victims. The lifetime of phishing websites is a vital factor which affects how damaging phishing attacks are, as well as measuring the success of any mitigation efforts. The statistics compiled by the APWG indicated that the average uptime of phishing attacks in the second half of 2009 was 31 hours 38 minutes, while the average lifetime during the same period in Taiwan was 51 hours 42 minutes.[702] Inspired by this statistic, the Advisory Committee of the Alliance sought to lower the lifetime of a phishing site and suggested a deadline by which to finish dealing with a phishing report.[703]

The current requirement set by the Alliance regarding the processing time of a phishing report is 24

[702] APWG (2010b), 'Global Phishing Survey: Trends and Domain Name Use in 2H2009'. <http://apwg.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf>, accessed 9 September 2014.

[703] Lin (2011a), op. cit.

hours. As mentioned above, the APNOW system checks the availability of the phishing site every hour since it passed the report on to the corresponding ISP. The system additionally sends an email notification at the 4th and 10th hour if the phishing site is still active. At the 16th hour, the system automatically requires the office director of the ISP to assist in terminating the connection to the phishing site and, at the 24th hour, the system informs the supervisory authority of the ISPs, i.e. the NCC, and requests appropriate intervention in the processing of phishing reports.

7.7.3.4. Suggestions to the APNOW

Having presented an overview of the operation of the APNOW reporting system, this research proposes the following suggestions regarding the future work of APNOW.

Elimination of the language barrier

This research firstly points out the language problem existing in the APNOW user interface. In addition to accepting reports from Taiwanese users, APNOW serves as an external window for receiving phishing reports from other countries. However, APNOW currently only adopts a Mandarin interface, and this language barrier leads to difficulties for users who wish to access the system but do not know Mandarin. The aim of APNOW to provide an effective international contact window for phishing incidents will fail if it cannot provide a friendly interface for international users.

Reduction of processing time required to take down a phishing site

Research shows that the first hour of phishing emails being received is the “golden hour” of phishing attack, as over half of stolen data is harvested within the first 60 minutes.[704] This means that successfully blocking a phishing site within the 60 minutes of its existence becomes absolutely crucial. Klein goes on to suggest that 80 per cent of stolen credentials are gathered and become usable by phishers within the first 5 hours and that, by 10 hours, more than 90 per cent of the data that a phishing site is able to collect has already been harvested.

Accordingly, it is vital that a phishing site is blocked or taken down within 5 to 10 hours. Therefore, the current APNOW requirement of processing time for a phishing report, i.e. 24 hours, appears to need to be further reduced in order to provide better protection for phishing victims.

The monitoring of phishing websites that have been taken down

Some phishing websites, particularly those hosted on botnets, may remain alive after the first attempt to remove them. In fact, more than 10% of phishing websites re-activate after one hour of being taken down. A phishing website can be declared down only if it can be confirmed to be no longer alive. Therefore, it is necessary for APNOW to continue to monitor each phishing website that has been shut down to ensure it stays down for a certain period of time.

Promotion of visibility to the public

According to the statistics gathered by TWNIC between 23 September 2010 and 18 February 2011, the number of suspected phishing sites reported to APNOW accounted to 147, including domestic and foreign IPs, with 144 targeted at foreign entities and only 3 targeted at local brands.[705] This figure shows that the phishing sites hosted in Taiwanese domains mostly focus on corporations

[704] Klein (2010), op. cit.

[705] Shiu, Nai-Wen (2011a), 'The Report of the Current Status of the Taiwan Information Security Strategic Alliance', *TAIS International Conference 2011* (TWNIC).

outside Taiwan, as most phishing perpetrators attempt to abuse the jurisdictional gaps to evade investigation and prosecution. Nevertheless, the big difference between the quantity of local and foreign reports also reflects the relatively low visibility of APNOW to Taiwanese users. Over nearly five months, there were only three reports of phishing attacks which targeted Taiwanese companies. One was hosted in a Taiwanese domain but was eventually verified a not a phish and the other two were hosted in foreign domains. The very few reports may be attributed to the insufficient awareness or knowledge of users about phishing. However, they can also be explained by the possibility that this newly-established reporting system is still not widely-known among general Internet users in Taiwan.

To address this problem, it is vital to promote the visibility of APNOW in a variety of ways, such as the public media, cross-sites' linkage or information security education or training. It is also worth introducing APNOW and providing its URL link in security reminder messages for users on portal sites and login pages which are particularly sensitive to financial information; for example, online banking login pages. Above all, it is necessary to ensure that APNOW is known in every aspect by all the CERTs or units that are in charge of handling computer security incidents in both the public and private sectors.

Enhancement of immediate communication and coordination with foreign CERTs

As aforementioned, the work of APNOW is primarily operated by an automated system, including the initial verification of phishing sites, assignment of reports to the corresponding teams, subsequent tracing of processing progress, and notification of the related persons or government authorities. The timeliness of phishing response should not be hindered by the delay caused by the need for human intervention.[706] However, APNOW still needs to rely on human intervention where

[706] Wardman, Brad and Warner, Gary (2008), 'Automating phishing website identification through deep MD5

the suspected phishing sites that have been reported are hosted in other countries. Given the difficulty of adhering to the 24-hour time limit for dealing with foreign suspected phishing sites due to the time difference and the potential delay caused by human operation between countries, the requirement of the processing time of a phishing report presently applies to phishing sites hosted in Taiwan only, and does not include foreign phishing sites.

However, an immediate reaction to cut phishing lines as soon as they are detected is crucial in order to succeed in the fight against phishing attacks. Any undue delay in taking down phishing sites should be avoided, even if these sites are hosted in other countries. The workload of APNOW should be handled by automating the notice-and-takedown process as far as possible. This makes it pressing to build an automatic reporting mechanism which bridges different CERTs between countries to optimize the ability of CERTs to make immediate response and take down verified phishing sites in a timely manner.

7.8. Taiwan's Anti-Phishing Scheme

Phishing arose as an issue in the late 1990s but did not receive proper attention in Taiwan until recent years. As I have mentioned in Chapter 3 (section 3.4), there was very little scholarly discussion on phishing countermeasures in Taiwan prior 2008. Although some progress had been made on anti-phishing research since 2008, it apparently only focused on the development of technical tools with very little attention to the countermeasures that can be implemented in other dimensions. The establishment of the TAPWG in July 2010 was a major breakthrough in the progress of Taiwan's anti-phishing work, as it manifested Taiwan government's ambition to coordinate the effort of the stakeholders in different fields – academia, CERTs of governmental, academic and commercial network and ISPs in responding to growing phishing attacks, and the

matching', *eCrime Researchers Summit, 2008* (IEEE), 1-7.

introduction of the APNOW in October 2010 further reflected the focus of Taiwan's anti-phishing work has shifted from concentrating on technological development only to notice-and-takedown strategy based on institutional network.

Nevertheless, things seem not to change too much. As I have pointed out in previous section (7.4), there are several problems regarding the usability and operation of the APNOW which may restrict its effectiveness and demand proper improvements. In addition, all the information about the TAPWG's meetings and the statistical data about the APNOW's reports and processing time are inaccessible, as this information is not released publicly but is only shared among their members. The effectiveness of APNOW in tackling phishing hence still remains a question and needs to be further examined. The existing Taiwanese literature only provides general information about the background, structure and the process of the above anti-phishing schemes,[707] there is no further research-based literature available which can provide a clue about the practical engagement of different stakeholders in current anti-phishing work. What work have various stakeholders undertaken to control phishing? What efforts have they made to engage in cooperation with other stakeholders, both nationally and internationally? How do they evaluate their work and the work of the other stakeholders? What improvement may be required to enhance future anti-phishing scheme? To provide insights into these questions, it was considered necessary to conduct an empirical study through holding interviews with the experts selected from different regulatory bodies, including law enforcement, NCC, ISPs, CERTs, online merchants, and key information security industry, to learn how and to what extent they get involved in anti-phishing work and seek their expertise on the effectiveness of the anti-phishing countermeasures that have been implemented, combined with their suggestions for future work.[708]

[707] Lin (2010), op. cit;Lin (2011a), op. cit;Liu (2010), op. cit.

[708] The list of the interviewees, see Appendix A.

It should be borne in mind that the examination of Taiwan’s multi-dimensional regulation of phishing is primarily based on existing documents and resources, but supplemented with insights provided by the information obtained from the interviews. Although this is a small-scale field work, it is the first study that synthesizes the opinions of Taiwanese experts from different fields, and examines the efforts that various stakeholders have devoted or are expected to devote to the Taiwanese anti-phishing work.

This compares and contrasts with a US study that integrates the expert opinions from various areas and examines the incentives of different stakeholders to devote to anti-phishing work by Sheng et al.[709] The authors conducted 31 semi-structured interviews with the experts selected from academia, law enforcement, CERTs, APWG and industry in the USA between May 2008 and May 2009 to seek their expertise on the state of phishing attacks, the countermeasures need to implemented, and the incentives of various stakeholders to engage in the fight against phishing. The study of Sheng et al. aimed to shed a light on the three main questions: where stakeholders should place their efforts? Do they have sufficient incentives to contribute? What countermeasures should be prioritized for the anti-phishing work?

My study also compares with another US study conducted by Nero et al.[710] who carried out telephone interviews with the representatives from five major financial institutions and five take-down companies to ask the interviewees to determine the most successful phishing countermeasure to financial institutions. This study especially sought to learn how financial institutions follow up with law enforcement to tract, arrest, and prosecute a phishing perpetrator.

The main findings of the Taiwan study are indicated below followed by a comparison with the US

[709] Sheng et al. (2009a), op. cit.

[710] Nero et al. (2011), op. cit.

studies. This is followed by a more detailed exploration of the Taiwan study.

7.8.1. Key findings of the Taiwan study

All the experts interviewed agreed that it is extremely difficult to catch phishing perpetrators in vast majority of cases, especially when they involve multiple jurisdiction. Although Taiwan became a member of G8 24/7 network in 2004, the expert, who was also the key person pushed Taiwan's entrance through, expressly indicated that it is almost impossible for Taiwan to receive assistance with the transnational investigation into phishing cases through the above network in practice. The expert also indicated that the companies which have been targeted mostly tend to resort to ISPs directly to ask for a removal of phishing sites rather than work with law enforcement agents due to a lack of confidence in the effectiveness of criminal investigation and prosecution.

Most of the experts identified that the ISPs of Taiwan stands in a key strategic position in combating phishing, especially in terms of proactive detection of phishing attacks and taking-down of phishing sites. Nevertheless, the expert from the largest ISP of Taiwan stressed that they have practical difficulty spotting phishing proactively. Some of the experts indicated that the ISPs sometimes are hesitant to suspend the connection to suspicious phishing sites in an absence of legal authorization and hence suggested a need for legal amendment. The expert from the NCC further emphasized the necessity of reinforcing the ISPs' legal responsibility for information security management.

Although most of the experts did not exclude from cooperating and exchanging the phishing database with other stakeholders, the expert from information security industry only preferred the cooperation model directed by industry, not government. In terms of evaluation of the current anti-phishing work, most of the experts agreed that the lack of users' awareness of information security and incentive to act in coordination with the security advices given by either the government, ISPs or industry has posed a crucial challenge to anti-phishing work. Some of the experts identified that the major weakness lies in insufficient capacity of Taiwan’s businesses, in particular SMBs, for ensuring web security and respond to information security incidents.

In terms of suggestions for future anti-phishing schemes, some of the experts recognized users’ education as a fundamental solution and suggested that more efforts should be made to promote users’ knowledge and awareness regarding information security. Some of the experts indicated that the priority should be placed upon the systematic development and planned training of IT personnel who are capable of ensuring web security and properly responding to phishing attacks.

7.8.2. Comparison with US studies

The field work I conducted is similar to the work of Sheng et al. in the sense that both invited the experts from different fields which are highly related to phishing and sought their opinions, standing in the position of various stakeholders, on phishing countermeasures that have been implemented and should be implemented. Nevertheless, the differences in the situation in the US and Taiwan are reflected in some of the differences in approach. The two works are different in terms of scale and methodology. While Sheng et al. focused on where the efforts should be placed to achieve effective action by asking the experts to specifically prioritize the recommendations on a list compiled by the authors through their research, my work aims to examine the individual role of each stakeholder in the fight against phishing and how they evaluate their work and the work of the other stakeholders. Given the difference of working background between the interviewees, the interview questionnaires were designed individually for each interviewee but they were all structured based on the following key themes: background information, involvement in the anti-phishing work, cooperation and connection with the other stakeholders, comments on the current anti-phishing work, and suggestions for future work.

Nevertheless, there were similarities between the findings of these two studies. While the potential victims who may suffer direct loss from phishing are usually expected to have an incentive to invest resources in safeguard measures to protect themselves, the experts suggested that many potential victims, especially customers and SMBs, act in a quite opposite way. In fact, a lot of potential victims do not feel the need to particularly strengthen the protection of their machines or servers because they fail to realize the threat of phishing and the impact that phishing could cause upon them and the integral security of Internet network, or we can say, they do not think that they will be the target. Although most experts identified the key position of ISPs in helping their customers with the compromised machines, the experts from the ISPs of both USA and Taiwan felt not much interested in undertaking this task as it is costly and its effect is rather limited.

Yet, there was a distinct difference in the experts' opinions on the priority of countermeasures between Taiwan and USA. While the US experts identified improving law enforcement and shutting down money trails as top priorities, the Taiwan experts suggested that more effort should be placed on facilitating taking-down procedure and enhancing training and education of IT personnel and customers. In fact, all of the Taiwan's experts regarded law enforcement as a countermeasure that is very unlikely to be effective against phishing because of the peculiar political situation of Taiwan. As emphasized in Chapter 6, an effectual legal enforcement largely relies on effective international cooperation between the related agents across countries from which the Taiwan experts could hardly expect too much. Taiwan has been suffering from its disadvantaged international status for more than four decades, and this has caused a significant obstacle for Taiwan to establishing or engaging in international cooperation with other countries.[711]

My work is also similar to the work of Nero et al., as both sought to learn how the institutions

[711] See Chapter 3, section 3.6 and Chapter 4, section 4.4.2.5.

interviewed cooperate with law enforcement in prosecuting phishers. Nevertheless, we had different groups of interviewee. While Nero et al. invited the employees from selected financial institutions and take-down companies, the experts in my study were selected from various stakeholders but not including the above two. Yet, the interviewees of the two studies had rather similar opinions about the effectiveness of law enforcement. Nero et al. study revealed a common complaint of the financial institutions interviewed about the slow pace of the legal enforcement and found none of them sought prosecutions against phishing attackers. One of the main reasons was the financial institutions stood on a different side to the law enforcement agencies, where the former were eager to take down the phishing website as quickly as possible, but the latter focused on collecting evidence for investigation and prosecution purposes, which may require them to keep the phishing website active for a certain time. Similar opinion could also be found in my study in the interview with the expert from online merchant.

7.8.3. Criminal investigation and prosecution

If there is someone who has ever postulated that criminal prosecution is the main approach that Taiwan has taken to deter phishing, the analysis demonstrated that this presumption is incorrect. All the interviewees acknowledged that phishing perpetrators were rarely prosecuted in the vast majority of cases, especially when they were operating in a cross-border manner.

7.8.3.1. Obstacles to investigation[712]

The interviewees gave multiple reasons for the ineffectiveness of the investigation of phishing. One of the criminal investigators interviewed (Interviewee A) stated:

[712] The challenges posed by phishing to legal enforcement, see Chapter 6, section 6.2.

> There are many methods that can be used to evade investigation. For example, I could place my [phishing] web page in a temporary web space which might be untraceable. I could even hide my IP address through an anonymous proxy if I am technically capable of doing so. These all greatly increase the difficulty of the investigation and tracking work.

Anonymity, as an important feature of the Internet, was frequently abused by phishing perpetrators to impede the investigations. The difference between the time at which the information was stolen and the phishing was discovered was another key factor that exaggerated the obstacle to identify the phishing perpetrator. The other investigator (Interviewee B) stated:

> In most cases, people are less likely to be aware of the fact that their account information has been stolen unless the information is used for illegal purposes such as online auction fraud. There is always a time lag. Also, the person who steals the information might sell it to a third party. Even if we know the time and the IP address where someone has logged into a victim's account from the logging record, we can hardly find out when, how and by whom the information was stolen. It is a troublesome situation unless we can catch the person who logs onto the victim's account and then trace this back to the phishing perpetrator where the success rate is very low.

Most importantly, the transnational nature of phishing attacks poses a severe challenge to the arrest of phishing perpetrators. Few efforts can be made by Taiwan's investigation organization to continue tracing the location of the IP as well as the phishing perpetrator once the fraudulent website has been identified as being hosted in a foreign country. The barrier to the cross-border investigation of a phishing case was largely due to the shortage of an effective cooperation network. Interviewee A stated:

> A majority of [phishing] cases are carried out across jurisdictions. If the phishing website is hosted in other countries, for example China, Vietnam or the U.S., I can

> only trace it to the IP gateway, at most. We are unable to continue tracing the IP outside Taiwan as we do not have a cooperation mechanism with other countries. This is a dilemma for the investigation of phishing cases that we currently face.
>
> Based on our previous experience, it is most unlikely that we will receive assistance from other nations. Therefore, when someone in Taiwan reports a foreign-hosted phishing website, we can only reply to the reporter or victim that this website is hosted in another country and we are hence unable to go any further.

7.8.3.2. Mutual legal assistance

In fact, Taiwan joined the G8 24/7 network[713] (hereinafter, the network or 24/7 network) as its 35th member country in 2004.[714] However, the legal specialist interviewed (Interviewee C), who played the principal role in pushing Taiwan's entrance through, stated that Taiwan could hardly seek assistance with the transnational investigation of phishing cases from the above network in practice. Interviewee C also confessed that there was clearly a gap of the effectiveness of this network in facilitating mutual legal assistance between what he had expected initially and the one that it actually had displayed. Interviewee C stated:

> I had very high expectations at first. However, granted that we know each other and have the contact email of other member countries, we rarely report a case to the network unless it involves terroristic attacks or a significant loss. Phishing, in simple terms, is a type of Internet fraud or a pre-phased act of Internet fraud. A case like phishing is unlikely to be admitted into the network. We once found that some hackers in China were attacking Taiwan's government through websites

[713] For a discussion of the G8 24/7 network, see Chapter 6, section 6.5.

[714] While the entrance into the G8 24/7 network under the name of 'Taiwan' has generally been regarded as a material breakthrough in Taiwan's diplomatic development, it displeased the Chinese government and was criticized as an act of country division. To date, China still refuses to join the above network. See 'A warning of Taiwan's diplomatic breakthrough', *CHINA.COM*, 10 August, 2004, available at: http://www.china.com.cn/zhuanti2005/txt/2004-08/10/content_5631835.htm.

> hosted in Japan. We tried to request assistance from the Japanese police through the network but received no response from them. We even asked the U.S. Department of Justice to communicate our request to Japan, but the result was the same. A case like this still failed to attract their attention. One can well image that a phishing case cannot get through the network.

In a further question asking about the evaluation of the effectiveness of the G8 24/7 network compared with the interviewee's own expectation, Interviewee C answered straightforwardly "It surely falls short of my initial expectation".

Every country had different levels of procedural requirement for initiating an investigation, such as access to private records or a search for evidence. While some countries empowered investigators to perform investigations to a certain extent by their authority, others required that a court order must be granted before the investigators can take certain investigative actions regarding a case. However, in practice, it was less possible to have a court order if the case were unrelated to the requested country, especially when it only involved damages and victims in the requesting country. This was a crucial factor which led to the ineffectiveness of the 24/7 network. Interviewee C explained:

> There are differences existing in the procedural requirements for performing investigations. For example, a U.S. prosecutor cannot access IP records or other information unless he is given a court order. If we inform the U.S. investigation organizations of the existence of a phishing website [which is hosted in America but targets Taiwanese users] and request them to access the relevant records for the phishing website in question, they tend to ignore such a request, as it is very unlikely that they will be granted a court order, since all of the victims of this case reside in Taiwan.

> I once brought up this question in a talk with the representative from the FBI in Japan and asked him why they always cannot provide Taiwan with assistance in investigative matters. The reason he gave me was that they are not allowed to do

> this without court orders.

On the contrary, as Taiwan had a lower procedural requirement for investigators to access to IP records, the investigators in Taiwan usually positively responded to other countries' requests to the least extent by verifying the IP location and identifying the potential phishing perpetrator. The investigators might perform further investigation if the information collected from the requesting country proved that Taiwan's domestic users were also being victimized. However, considering the low likelihood of acquiring information from the requesting country, the investigators usually tried to shut down the phishing website instead of carrying out any further investigation. Interviewee A stated:

> At least, we will verify where the IP [of the phishing website] is and whether the user of the hosting machine is unwitting or intentional. If this user is the perpetrator, we may try to ask for information from the requesting country to see if there is any victim in Taiwan. We may then apply for a search warrant to perform the subsequent investigation after collecting relevant evidence, if there are victims in Taiwan. However, such an investigation is hardly possible in the absence of judicial agreements, as it involves differences in laws and the problem of jurisdiction. Our experience of communicating with other countries reveals that it seems impossible to acquire information regarding an investigation from them. Afterwards, we turn to the measure of taking-down phishing websites. This is the simplest method which can deal with the problem in the speediest way.

7.8.3.3. Mistrust of the effectiveness of investigation

The ineffectiveness of criminal investigations into phishing also influences the intention of the financial institutions that are likely to be targeted to cooperate with the legal enforcement agencies when they detect an imitation website. This point is similar to Nero et al. findings,[715] as mentioned

[715] Nero et al. (2011), op. cit.

in section 7.8.2. Interviewee C, who had served as a Chief Information Security Officer (CISO) for a world well-known online merchant, stated:

> Rather than rely on polices to tackle phishing websites, we actually resorted to the collective defence operated among ISPs on a global scale. At the time when I worked for [the name of an online merchant], our major work in respect of phishing was to search for every phishing website related to our company. If we found a phony website, we contacted the CISO of that country where the phishing website was hosted so that they could go to the ISP and request a taking-down of that website.

> Going to the ISP was much more efficient than going to the police to take the phishing website down. The longer a phishing website existed, the more users were victimized. While phishing websites can never be eliminated, what we could do was to remove them as soon as they were detected. We barely reported phishing cases to the police, as we knew that the chance of catching the phishers was extremely low.

In summary, the legal enforcement officers interviewed explained the particular challenges posed by the global nature of phishing to the investigation, and expressly admitted the ineffectiveness of cross-border legal enforcement in tackling phishing activities in practice even though Taiwan has become a member of the G8 24/7 network in 2004. Although Taiwan participated in the 24/7 network, which was established to connect the police and investigation agencies across borders, the actual effectiveness of the network in improving the collaboration of the investigative powers of different countries was doubted. The inconsistent procedural requirements for initiating investigations were deemed a key factor leading to different responses to MLA requests in different countries which significantly diminished the effectiveness of the transnational cooperation network in the fight against phishing. Another major cause which hampered the follow-up investigation and prosecution of phishing perpetrators was the negative response from other countries to Taiwan's request for information sharing.

The priority for the financial institutions that were likely to be targeted was how they could enable a phishing website to be shut down as soon as it was detected. Given the slow pace of law enforcement regarding this point and the ineffectiveness of the criminal investigation into phishing, the financial institutions resorted to ISPs directly in order to remove the fraudulent websites instead of reporting the case and working with law enforcement agencies.

7.8.4. ISPs' work in regulating phishing

This subsection aims to examine how the ISPs of Taiwan have engaged in the anti-phishing work and the practical challenges encountered by the ISPs in dealing with phishing. This was primarily conducted by interviewing the representative (Interviewee D) from the information security department of Taiwan's largest ISP.[716] This subsection also attempts to generate an analysis of the opinions of the other interviewees about how the ISPs can refine their role and strengthen their participation in the task of combating phishing.

According to Interviewee D, the ISP participated intently in the tasks of TAPWG and worked closely with TWNIC in drawing up the anti-phishing policies and constructing the phishing reporting system by exchanging opinions at regular periodical meetings of the TAPWG and providing assistance with testing the operation of APNOW. The representative from TWNIC (Interviewee E) also stated that the ISPs provided solutions at the request of TWNIC to block all visit and access to a phishing website once it had been detected which had the least influence on the unsuspecting customers' connection to the Internet.

[716] This is the largest provider in Taiwan in terms of revenue and customer numbers for fixed line services, mobile services, Internet connection services, and other Internet services, such as web hosting or information and communication technology services to corporate customers.

Taiwan's ISPs plays a crucial role in the current anti-phishing network, especially in two respects: the proactive detection of phishing attacks via the disposal of honeypots and the taking-down of verified phishing websites as soon as they are detected or reported.

7.8.4.1. Proactive detection measures

Under the vertical reporting system directed by the NCC, the five leading ISPs of Taiwan are required to dispose honeypots in their central control room to detect malicious attacks by non-actively attracting attackers and to gather information about attacking activities, including the collection of malicious emails such as phishing messages. Nevertheless, the effectiveness of honeypots in terms of the detection of phishing, particularly targeted phishing attacks, was doubted by Interviewee D and the specialist (Interviewee F) from a world reputed company for security software. Interviewee F stated:

> A thing like a honeypot is hardly able to catch information about attacks. How do I let attackers know that we have a website here which is waiting for attacks? What makes an attacker target a honeypot among the enormous number of websites available? Attackers may sometimes blunder into the honeypot, which means that most honeypots can only detect the type of attack with unspecified targets but barely have a chance to attract attackers who have set a particular attacking object.

In addition to honeypots, the ISP attempted to prevent phishing emails, in the format of spam, from being delivered to users' inboxes through the use of a spam filter. For outbound emails, the ISP would stop users who had sent emails exceeding a certain volume within a short timeframe from continuing mailing. Although Interviewee D admitted the restricted function of the spam filter in detecting phishing emails, particularly targeted phishing messages, the interviewee stressed that it was an unavoidable situation under the requirement of privacy policy that should be observed by an ISP. Interviewee D stated:

> Being an ISP, we will never watch the content of emails because it is highly related to customers' privacy. We usually identify a spam email by only focusing on the mail header or other patterns which are usually related to a spam, and we absolutely won't touch the mail content. Therefore, we are unable to detect a targeted phishing email if it is undetectable without looking into its content.

Interviewee D also emphasized that the ISP only guaranteed the security of the web hosting server and provided pay services such as vulnerability scanning for its customers to strengthen their website security. However, as an ISP had to avoid interfering with the content of websites, it hence became extremely difficult for an ISP to detect a phishing website hosted on its server at the time when the website was created. Interviewee D claimed:

> So far, we have been unable proactively to spot phishing in most cases. We usually learn of the existence of phishing from the reports originating in Taiwan or other countries.

7.8.4.2. The taking-down of phishing websites

As aforementioned, reports were the major source for the ISP to learn about phishing. According to the statement by interviewee D, all of the reports of phishing were handled by the specialists of the Security Operation Center (SOC) at 24 hours. Once a report of a phishing website had been delivered, the SOC would test the website reported and block the Internet connection to this website by suspending the TCP Port 80 as soon as it was confirmed to be a phishing site and also return to the reporter in four hours. The SOC would capture the evidence from the phishing website and contact the user of the hosting machine by email or phone within 24 hours to ask that user to remove the phishing website. During the time before the phishing website was taken down, the ISP would continue to suspend the connection to the website based on the terms and conditions of the ISP service contract engaged between the ISP and the user.[717]

While Interviewee D claimed that the ISP's practice of suspension was adequately supported by the contractual agreement and it incurred complaints from customers only under very exceptional circumstances, Interviewee E mentioned that the ISPs of Taiwan sometimes were hesitant to take suspension measures in the absence of legal authorization. Interviewee E stated:

> In some cases, especially when the customer is also the victim, unaware that his/her machine has had a phishing page inserted, the ISPs have scruples about suspending the connection instantly because of their fear of being sued by the customer. This makes it pressing for NCC, the supervisory authority of the ISPs, to give an impetus to amend the Telecommunication Act to empower the ISPs to take the necessary measures in responding to phishing.

An amendment bill to the Telecommunication Act was drafted by NCC to explicitly allow the ISPs to discontinue providing Internet services where necessary to the protection of information and telecommunication security. In the meantime, it requires the ISPs to enable their customers to be aware of the potential disadvantages upon them if there is a violation against information security. The need to strengthen the legal basis to support the ISPs was also recognized by the official representative from NCC (Interviewee G). Interviewee G stated:

> The ISPs will hold back from disconnecting, especially when the attack is not that

[717] According to the terms of service contract, the ISP is entitled to suspend or terminate Internet services or terminate the contract under one of the following situations: if the user: 1. steals, alters or destroys the other person's information; 2. endangers the security of telecommunication or influences the other user's rights; or 3. sends email to other people without authorization which has caused persecution to the recipients.

> evident, if there is a shortage of distinct legal authorization. We drafted an amendment bill to the Telecommunication Act by adding an article which authorizes the ISPs entirely or partially to suspend or terminate their services while encountering grave information security incidents.[718] The ISPs are also obligated to enumerate the forbidden circumstances that may result from the suspension of the service contract and the ISP's operating instructions to enable their customers to be aware of the above information to the largest extent.[719] If the forgoing article becomes law, the NCC will be authorized to make rules for the ISPs to define the specific content of a 'grave information security incident'. Although we have been able to find similar stipulations in nearly all the ISPs' contracts, we believe that it will help the ISPs thoroughly to practise the suspension or termination of service according to the agreement without hesitation if their above actions are also clearly authorized by law.

7.8.4.3. Reinforcement of ISPs' responsibility to safeguard information security

To ensure the security of Internet services, the NCC's draft of the Telecommunication Act also requires ISPs to be responsible for taking specific information security initiatives, including establishing a security management system, installing safeguarding and detection devices, and setting up a collaborative defence and response mechanism to deal with reports of security incidents, handle these incidents and return to the reporter (Art. 55.1). The failure of ISPs to meet the requirements provided under Art. 55.1 and 55.4 attracts a fine of NT 60,000 -300,000 (Art. 86.1 (2)). Interviewee G emphasized that the above compulsory provisions were added to the Telecommunication Act in order to ensure the fulfillment of the ISPs' duty to safeguard information security. Interviewee G explained:

> I repeatedly highlight a conception at every meeting with the ISPs. The customers are your bread and butter. Since you are paid by your users for Internet services, you are naturally responsible for safeguarding the security of these services. An

[718] Art. 55.3 of the amendment bill of the Telecommunication Act.

[719] Art. 55.4 of the amendment bill of the Telecommunication Act.

> appropriate analogy would be that you build a highway and charge drivers toll fees. Of course, it is your duty to ensure the safety of the highway by setting up traffic signs, maintaining the road or installing other facilities to protect the drivers. At present, we are unable to punish the ISPs if they fail to carry out their duty. This is why we need a compulsory provision to force the ISPs collaboratively to protect and safeguard the security of information and telecommunication.

7.8.4.4. Challenges to the ISPs' work

Interviewee D saw the general lack of awareness about self-responsibility involving information security among Taiwanese users as the major challenge to the ISP's work in dealing with information security incidents. Most users recognized neither the necessity of securing their computers nor the potential threat it might cause to information security in relation to themselves and other users if they failed to protect their computer. Interviewee D stated:

> In our experience of dealing with botnet, we find that the users whose computers have been identified as suspected bot-infected machines often do not realize their responsibility to keep their computers secure from being exploited for malicious use. In most cases, the users see themselves as innocent victims and don't feel that there is a need particularly to strengthen the security of their computer even after we inform them of the security problem with their machine. There is an apparent lack of users' consciousness of individual responsibility in respect to information security as a participant in the cyber world. We also feel a lack of users' perceptions of the interrelation between their behavior and the integral security of the Internet network.

Another setback for the ISP's work in combating malicious attacks was the low willingness of the users to coordinate with the information security policy of the ISP. The ISP interviewed made considerable effort to help its users to protect their computer against invasion or infection; however, it received very limited feedback from the users. Interviewee D stated:

> Being an ISP, we often suggest that our customers should install at least anti-virus software or take some measures to protect their computer, but we find that, overall, the purchase rate of anti-virus software has been rather low. Although we have made great effort to contact the customers who may have computer security problems and give them advice about how to solve the problem, our work appears unhelpful in raising the awareness and motivation of users to secure their computer. They usually won't take any measure such as virus scanning or reinstallation unless we suspend their connection. I've been dealing with this kind of cases for many years but I feel very frustrated about this situation.

To sum up, the ISPs play a key role in Taiwan's anti-phishing work in both TAPWG and APNOW. Besides the participation in the policy-making work in TAPWG, the ISPs mainly function by taking phishing websites offline as soon as they receive phishing reports which may come from financial organizations or individual users directly or be forwarded via the platform of APNOW or NCC.

The interviewee from the ISP claimed that they had no scruples about taking down a phishing website immediately, as this practice was upheld by the agreements contained in its Internet service contract. However, the interviewees from NCC and TWNIC held different opinions and recognized the hesitation among ISPs to suspend an Internet connection right away in responding to a violation of information security in the absence of a distinct legal authorization. The interviewee from NCC also particularly highlighted the need to strengthen the legal requirement laid down in the Telecommunication Act for ISPs in respect of ensuring the security of the facilities and services and conducting specific initiatives for information security purposes.

In addition to the taking-down strategy, the ISP employed honeypots and spam filters in order to mitigate the threat of phishing. However, the above attempt proved ineffective in proactively spotting phishing activities, especially in the detection of targeted phishing attacks. The insufficient awareness among users about their roles and responsibility involving integral information security posed a crucial challenge to the ISP's work. The interviewee from the ISP also revealed a great frustration about users' noncooperation with the ISP on enhancing security measures to protect their computer devices from being exploited for malicious attacks.

7.8.5. Other problems with Taiwan's anti-phishing work

This subsection attempts to examine other problems raised up by the interviewees about Taiwan's anti-phishing work and find suggestions for improving the capability and strength of Taiwan in the fight against phishing.

7.8.5.1. Cooperation and exchange of databases on phishing

Interviewee E expressed an intention of the TWNIC to seek cooperation with other companies or institutions which also assembled phishing data, for example browser industries or Internet search service providers, to facilitate the exchange of information and databases on phishing in order to deal with the phishing websites hosted in Taiwan more effectively. Interviewee E stated:

> We are trying to contact some organizations to build up a cooperative relationship in order to exchange information and databases about phishing. For example, Internet Explorer has done a lot of work to prevent its users from visiting suspicious phishing websites. If they pass the list of blocked phishing websites to us, we can remove those websites rather than solely blocking visits. Also, if we can obtain more information about malicious websites generated through web search engines from search service providers such as Google, we can take these known phishing websites down or cope with them in a better way. It needs some time and more communication still needs to be done, but we will continue to look for more possibilities to establish cooperation with relevant companies or organizations.

However, the representative from Taiwan’s top-ranked company in terms of market share for anti-spam products and services (Interviewee H) mentioned that they used to consult with TWNIC for the purpose of interchanging research data but they received a negative answer. Interviewee H stated:

> We used to talk to TWNIC to see if it was possible to exchange research data about botnets, but they were unable to cooperate with us in this aspect. We have barely had any discussion with them on this issue since then.

Notably, in responding to the question about engagement in cooperation, Interviewee H revealed a preference for working alone, building up its own database for the company’s exclusive use and showed no interest in coordinating with other companies or institutions, especially if this cooperation model was directed by the government. Interviewee H stated:

> We would prefer to establish a research unit on our own. In fact, we already have an anti-spam research centre which not only conducts research on spam but also continues to accumulate data about spam mails. As our company is the only sponsor of this research centre at present, the research outcome and database currently are not released to the public but exclusively used by our company for developing our commercial products.
>
> In our long-term plan, we’re considering making our database available to domestic or foreign organizations for a fee if this research centre can be independently operated but, given the difficulties of harmonizing the different views posed by various stances, we would prefer not to cooperate with others but do the work on our own in order to have better control.

Furthermore, Interviewee H pointed out the major differences between a government-directed cooperation scheme and a non-government-based cooperation model in terms of the attitude towards operations, flexibility in the management of funds, and coordination of the conflict of interests between the participants. Interviewee H stated:

> There is a huge difference between the fundamental standpoints and perceptions of the government and non-government organizations so that it is hard to expect the government to establish a cooperation scheme from the angle of a commercial operator. The government officials always make us undertake a particular task by ordering but they barely consider the reasons why we should take the orders if we don’t mutually benefit from the same thing. It is absolutely unacceptable to be forced to contribute only, without being given any favour.
>
> The fund is also a problem, as it involves a government budget which does not allow us to manage and control it in a flexible way. Another problem is the coordination among different information security companies. These companies are usually the main contributors but very often they are also industrial competitors. It will be a hard challenge to the government to deal with the conflict of interests between members.

7.8.5.2. Training and education of information security specialists

The insufficient ability of information technology personnel (IT personnel) of businesses to ensure web security and properly respond to information security incidents was deemed by some of the interviewees as a major weakness in effectively combating phishing. According to Interviewee F, this was largely caused by the fact that the enterprises failed to give adequate weight to the information technology department and to respect the professionalism of information security. Interviewee F stated:

> Generally speaking, the field of information technology does not receive

> appropriate attention from most enterprises in Taiwan. A majority of Taiwanese enterprises see IT as a department which only consumes money without bringing too much benefit. Thus, these enterprises usually ask their IT personnel to be an all-purpose engineer who needs to do all of the works related to computers, the Internet, or even machines in order to save costs. I used to be asked to repair air conditioning and fire equipment when I was a web engineer for a private corporation before. Taiwan's enterprises are used to ask their IT personnel to do as much work as possible, no matter if they are capable of doing so. Unreasonable workloads on IT engineers have, in fact, resulted in great vulnerabilities in the websites of many enterprises in Taiwan. Unfortunately, this is a common failing in Taiwan.

Interviewee F pointed out that the size of enterprise was a key factor in determining the amount of resource available to information security work. Since small and medium-sized business (SMBs) form the majority in Taiwan,[720] it was hence difficult to expect most of Taiwan's businesses to employ an IT engineer to take charge of information security. In the opinion of Interviewee F, the IP personnel in Taiwan's private sector generally had a weak capacity for responding to phishing incidents, which highlighted the need particularly to strengthen the ability of the IT personnel to serve as a competent first responder. Interviewee F stated:

> I feel that Taiwan's IT personnel should improve their first responder ability. In the field of computer forensics, a first responder is the person who first arrives at the crime scene. This person does not necessarily need to have excellent, sophisticated computer skills but he needs to clearly know what necessary evidence he must preserve, to the least extent. If I were a first responder, I have to cordon off the scene as soon as an information security incident is detected. It didn't matter whether I knew how to analyze the evidence or not, as the main task of a first responder is to preserve the integrity of the evidence. Once a first responder fails in his/her task, the following investigation and analysis of evidence will become useless.

[720] See Chapter 3, section 3.3.2.

While Interviewee D from the ISP considered that the solution to improving the capacity of IT personnel in responding to and dealing with information security incidents should be grounded in school education, Interviewees F and H recognized that the systematic development and planned training provided by a selected group of information security professionals should be prioritized.

Interviewee F stated:

> It requires a long-term training and a rich-resourced environment. Sound learning under the guidance of information security experts and an adequate knowledge base are the two essential elements in developing competent information security engineers. Finding several seeded companies which conform to the above two conditions to take on training work may be worthwhile considering.

Interviewee H further attacked the government's neglect of national cyber security in terms of fostering and retaining information security talents. This exposed the sensitive information systems and networks of government agencies to an increasing threat of cyber-attacks, particularly the malicious attacks launched by China's Cyber Army.[721] Interviewee H claimed:

> In fact we have many top hackers in Taiwan but the government seldom considers systematically recruiting these people. Taiwan has been a well-known attacking object of China's Cyber Army. Although several hackers in Taiwan have attempted to create an underground defence against attacks originating from China, individual effort solely based on voluntary action can only produce very limited effects. I feel that the government really needs to concentrate more on this problem. There is still a lot of work to be done by the government either

[721] May 2011 bought a revelation that China's military had set up an elite Internet security task force, called the "Cyber Blue Team". Being the core force of the People's Liberation Army, it was constituted of 30 members and organized under the Guangdong military command in the country's south. Although China's Cyber Army was created to fend off external cyber-attacks, more and more countries alleged that it was in fact designed for launching immense cyber-attacks on the computer systems of governments and corporations worldwide. Yu, Eileen (2011), 'China dispatches online army', *ZDNet*. <http://www.zdnet.com/china-dispatches-online-army-2062300502/>, accessed September 12 2014. The intense malicious cyber-attacks from China to Taiwan, see Chapter 3, section 3.3.4.

> systematically to organize these information security talents or to employ them to find and train more information security specialists and thereby reinforce Taiwan's cyber defensive strength.

7.8.5.3. Promotion of users' awareness of information security

While the promotion of users' awareness of information security was recognized by most of the specialists interviewed as an essential solution to combating phishing, it was also regarded as the most difficult part to address. Not only had the interviewee from the ISP experienced significant difficulty in improving users' awareness of information security, but the interviewees from NCC and the information security service provider also mentioned the dilemma of having users to act in coordination with the necessary practice in order to protect themselves from falling victim to cyber-attacks. Interviewee G stated:

> Dealing with the computer security problem existing at the user end is always the toughest work. This is also a common consensus reached by different countries at some international conferences and meetings that I have attended. We may inform users of the security vulnerabilities that have been detected on their computers and suggest how they can fix them with patches[722] or by re-installment. However, we have no alternative if a user chooses to ignore our information except that the security problem of this user's computer has endangered other users. It is hard to expect every user to know about information security.

Interviewee F demonstrated that most customers were unwilling to take security measures in coordination with the advice given by their information security consultants unless certain damage had occurred.

[722] A patch is a piece of software designed to update a computer program to improve its usability or performance or fix problems such as security holes and bugs. See: http://en.wikipedia.org/wiki/Patch_(computing).

> In most cases, the victims are not conscious that they have become victims and usually are loath to work with you as they think it is your problem. They will start to act in coordination with your advice only if the security problem has physically caused damage to them.

Interviewee G suggested two ways to improve users' awareness of information security: fundamental school education and assistance from ISPs with detecting and dealing with security vulnerabilities. Interviewee G stated:

> The current education has apparently fallen behind the fast-changing development of information technology. This proves that there exists a need to strengthen information security education, particularly fundamental school education, to improve public awareness of information security. Another way is to enhance free or pay service of ISPs to help their users to ensure the security of their websites or devices by making regular vulnerability checks or removing threats.

7.9. Conclusion

Phishing demands a broad understanding of regulation which refers to any force that makes it possible to prevent or interrupt a phishing attack. Regulation of phishing can be a piece of legislation, a computer program, a management initiative, or even an educational programme, as long as it can effectively increase the cost or difficulty to attackers to perform phishing or reduce the probability of attackers to succeed. This chapter considered a multi-dimensional regulatory framework which primarily consists of law, technology, education and institutional networking. While the previous chapters have focused on the legal regulation of phishing, this chapter examined the other three form of regulation in terms of their respective effect and limitation on phishing control.

Technology features largely in the fight against phishing and has served as the front line of defense through proactive detection of phishing at email or website level. However, a number of usability studies demonstrated the ineffectiveness of technical tools in preventing users from falling for phish, as users often explain away the warnings of anti-phishing toolbars or ignore suspicious signs coming from the browser security indicators due to a lack of a baseline level of security awareness. Phishing is a typical social engineering attack which exploits the weakness in human nature and also takes advantage of users' inability to distinguish spoofed emails or websites from legitimate one. Education is used as the baseline of defense by teaching users to spot phishing and prevent them from engaging in potentially risky activities. However, the difficulty of inspiring users' motivation of pursuing education and the obstacles to transferring education materials to users' secure online behaviours are always the problems that may negatively influence the effectiveness of education measures. Notice-and-takedown is another dominant anti-phishing approach based on institutional network which functions by removing a phishing website as soon as it is detected in order to minimize the potential damage and victims that the site may cause. However, the phishing sites that are hosted in free web-hosting environment or on compromised machines, in particular fast-flux and rock phish sites, have posed a crucial challenge to takedown strategy. The actors responsible for phishing takedown are not equally-cooperative and some of them, especially domain registrars, may even disregard the removal requests. This can be addressed by ICANN by setting standards for registrars and registries to respond to domain abuse and enforcing compliance through accreditation mechanism.

There is no single perfect solution that can adequately deal with phishing, as each countermeasure has its strengths and weaknesses. This chapter does not intend to provide a flawless strategy but suggests the essential elements that should be included in the regulatory framework for phishing. A combined approach that comprises laws, technology, education and institutional network may be an approach that merits substantial consideration.

An effective anti-phishing strategy largely relies on the joint efforts of the stakeholders from various fields. The establishment of the TAPWG and the APNOW showed that Taiwan is in a right direction, but whether these initiatives can practically produce effect on combating phishing still remains a question. This chapter observed several problems from the APNOW based on the existing available resources and data and suggested that it should endeavor to reduce the process time required of takedown, continually monitor the phishing sites that have been taken down, improve its visibility and usability, and enhance immediate communication with Foreign CERTs.

Nevertheless, the existing Taiwanese literature only provides general background information about the current anti-phishing initiatives. There is a lack of scholarship that examines the role and contribution of different stakeholders in Taiwan’s anti-phishing community. Moreover, all the information about the internal operation of TAPWG and the statistics regarding APNOW’s process times are not unveiled publicly but only shared among their members. Given the shortage of research-based literature, I conducted an empirical study to synthesize the opinions of the key persons from different organizations involved in order to provide insight into the efforts that various stakeholders have devoted and are expected to devote to anti-phishing work combined with the difficulty that they have experienced in combating phishing.

There were several key findings. The cross-border nature of phishing posed a huge challenge for Taiwan’s investigators in tracing phishing perpetrators even though Taiwan is the member of the G8 24/7 network. The weak legal enforcement of phishing led to a general mistrust in the regulatory power of laws and also undermined the intention of the financial institutions that were likely to be spoofed to work with law enforcement agencies when they detected a phishing site.

The ISPs were identified as being in a key position in combating phishing. While going to the ISPs directly to take phishing sites down was generally regarded to be a more efficient method of dealing with phishing, the ISPs sometimes were hesitant to take suspension measures. An explicit authorization by law was considered helpful to back up the ISPs to take the suspected phishing sites offline immediately after verification without hesitation. Another major deterrent to the ISPs' anti-phishing work came from inadequate customers' awareness of computer and information security. Most customers were unconscious of their responsibility in respect of information security and therefore seldom to act in concert with the security policy of the ISPs.

There was currently no significant development of cooperation and information sharing in terms of phishing between the stakeholders. The government and industry usually had different requirements and expectations about a cooperation model, and it is hard to achieve co-ordination or reconcile conflicting interests of stakeholders.

The major weaknesses of the anti-phishing work were identified to lie in the lack of users' awareness of information security and insufficient capacity of Taiwan's businesses, in particular SMBs, for ensuring web security and respond to information security incidents. Therefore, in terms of suggestions for further work, the priority was placed on effective education of users that can promote users' knowledge and awareness about phishing and information security and systematic training of IT personnel that can enable competence in ensuring web security and properly respond to phishing.

CHAPTER 8 CONCLUSION

The increasing threats to information privacy and the great costs to society have inspired growing demands for the regulation of phishing. However, the question is: how can we effectively regulate phishing? It can also be asked in another way: how can we effectively prevent phishing or diminish the damage that phishing is likely to cause? In my opinion, the regulation of phishing can be achieved in two ways: increasing the cost or difficulty of performing phishing and decreasing the possibility of successful phishing.

An analogy would be if we wished to prohibit any person from approaching a lake to fish. We could position a warning notice by the lake, saying ‘No fishing allowed. Violators will be punished or fined’. We could also build a fence around the lake to stop fishermen getting close to the fish or establish an alarm system which will report to the patrolman if someone casts a hook into the water so that the patrolman will come to cut the fishing line as soon as he has been alerted. Teaching fish to be more skilled in distinguishing real food and lures is also a way to protect them from being hooked.

There are many possible ways to deter fishermen or prevent successful fishing, but there is no perfect solution that can provide a watertight safeguard. Fishermen are very likely to ignore the warning notice if they feel that they are very unlikely to be caught. A thinking fisherman can also easily get through the fence as long as he can find a crack or successfully bore a hole in it. A patrolman may be able to stop the continuation of fishing, but would be unable to determine how many fish may have been caught before he arrives and when or where the fisherman will return. Fish have a great chance to take the bait if they fail to detect a lure due to inadequate knowledge or do not fully perceive the danger that the lure may pose for them.

In terms of regulation of phishing, law serves as a typical deterrent by imposing a threat of punishment. Law can also be used to promote security, privacy, and anti-phishing conscious behaviour among technology providers. Technology features largely in the regulation of phishing, as it physically constrains phishers from performing attacks through the codes embedded in the hardware and software. Institutional networking controls phishing by monitoring or interrupting the performance of phishing through close cooperation encouraged where appropriate by legal measures between different institutions involved. Teaching users to spot phishing signs and act as an educated user about information security is also an important measure helping users to stay from phishing traps which in turns reducing the probability of success of phishing.

Each form of regulation can produce different regulatory effects upon phishing, but their effect is limited in certain aspects. Given the unique function of different forms of regulation combined with their strengths as well as weaknesses in combating phishing, this research proposed a multi-dimensional regulatory framework incorporating the countermeasures developed in various areas, including legal, technical, educational, and institutional networking, in order to maximize the regulatory power at each step of the process of a phishing attack.

This research examined the regulation of phishing in Taiwan, with a primary focus on law but also other forms of regulation, and, because of the transnational nature of phishing, law and regulation in other domains and the interaction between Taiwan and international regulatory interfaces. This concluding chapter revisits the research questions set out in the Introduction to draw conclusions about the examination of each form of regulation – what their respective roles are in the fight against phishing, how they have been developed to date and the factors that may impede their effectiveness. It also includes suggestions for the future development of Taiwan’s multi-dimensional regulatory framework to strengthen the overall defensive and responsive capacity against phishing and improve the domestic and transnational cooperation between different regulatory bodies.

8.1. Legal regulation – an essential but weak countermeasure

This study has raised concerns about the effectiveness of the traditionally national legal approach of criminalization of phishing as well as of the international approach of harmonization of legal standards and cross-border cooperation between legal enforcement agencies.

8.1.1. Gaps between laws and phishing

Outlawing phishing is the first step to make a phishing attacker accountable for his conduct and is also the fundamental work to enable the universal criminalization of phishing in order to achieve effective international regulation of phishing. As phishing is generally not regarded as a sui generis problem, most countries usually deal with phishing by upgrading existing provisions to cover phishing or doing nothing but applying the existing law to phishing. The research examined the criminal laws in Taiwan and also other countries such as UK and USA as well as the relevant international laws relating to cybercrime and found that there have existed several gaps between the coverage of these laws and the true context of phishing, which raise a question about the capability of legal regulation to deal adequately with phishing.

It found that most of the gaps between laws and phishing results from inadequate understanding of the characteristics of phishing and insufficient consideration of the compatibility of the elements of the provisions and phishing.

8.1.1.1. Misunderstandings of the nature of phishing

A clear understanding of the nature of phishing is very important to identify the true context of phishing so that we can easily recognize the elements that have been legally addressed and those that may have been missed.

Phishing can be carried out by both social engineering and technical subterfuge schemes, which may involve illegal access to computer storage along with malware infection but not always the case. A phishing attack may target a variety of confidential information, ranging from financial or personally sensitive information to business or even national security secrets, which usually do not have business value and cannot be transacted. Although many phishing attacks are motivated by financial gain, the target of phishing is actually obtainment of confidential information which may not necessarily yield financial profit. Phishers may make profit directly from solicited data but can also exploit it as a stepping stone for subsequent malicious use. Most importantly, phishing is not an offence against property but an offence against information security. As, unlike a physical movable property, an electromagnetic record is duplicable in nature, acquisition of certain sensitive information is very often not accompanied by a loss of data subjects or data controllers of that information. Obtainment of confidential information does not necessarily mean monetary damage to data subjects or controllers. The damage that phishing is likely to cause includes not only direct loss of money or goods but also indirect cost used to redress phishing as well as loss of potential customers or damage to credit or reputation. The reason why phishing demands criminalization is not because it causes violation against property interests but it constitutes infringement of information security which involves computer security and information privacy.

8.1.1.2. Phishing is not equivalent to identity theft or identity fraud

Phishing is a malicious cyber activity that directly targets the obtainment of personal, financial or other confidential information by masquerading as a trustworthy source to deceive users into rendering target information or gaining direct access to data storage through malware infection. It consists of two elements: object (confidential information) and two acts (using the identity and obtaining information).

In some countries, such as the US and UK, the criminalization of phishing is covered by the offence of identity theft or identity fraud, under the umbrella term 'identity-related crime'. While there are certain overlaps of the elements between these two offences and phishing, this research argued that they are unable to fully cover phishing but only partially. Phishing is similar to identity theft, as both activities usually involve the unauthorised use of another person's identity. However, the object of identity theft is only specified for identity-related information while the object data of phishing can include not only information related to identity but also a variety of confidential information concerning a person, corporation or country. Phishing is also similar to identity fraud, as it also uses false identity to defraud someone. Nevertheless, identity fraud concentrates on monetary or financial gain whereas phishing may do so but not always.

8.1.1.3. 'Obtaining' information, not 'stealing'

Taiwan introduced two major legal amendments in 1997 and 2003 which brought the Criminal Code of Taiwan into a new era in responding to the rise of new forms of offences committed by computer technologies and Internet networks. The 1997 Act provided electromagnetic records the same legal status as a movable property and expanded the object of property crime, such as larceny or fraud, from physical property to electromagnetic records. Nevertheless, the lawmakers apparently failed to take into account of duplicable nature of electromagnetic records. The obtainment of an electromagnetic record by duplication does not simultaneously destroy the original possession of that record so that such obtainment is unable to satisfy the elements of larceny. The above incompatibility also happened in fraud law. In short, electromagnetic records, strictly speaking from a legal perspective, can only be ‘obtained’, not ‘stolen’.

8.1.1.4. Consent obtained by fraud is not an authorisation

The 2003 Act, which took the CoE’s Convention on Cybercrime as a model, created a sui generis chapter for the regulation of the offences against computer use and electromagnetic records. This Act removed electromagnetic records from the objects of the larceny law and replaced it with Art. 359 which deals with obtainment of electromagnetic records from another person’s computer or related equipment without authorisation. This removal also produced the same effect, mutatis mutandis, on the law of fraud. The 2003 Act was particularly important to the regulation of phishing, as it explicitly provided protection for information security by granting electromagnetic records an independent legal status separate from the general movable property protected under the larceny or fraud law.

The enactment of Art. 359, theoretically, should have put an end to the debate over whether the larceny or fraud law is applicable to the case of illegal obtainment of electromagnetic records. However, researchers still argued that phishing should be dealt with by the fraud law, as Art. 359 can only apply to the case where the obtainment of data is undertaken without the awareness of the victim; for example, phishers access the data storage by malware infection. In the case where phishers deceive another person into giving away his information is not unauthorised obtainment as this obtainment is carried out under consent, even if fraudulent.

This research questioned the above approach and suggested that ‘unauthorised’ should be seen as a special element purposely laid down by the lawmakers in the offences against personality and should not be excluded by the excuse that applied to the offence against property. In addition, the commitment of the offence of fraud requires an occurrence of actual damage to property (Art. 339). It argued that this is unlikely to happen in the case of phishing unless the targeted information itself has business value and this value will transfer to phishers immediately following the delivery of information.

8.1.1.5. The main concern about phishing is its threat to information security, not property

Acquisition of another person's electromagnetic records without authorisation does not constitute an offence if no damage has been caused to that person or to the public pursuant to Art. 359. But the question is: what is the context of damage and how to determine whether damage has been caused?

There is a difference of opinion between researchers and the judges of Taiwan. For researchers, the damage does not have to be monetary damage and should be capable of a broad interpretation; but for the judges, a person should not be found guilty if the record has no value or the obtainment has not resulted in monetary damage. Judges see unauthorised obtainment of electromagnetic records as an offence against property, even though the 2003 Act clearly indicated that Art. 359 was intended to protect information security. This judicial interpretation opens a loophole where the victim fails to specify his monetary loss. This research suggested that it is necessary to escape from the old thinking and adopt a broad interpretation of damage under Art. 359.

The various gaps between law and phishing raise questions about the capability of the Criminal Code in addressing phishing and suggest the need to consider alternatives.

8.1.2. The role of information privacy protection

8.1.2.1. The role that has been ignored

Law can not only serve as a corrective measure which constrains phishing through coercion or punishment but also act as a preventative through ensuring protection of information privacy, an area which has been ignored in current legal discussion. This research suggested that, apart from being a direct infringement of information privacy, phishing is often used as a leading vector for data breach which usually involves exploitation of personal information gathered from social networking sites. More and more phishing attacks, especially spear phishing, target enterprises and even governments rather than end users, as the attackers can easily walk off with enormous personal data as long as they can get the key to the database systems. The abundant personal information available on social networking sites, in this case, provides the best materials for phishers to craft a highly convincing lure to gain a toehold in a specific target's environment.

There is a complementary relationship between phishing and data breach. While phishing largely enhances the chance of attackers to successfully breach a database system, the huge amount of stolen personal data obtained from data breach, on the other hand, also greatly promotes the creation of numerous phishing scams. There is a need to ensure the legal protection of personal information, especially in respect of maintaining the confidentiality of personal data, strengthening data controllers' obligation towards security of data, and reinforcing individuals' control and choice regarding their information in order to achieve effective legal regulation of phishing.

8.1.2.2. The awkward position of the Personal Information Protection Act of Taiwan

This research examined the legal frameworks of personal data protection that have been developed at three different levels, including global, Asia-Pacific region, and Taiwan national level to explore the interaction between different regulatory interfaces, with a primary focus on the analysis of whether the personal information protection law of Taiwan is able to provide adequate protection of personal information in responding to the requirements raised from the regulation of phishing.

Taiwan started its legislation work on personal data protection in the 1980s and passed its first data protection law, which was largely built upon the OECD Guidelines, in 1995. In order to better harmonize with international standards of personal data privacy, Taiwan additionally incorporated several data protection principles set out in the EU Directive and adopted the APEC Privacy Principles in its enactment of the PIP Act, which was passed in 2010 and came into force in 2012. The PIP Act made several key amendments to the previous law which were seemingly very useful in offering a more comprehensive protection for personal information but in fact did very little to limit phishing, as the devil is in the detail.

The PIP Act not only failed to redress the pre-existing problems of the previous law but also appeared to be incapable of providing effective protection for personal information and even caused a reverse-effect on the data protection against phishing. The fundamental problem lies in the failure of the lawmakers to achieve a balance between the protection of two values - the value of information privacy and the value of efficiency of data collection, processing, and use. This argument was based on the following defects observed in the Act.

Ample exceptions to data collection prohibitions and improper use of indeterminate legal concepts

In 2004, the constitutional status of the right of privacy was for the first time recognized by the Taiwan Constitutional Court, which further defined the right of privacy as "*the right to decide whether or not to disclose their personal information, and, if so, to what extent, at what time, in what manner and to what people such information will be disclosed.*" The right of information privacy is a recognized fundamental human right which can only be restricted by explicit laws under very exceptional circumstances pursuant to the Constitution. However, the PIP Act provided ample exceptions for both government and non-government agencies for justifying their collection of personal data, with little respect for information privacy.

Moreover, it largely used different indeterminate legal concepts in its provision in relation to the exceptions to data collection prohibitions. The use of indeterminate legal concepts itself is not improper and sometimes is unavoidable given the flexibility for administrative authorities in determining its content. However, their excessive use raises questions of propriety, especially currently Taiwan in the absence of a specific authority to deal effectively with disputes. This indeterminacy in legal protection of personal information even indirectly encourages phishers to leverage efforts to obtain personal information from so-called ‘publicly available resources’, irrespective of the awareness of the data subjects, for subsequent malicious use.

Insignificant distinction between identifiable information and de-identifiable information

The term ‘personal information’, according to the PIP Act, referred to the information which may be used to identify a natural person, both directly and indirectly (Art. 2(1)). This research questioned the significance of distinguishing ‘identifiable information’ from ‘un-identifiable information’. The line between these two kinds of information has become blurred, as supposedly anonymous information can still be linked to an individual through a combination of anonymous data or a use of technology. More importantly, the constraint on the scope of personal information leaves an unregulated circumstance in which the information is sensitive to a person but may not be linked to him, such as financial information that has been at the highest risk of being phished. The context of personal information should not be subject to discrimination based on whether or not it can be used to identify a person and should include all data that is closely associated with a person.

Disadvantaged position of data subjects

Taiwan’s personal information protection law, as aforementioned, has no specific authority to supervise the data controllers and monitor their compliance with the laws, and where necessary, prosecute and sue corporations which fail to comply with the legal requirements leading to the theft of personal information. An independent privacy protection authority is not only important for dealing with disputes over indeterminate legal concepts but also particularly valuable to ensure the protection of data subjects by representing the interests of individuals to compete against the power of the government agencies and large, wealthy corporations.

Compromise to data controllers

The increase in the prohibition and liability of the data controllers with regard to the unauthorised collection and use of personal information in the PIP Act created extreme anxiety among both government and non-government agencies. The PIP Act, particularly the prohibition of collection, processing or use of special categories of data (Art. 6), the criminal liability for non-compliance with the Act (Art. 41) and the one year notice duty (Art. 54) led to strong complaints among Taiwanese enterprises about the difficulty of implementation. The continuous interventions by these enterprises deterred the enforcement of the PIP Act for 28 months and, in consequence, they have successfully impeded the enforcement of Art. 6 and 54 and also propelled the government to initiate re-amendment to the Act by adding two extra exceptions to data collection prohibitions easing the notice duty of the controllers.

There was a fundamental difference in the expectations regarding the PIP Act between the data controllers and subjects. The primary concern of enterprises was how they can ‘legally’ collect individuals’ personal information to the maximum standard while decreasing their risk of being punished or sued for compensation to the minimum standard. Very little consideration has been given to improvement of the protection of information privacy by reducing the unnecessary collection of personal information and underpinning security measures to safeguard information against illegal access such as phishing. The regular compromise towards data controllers reveals the lawmakers’ bias in favour of the convenience and efficiency of data collection and against the information privacy of the data subjects.

8.1.3. Challenges to legal enforcement

While the power of legal regulation, to a certain extent, depends on successful prosecution and conviction of criminals, the transnational and transient nature of phishing has significantly increased the difficulty for law enforcement agencies to trace and prosecute phishing perpetrators. The challenges posed by phishing to law enforcement work have to be addressed by international harmonization of legal standards and cross-border cooperation between law enforcement agencies, which is not an easy task to achieve if there exists no mutual legal assistance agreements and is particularly difficult for Taiwan which suffers from political obstacles in engaging in international conventions and cross-border cooperation.

8.1.3.1. General challenges and corresponding measures

Phishing, by its transnational and transient natures, has caused problems for law enforcement. A phishing attack usually involves two or more jurisdictions, but cross-border investigation is not made possible without cooperation of the law enforcement agencies in all of the countries involved. MLA has been an essential tool to achieve law enforcement cooperation which is on dual criminality, but dual criminality sometimes becomes a necessary requirement when it comes to coercive measures such as search or seizure which are often required in phishing investigations. It is hence very important to ensure the prevalence of the criminalization of phishing and promote the consistency and compatibility of the national laws by establishing transnational legal standards to eliminate safe havens for phishers and diminish uneven regulation of phishing resulting from the divergence between the phishing laws of different nations.

The CoE's Convention on Cybercrime is the first and the only binding international instrument to deal with cybercrimes, which represents a significant step forward in fighting cybercrime by providing a fundamental basis for European countries as well as many countries outside Europe to formulate their national laws on cybercrime. This research found that while the Convention deals with the falsification of scam emails (Art. 7), access to a computer system by malware infection (Art. 2), the obtainment of information by interception of communication through technical means (Art. 3), and the possible fraudulent use subsequent to obtaining the information (Art. 8), it fails to address the act which features largely in phishing – a social engineering attack. A review of the Convention in respect of the regulation of phishing is therefore necessary.

The transient nature of phishing is another crucial challenge to legal enforcement. Phishing websites usually exist for only few days or even few hours and the speed at which phishers can shift to another sever after the bogus sites have been taken down largely increase the difficulty of investigation and place the law enforcement agencies under heavy time pressure to identify and trace of phishing perpetrators. Cybercrime investigations are time-sensitive, which makes it an imperative to ensure the close cooperation and timely communication between law enforcement agencies. To keep up with the need for rapid cybercrime investigations, there has been an international progress in the establishment of 24/7 contact points to provide assistance in the preservation of data, collection of evidence, and location of suspects.

The creation of G8 24/7 Network in 1997 set a dominant model for a number of international protocols to construct a 24/7 network to speed up the communications between countries and expedite investigations against cyber criminals. However, whether or not the 24/7 network is practically effective in facilitating a global seamless web of legal enforcement against phishing is a question that remains unanswered.

8.1.3.2. Dilemma of Taiwan

Taiwan has been at great risk of phishing but also has been experiencing particular difficulty in pursuing effective cross-border legal enforcement. A major deterrent is its disadvantaged political status. Because of the political tensions between Taiwan and China, Taiwan has struggled to regain its pre-1971 international recognition status. In the circumstances, Taiwan has focused on membership of international organizations. However, pressure from China continues to impede Taiwan's attempts to take part in the international arena. Taiwan has long been excluded from most international organizations and has been prevented from being a signatory to a great majority of international conventions, but has been permitted as Chinese Taipei to join the G8 24/7 network.

This research provided an analysis of the data collected from the interviews with the key persons selected from different regulatory bodies in Taiwan, which revealed a general mistrust about the effectiveness of Taiwan's legal enforcement in phishing cases. The weak legal enforcement was attributed to several factors, but the transnational element of phishing was regarded as the most crucial barrier to investigation, as it was almost impossible for the investigators to track the IP any further once the phishing site had been identified as being housed in a foreign country due to a lack of MLA. In spite of Taiwan's membership of the G8 24/7 network, it has been very difficult to seek assistance from other countries even in cases involving national security. This is largely due to the different procedural requirements in countries for launching an investigation. While many countries require a court order before certain investigative actions are triggered, it has been practically difficult to have a court order if the case is unrelated to the requested country, especially when it only concerns damage and victims in the requesting country.

The analysis also demonstrated that ineffective law enforcement undermined the intention of other stakeholders, especially the potential victims such as online merchants, to cooperate with the law enforcement agencies when they detect a phishing site. In addition, the priority of the merchants was how they could enable a spoofed site to be shut down as soon as it was known, whereas the law enforcement agencies focused on evidence collection which may require the bogus site to be kept active for a certain period. Therefore, the merchants tended to resort to ISPs directly for removal of phishing sites instead of working with law enforcement agencies.

Although law has been an essential regulator in the both real and virtual world, its regulatory power is hardly fulfilled if it fails to increase the risk experienced by perpetrators of being prosecuted and make them accountable for their conduct. This research suggested that while legal regulation is important, it has to be located within a broader multi-dimensional regulatory framework in order to effectively combat phishing.

8.2. Technology – the defective front-line countermeasure

The technical regulation of phishing refers to any software or hardware that physically constrains the performance of certain behaviours involved in a phishing attack. Significant technical countermeasures have been developed to interrupt phishing at different steps, and most of which focus on detection of phishing to prevent phishing emails from reaching intended recipients or prevent potential access to phishing sites. This research considered various technical approaches for identification of phishing emails; for example spam filters, phishing emails classifiers, and email authentication or for detection of phishing sites such as blacklisting and heuristic-based approaches.

Technical tools are often used as the front line of defence against phishing. While much work can be done technically to detect phishing, a solution that can perform flawlessly is unlikely. At the early stage, spam filtering techniques were prevalently used to prevent the delivery of phishing messages; however, it appeared inadequately effective to intercept phishing as soon as the phishing strategy became more sophisticated and targeted. Phishing classification is another popular approach which is capable of distinguishing phishing and legitimate messages automatically by learning specific features in the emails. While much research on phishing classification claimed to have achieved high accuracy in identifying phishing emails, false positive is always a problem for phishing classifiers to overcome. It is also necessary for the classifiers to keep updating their systems since the content of phishing emails is continually evolving. In addition, a content-based classifier is usually weak in detecting spear phishing which is highly personalized for a particular group or person and has no specific identifiable features. Sender authentication can help to reduce phishing by detecting spoofed emails. Both SPF and DomainKeys aim to validate whether an email comes from a legitimate domain; however, as a vast majority of phishing emails are sent from bot-infected or compromised computers, an email that has been verified as coming from a legitimate source does not necessarily suggest that it has been sent by the person it appears to be.

Considerable research has also been conducted into ways keeping users from phishing sites. Blacklisting, which is typically built into web browsers and available as a web browser toolbar, functions by checking the websites against a list of reported phishing URLs when a web address is rendered into a browser to prevent users from accessing suspicious phishing sites. However, this approach always suffers from the time gap between the appearance of phishing sites and the updating of the blacklist, as it always needs to take some time before a new phishing URL is reported and added to the blacklist. The lag before verification has been the major challenge to a blacklisting approach in protecting users from phishing sites in time. Heuristic-based techniques can estimate whether a given page is phishing by looking into certain phishing characteristics in URL or/and website content. Although a heuristic-based approach is able to intercept phishing sites as soon as they are launched with no need to wait for blacklists to be updated, it is very likely to produce high false positive rates due to the high similarity between phishing and legitimate sites.

The NCC of Taiwan required the five leading ISPs in Taiwan to dispose honeypots in order to detect phishing attacks by non-actively attracting phishing. Spam filtering was also a common method adopted by the ISPs to protect their users away from scam emails. However, some of the interviewees, including the interviewee from the largest ISP of Taiwan, admitted that the above attempts proved practically ineffective in intercepting phishing messages, particularly those, such as spear phishing, designed for specific recipients.

Having examined a series of technical countermeasures against phishing, this research found a flawless technical solution is almost impossible, as each has its advantages and disadvantages. Phishing tactics are constantly being modified and refined to exploit the vulnerability of computer systems embedded in software and hardware. It is like a race between the technology developer and the phishers, where the attackers can easily find ways to circumvent phishing detection by abusing the faults existing in the codes or launching zero-day attacks, the technology developers find it hard to predict the next step of the attackers.

Most importantly, phishing abuses the weakness of both computer infrastructure and humankind, and the variable of humans should also be taken into account in order to make any meaningful evaluation of the effectiveness of technological measures. Even if there was a perfect solution which could identify all phishing sites, the result of several usability studies showed that technology alone is not enough to combat phishing as users are very likely to bypass the warnings or ignore the clues that tell them that the websites are very likely to be malicious if they lack a baseline level of security awareness.

8.3. Education of Users – the unmanageable base-line countermeasure

An experienced fisher is skilled at luring fish to take the bait, and a skilled phisher is proficient at manipulating the weakness in human nature to entice users to respond to his requests. Phishing is a typical form of social engineering attack which attempts to persuade potential victims with appeals to strong emotions such as curiosity, excitement, or fear or creations of feeling of trust and commitment. In addition, most users find it difficult to distinguish deceptive sites from genuine ones, and even the most sophisticated users are likely to be fooled by a well-crafted bogus site. This highlights the need for the education of users, which serves as the baseline of defence to protect users from falling phish by teaching them to spot phishing and enabling them to engage in secure online behaviour.

A variety of anti-phishing educational materials is available online; however, this research indicated that users seldom look for these materials and tend to ignore the emails that direct them towards these. An interactive protocol in the format of games or tests is generally considered to be more effectual by providing a natural and interactive environment allowing users to assess their vulnerability to phishing or learn to spot suspicious phishing by doing. Several proposals for anti-phishing education programs have been put forward in both academic work and industry, most of which demonstrated satisfactory results in helping users to better identify potential phishing. Nevertheless, an alternative opinion argued that phishing tests only increase users' suspicion about phishing rather than improve their ability to recognize phishing. Some also questioned whether the knowledge provided can be really transferred to secure online behavior and how long the knowledge can be retained beyond the specific points it trained on. The most important factor that undermines the effectiveness of educational measures is the difficulty of inspiring users' motivation of pursuing education while most users only see security as a secondary goal.

The lack of users' awareness of information security and insufficient incentive to act in coordination with the security advices such as installation of anti-virus program or repair of computer infection were regarded by most of the interviewees as a crucial challenge to the anti-phishing work in Taiwan. Most users did not realize their individual responsibility in respect of information security as a participant in the cyber world nor did they recognize the potential damage it is likely to cause upon them and others if they fail to secure their computers. Although some of the interviewees stated that they had made significant efforts to customer education, they found this attempt proved unfruitful in raising users' awareness of information security.

A prominent feature of phishing is that it targets the weakest link in the security chain, namely human, which is almost impossible to manage and control. Education may serve as the best effective regulation of phishing if we assume that users are all aware of the need to pursue knowledge about phishing and act as educated users in responding to phishing attempts. Nevertheless, the above assumption can hardly be realized in reality. Users can be phishing conscious, as long as they realize how they are related to phishing and perceive the danger of phishing as well as the need to adopt secure behaviour in order to avoid being phished. To intensify users' motivation to learn how to detect and respond to phishing, it is important to strengthen their awareness of the correlation between their engagement in potentially risky behaviours and the huge damage that could cause to themselves and lots of other users.

8.4. Institutional Network – a cat and mouse game

Institutional networking is a regulatory device to constrain certain prohibited behaviour through national or international organized cooperation and connection between public and/or private institutions in different interfaces. The best example of the regulation of phishing in institutional network fashion is the notice-and-takedown strategy. A takedown scheme has been widely employed as a response to phishing attacks, which functions by removing fraudulent websites as soon as they are detected in order to minimize the potential damage and prevent more users from falling victims.

A takedown process usually starts when the brand owners, for example banks or financial institutions, or their contracted takedown company are alerted to existence of a spoofed site and then contact the hosting companies, the system administrators, or ISPs to bring that site down or go to the domain registrars to suspend the domain name. While the value of a takedown strategy lies in speedy communication between institutions and immediate reaction to have phishing sites shut down, smart phishers usually host their websites in the countries with inadequate legal enforcement resources to ensure that the process is as time-consuming as possible. Most phishers also host websites in free hosting web space or on compromised machines in order to evade being traced. In this case, a takedown company needs to approach the free web-hosting companies or the system administrators to ask them to remove the website or contact the ISPs to request a disconnection to the offending web pages. Research pointed out that phishing sites usually are removed speedily once the hosting companies and administrators receive the takedown request, but how long the phishing sites stay alive is primarily decided by how quickly the brand owners are aware of the existence of these sites.

However, in the case that attackers register a domain name especially for phishing use or operate rock-phish or fast-flux phishing network, the only viable way to remove the website is to have the domain name suspended. While domain registrars and registries are one of the key actors responsible for phishing takedown and stand in an excellent position in combating phishing, their reaction to phishing incidents is rather lagging. A study indicated that some registrars and registries will act upon complaints but the others will take no action due to limited manpower and resources and low incentive to spend money to address domain abuse. This research suggested that ICANN should exert a key influence over the response of the domain registrar community to phishing by setting standards of domain abuse for registrars and registries, ensuring compliance through the accreditation mechanism and intensify the incentive of registries to adopt anti-abuse policies by taking it as part of evaluation criteria for registry application.

While the removal of phishing sites may be helpful in reducing potential damage and number of victims by bringing the sites down in a timely manner, it is often perceived as an endless task because many phishing sites, especially those on compromised machines, are very likely to reappear shortly after they are first taken down and continue to make users fall for phish. Phishing attackers operate in real time whereas takedown measures can only be reactive in nature. This is like a cat and mouse game, and takedown companies always fall behind the phishers.

A notice-and-takedown strategy has been adopted as salient countermeasures in Taiwan to combat phishing attacks since 2010. Taiwan activated a phishing reporting platform known as APNOW in October 2010 which serves as an internal and external window for receiving reporting of suspected phishing incidents coming from a variety of sources. Once a phishing site has been reported, the APNOW passes to the corresponding CERTs or directly to the ISPs after a preliminary verification. The CERTs or ISPs then ask the hosting companies or administrators to repair or shut down the website in question. This process is required to be completed within 24 hours.

However, this research raised several questions regarding the practical operation of APNOW and questioned its effectiveness in combating phishing. One major problem is the delay in removing foreign-hosted phishing sites. As it still needs to rely on human operation where the phishing site reported is housed in other countries, in this case which is very often true in the phishing attacks that target Taiwan users, the takedown process is free of the time frame based on the 24-hour requirement. While the speed to have a phishing site removed is the key determining the effectiveness of a takedown scheme, it is necessary to cut down the time required for the removal of phishing sites by enabling a full- automatic notice-and-takedown system which can promptly bridge the CERTs between different countries to ensure immediate communication within the institutional network.

Some of the interviewees indicated that the ISPs of Taiwan hesitate to make an immediate Internet disconnection to the phishing sites in the absence of explicit legal authorisation, especially when the attack is not that evident or their customer is also a victim of phishing, for example, the operator of a compromised website. It is necessary to amend the Telecommunication Act to provide a legal basis to support the ISPs' termination or suspension measures; but in the meantime, the new law should include the requirement for the ISPs to enable their customers to be aware of the forbidden circumstances and the potential disadvantages for them to the largest extent.

8.5. Suggestions for future anti-phishing work in Taiwan

Although phishing arose as an issue in the 1990s, Taiwan's movement on anti-phishing work was very slow until 2010. The introduction of TAPWG and APNOW in 2010 was the first national response to phishing which declared an attempt to assemble the effort of the stakeholders across sectors in combating the growth of phishing attacks. However, having examined the legal regulation of phishing in Taiwan and also the countermeasures that have been undertaken in other dimensions on the basis of the existing literature and the insights provided by the interviews, this research found that there exist many problems in current Taiwan regulation of phishing that have significantly impeded the fulfillment of an effective multi-dimensional regulatory framework. I therefore propose the following suggestions for the future work.

8.5.1. Review of the laws

A review of the Criminal Code and the Personal Information Protection Act is necessary in order to ensure adequate criminalization of phishing and sufficient protection of information privacy. Both the elements of ‘obtainment’ and ‘damage’ laid down in Art. 359 of the Criminal Code should be capable of a broad interpretation and should not be subject to discrimination based on obtainment methods and monetary loss. To enable the PIP Act better to respond to the requirements raised from the regulation of phishing, it is necessary to re-define the term ‘personal information’ and reduce exceptions to unauthorised collection as well as the use of indeterminate legal concepts. It should not be an option but a sine qua non to have an independent privacy protection authority representing individual data subjects to compete against the power of both public and private data controllers.

The lawmakers should re-consider carefully the line between the protection of information privacy and the efficiency of personal information handling. The anxiety of the data controllers about the PIP Act mostly arises from their uncertainty about the extent to which they are allowed for data collection and the obligations they are required to fulfill to avoid being punished. This should be explicitly indicated in the Enforcement Rules of the PIP Act or the administrative guidance provided by the supervisory authorities for the related sectors rather than addressed by continuous compromise of the lawmakers to the interests of the data controllers.

8.5.2. Improvements in APNOW

The existing APNOW user interfaces demands some improvements especially in the language options to make it friendlier to international users. Given many phishing sites may be re-activated after the first attempt to remove them, it is necessary for APNOW to continue to monitor each site after it has been brought down to ensure that it is no longer live. It is also important to devote more resources to promotion of the visibility of APNOW to make sure it is well known, nationally and internationally, by the users and CERTs in both the public and private sectors. APNOW should be operated on an automated base to the largest extent in order to cut down the time required for the removal of phishing sites, in particular those hosted in other countries.

8.5.3. Reinforcement of the role of ISPs in the regulation of phishing

ISPs actually stand in a key strategic position in the regulation of phishing but their role needs to be reinforced by laws. ISPs should be explicitly authorized and required by laws to take necessary measures, such as disconnection or termination of the Internet services, when confronting incidents that have endangered information and telecommunications security. An ISP is not only the provider of connection or other services related to the infobahn, it should commit itself to ensure the security of the services provided for its users. It is necessary to strengthen ISPs' responsibility to prevent, manage, and report phishing attacks by requiring them to take appropriate measures; for example, strengthening detection and monitoring systems, providing assistance or pay services for their customers to deal with phishing, and coordinating the response to phishing incidents with other ISPs, to safeguard the security of their services.

8.5.4. Promotion of information security education and professional training

Taiwan is a highly computerized country, with high level of Internet usage and connectivity but a general lack of information security awareness and insufficient management of web server security. While there is a great number of Internet users in Taiwan, many care very little about the issue of information security or do not realize the importance of information security. Nor do they feel any responsibility to protect their computers as being netizens. This research suggests that the education of information security should be given as early as possible and rooted in school education in order to foster online secure behaviour and consciousness of the threat of various malicious attacks.

In addition, insufficient capacity of Taiwan's businesses, in particular small and medium-size businesses, for ensuring web security and respond to information security incidents has been a major weakness in the regulatory framework of phishing. This is largely because most IT personnel are not capable of information security tasks, which should be addressed by the government to organize or encourage systematic and solid training for the IT personnel to improve their ability to manage information security work and respond to information security incidents.

8.5.5. Enhancement of cooperation between stakeholders

This research suggests that the TAPWG introduced in 2010 should invite the participation of more stakeholders involved in the fight against phishing; for example law enforcement agencies, technology industries and potential victims and enhance cooperation and facilitate exchange of phishing data between stakeholders. To encourage the engagement of the industries, it is advisable to promote a more flexible cooperation model ensuring that each participant can benefit from this cooperation.

Besides cooperation between national stakeholders, it is necessary to promote international cooperation between non-governmental stakeholders. This is particularly important to Taiwan, as Taiwan suffers from political obstacles to intergovernmental cooperation. This research suggests that both ISPs and CERTs can play a very good role in bridging communication and coordinating anti-phishing policy between different countries.

While there is no silver bullet to cure phishing, the above suggestions may ameliorate many of the problems involved.

BIBLIOGRAPHY

Abawajy, Jemal and Kelarev, Andrei (2012), 'A multi-tier ensemble construction of classifiers for phishing email detection and filtering', in Xiang Yang, et al. (eds.), *Cyberspace Safety and Security, 4th International Symposium, CSS 2012,* (Melbourne, Australia: Springer), 48-56.

Abel, Wiebke and Schafer, Burkhard (2010), 'The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems–a case report on BVerfG, NJW', in V. Madhuri (ed.), *Hacking: A Legal Quandary* (Icfai University Press), 167-91.

Abu-Nimeh, Saeed, et al. (2007), 'A comparison of machine learning techniques for phishing detection', *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (Pittsburgh, PA, USA: ACM), 60-69.

Abu Rajab, Moheeb, et al. (2006), 'A multifaceted approach to understanding the botnet phenomenon', in Jussara Almeida, Virgilio Almeida, and Paul Barford (eds.), *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement* (Rio de Janeiro, Brazil: ACM), 41-52.

Aburrous, Maher, et al. (2010), 'Experimental case studies for investigating e-banking phishing techniques and attack strategies', *Cognitive Computation,* 2 (3), 242-53.

Acoca, B (2008), 'Scoping paper on online identity theft (Ministerial Background Report DSTI/CP (2007) 3/FINAL. Retrieved May 27, 2009'.

Acquisti, Alessandro and Gross, Ralph (2006), 'Imagined communities: Awareness, information sharing, and privacy on the Facebook', in George Danezis and Philippe Golle (eds.), *Privacy enhancing technologies* (Cambridge, UK,: Springer), 36-58.

Acquisti, Alessandro, Friedman, Allan, and Telang, Rahul (2006), 'Is there a cost to privacy breaches? An event study', *27the International Conference on Inofmration Systems (ICIS 2006)* (1; Milwaukee, Wisconsin, USA), 1563-80.

Adams, Anne and Sasse, Martina Angela (1999), 'Users are not the enemy', *Communications of the ACM,* 42 (12), 40-46.

Ademaj, Ilir and Schuck, Amie M. (2009), 'Internet security: Who is leaving the 'virtual door' open and why?', *First Monday,* 14 (1), 1-1.

Adida, Ben, Hohenberger, Susan, and Rivest, Ronald L (2005), 'Fighting phishing attacks: A lightweight trust architecture for detecting spoofed emails', in Drew Dean and Markus Jakobsson (eds.), *DIMACS Workshop on Theft in E-Commerce: Content, Identity, and Service* (University, Piscataway, NJ, USA).

Almerdas, Suhail (2014), 'The Criminalisation of Identity Theft under the Saudi Anti-Cybercrime Law 2007', *Journal of International Commercial Law and Technology,* 9 (2), 80-93.

Alsalman, Rami (2012), 'MALURLS: A Lightweight Malicious Website Classification Based on URL

Features', *Journal of Emerging Technologies in Web Intelligence,* 4 (2), 128-33.

Anandpara, Vivek, et al. (2007), 'Phishing IQ tests measure fear, not ability', in Sven Dietrich and Rachna Dhamija (eds.), *Financial Cryptography and Data Security* (Springer), 362-66.

Anderson, Keith B, Durbin, Erik, and Salinger, Michael A (2008), 'Identity theft', *The Journal of Economic Perspectives*, 171-92.

Anderson, Ross, et al. (2013), 'Measuring the Cost of Cybercrime', in Rainer Böhme (ed.), *The Economics of Information Security and Privacy*, 265-300.

Apple 'Safari: phishing website warning', <http://support.apple.com/kb/PH17210>, accessed August 15 2014.

APWG (2008a), 'Phishing Activity Trends: report for the month of January 2008'. <http://docs.apwg.org/reports/apwg_report_jan_2008.pdf>, accessed September 15 2014.

--- (2008b), 'Best Practices Recommendations for Registrars'. <http://docs.apwg.org/reports/APWG_RegistrarBestPractices.pdf>, accessed September 15 2014.

--- (2010a), 'Phishing Activity Trends Report: 4th Quarter 2009'. <http://docs.apwg.org/reports/apwg_report_Q4_2009.pdf>, accessed August 20 2014.

--- (2010b), 'Global Phishing Survey: Trends and Domain Name Use in 2H2009'. <http://apwg.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf>, accessed 9 September 2014.

--- (2012), 'Phishing Activity Trends Report - 1st Quarter (January -March) 2012'. <http://www.antiphishing.org/reports/apwg_trends_report_q1_2012.pdf>, accessed September 9 2014.

--- (2014), 'Global Phishing Survey: Trends and Domain Name Use in 2H2013'. <http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf>, accessed September 9 2014.

Arachchilage, Nalin Asanka Gamagedara and Love, Steve (2013), 'A game design framework for avoiding phishing attacks', *Computers in Human Behavior,* 29 (3), 706-14.

Archick, Kristin (2005), 'Cybercrime: The council of Europe convention', *Congressional Research Service Report (CRS Report for Congress)*. <http://mail.iwar.org.uk/news-archive/crs/10088.pdf>, accessed September 19 2014.

Armerding, Taylor (2012), 'The 15 worst data security breaches of the 21st Century', *CSO Security and Risk, February 2012*.

Arrington, Michael (2008), 'Phishing For Facebook', *TechCrunch*. <http://techcrunch.com/2008/01/02/phishing-for-facebook/>, accessed September 8 2014.

Bacher, Paul, et al. 'Know your enemy: Tracking botnets', <http://www.honeynet.org/papers/bots>, accessed 10 June 2014.

Bainbridge, David (2007), 'Criminal law tackles computer fraud and misuse', *Computer Law & Security Review,* 23 (3), 276-81.

Baker, Dennis J (2009), 'The moral limits of consent as a defense in the criminal law', *New Criminal*

Law Review, 12 (1), 93-121.

--- (2011), *The right not to be criminalized: demarcating criminal law's authority* (Ashgate Publishing, Ltd.).

Baker, Wade, et al. (2011), '2011 data breach investigations report', *Verizon RISK Team*, 1-72. <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf>, accessed August 30 2014.

Bakhshi, Taimur, Papadaki, Maria, and Furnell, Steven (2009), 'Social engineering: assessing vulnerabilities in practice', *Information management & computer security,* 17 (1), 53-63.

Baldwin, Robert, Cave, Martin, and Lodge, Martin (2010), 'Introduction: Regulation—the Field and the Developing Agenda', in Robert Baldwin, Martin Cave, and Martin Lodge (eds.), *The Oxford Handbook of Regulation* (Oxford: Oxford University Press), 3-13.

Banisar, David and Davies, Simon (1999), 'Privacy and human rights: an international survey of privacy laws and practice', *Global Internet Liberty Campaign*.

Barbaro, Michael, Zeller, Tom, and Hansell, Saul (2006), 'A face is exposed for AOL searcher no. 4417749', *New York Times*.

Baron, David P (1989), 'Design of regulatory mechanisms and institutions', in Richard Schmalensee and Robert Willig (eds.), *Handbook of industrial organization* (2), 1347-447.

Basnet, Ram, Mukkamala, Srinivas, and Sung, Andrew H (2008), 'Detection of phishing attacks: A machine learning approach', in Bhanu Prasad (ed.), *Soft Computing Applications in Industry* (Springer), 373-83.

Bayley, Robin and Bennett, Colin (2014), 'Canada's "anti-spam" law comes into force on 1 July this year', *Privacy Laws & Business International Newsletter,* 129, 19-20.

Bencsáth, Boldizsár and Vajda, István (2007), 'Efficient Directory Harvest Attacks and Countermeasures', *IJ Network Security,* 5 (3), 264-73.

Benson, Brett V and Niou, Emerson MS (2000), 'Comprehending strategic ambiguity: US policy toward Taiwan security', *Taiwan Security Research*.

Bergholz, André, et al. (2010), 'New filtering approaches for phishing email', *Journal of computer security,* 18 (1), 7-35.

Bin, Sun, Qiaoyan, Wen, and Xiaoying, Liang (2010), 'A DNS based anti-phishing approach', *2010 Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC)* (2; Wuhan, Hubei, China: IEEE), 262-65.

Birk, Dominik, et al. (2007), 'A forensic framework for tracing phishers', *IFIP Summer School on The Future of Identity in the Information Society, Karlstad, Sweden*.

Blanco, Carlos L. (2011), 'The eG8 Summit in Paris – a step forward for global Internet and broadband policy', *Telefonica*. <http://www.publicpolicy.telefonica.com/blogs/blog/2011/06/07/the-eg8-summit-in-paris-%E2%80%93-a-step-forward-for-global-internet-and-broadband-policy/>, accessed September 8 2014.

Bonneau, Joseph and Preibusch, Sören (2010), 'The privacy jungle: On the market for data protection in social networks', in Tyler Moore, David Pym, and Christos Ioannidis (eds.), *Economics of information security and privacy* (Springer), 121-67.

Bose, Indranil and Leung, Alvin Chung Man (2007), 'Unveiling the mask of phishing: threats, preventive measures, and responsibilities', *Communications of the Association for Information Systems,* 19.

Brenner, Susan W (2004), 'Toward a criminal law for cyberspace: A new model of law enforcement', *Rutgers Computer & Tech. LJ,* 30, 1.

Brenner, Susan W and Schwerha IV, Joseph J (2001), 'Transnational evidence gathering and local prosecution of international cybercrime', *J. Marshall J. Computer & Info. L.,* 20, 347.

Broadhurst, Roderic (2006), 'Developments in the global law enforcement of cyber-crime', *Policing: An International Journal of Police Strategies & Management,* 29 (3), 408-33.

Brody, Richard G, Mulig, Elizabeth, and Kimball, Valerie (2007), 'Phishing, pharming and identity theft', *Academy of Accounting & Financial Studies Journal,* 11 (3).

Broersma, Matthew 'Trojan Targets Microsoft's AntiSpyware Beta', <http://www.eweek.com/c/a/Security/Trojan-Targets-Microsofts-AntiSpyware-Beta/>, accessed 15 June 2014.

Butler, Rika (2007), 'A framework of anti-phishing measures aimed at protecting the online consumer's identity', *Electronic Library, The,* 25 (5), 517-33.

Bygrave, Lee A (1998), 'Data protection pursuant to the right to privacy in human rights treaties', *International Journal of Law and Information Technology,* 6 (3), 247-84.

Cannataci, Joseph A. (2008), 'Lex Personalitatis & Technology-driven Law', *SCRPIT-ed,* 5 (1).

Cao, Ye, Han, Weili, and Le, Yueran (2008), 'Anti-phishing based on automated individual white-list', in Elisa Bertino and Kenji Takahashi (eds.), *Proceedings of the 4th ACM workshop on Digital identity management* (Alexandria, VA, USA: ACM), 51-60.

Casey, Eoghan (2011), *Digital evidence and computer crime: forensic science, computers and the internet* (3 edn.: Academic press).

Castells, Manuel (2011), 'Network Theory| A Network Theory of Power', *International Journal of Communication,* 5, 15.

Ceesay, Ebrima N (2008), 'Mitigating phishing attacks: a detection, response and evaluation framework', (University of California at Davis).

Central Intelligence Agency (2012), 'The World Factbook'. <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2184rank.html>, accessed September 1 2014.

Chandrasekaran, Madhusudhanan, Narayanan, Krishnan, and Upadhyaya, Shambhu (2006), 'Phishing email detection based on structural properties', *NYS Cyber Security Conference*, 1-7.

Chang, Kai-Jie and Chang, Chin-Chen (2007), 'An e-mail signature protocol for anti-spam work-in-progress', in Li Jianzhong, Lee Wang-Chien, and Fabrizio Silvestri (eds.), *Proceedings of the 2nd international conference on Scalable information systems* (Suzhou, China: ICST

(Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering)), 1-2.

Chang, Yao-Chung (2012), *Cybercrime in the Greater China region: regulatory responses and crime prevention across the Taiwan Strait* (Edward Elgar Publishing).

Chao, Y (2010), 'Google attacks used addresses based in Taiwan', *Taipei Times,* 16 January 2010.

Chen, Chia-Mei, Guan, DJ, and Su, Qun-Kai (2014), 'Feature set identification for detecting suspicious urls using bayesian classification in social networks', *Information Sciences*.

Chen, H. L. (2013), 'Taiwan's PIPA into force, with controversial sections removed', *Privacy Laws & Business International Report*.

Chen, Kuan-Ta, et al. (2009), 'Fighting phishing with discriminative keypoint features', *Internet Computing, IEEE,* 13 (3), 56-63.

Chen, Teh-Chung, Dick, Scott, and Miller, James (2010), 'Detecting visually similar Web pages: Application to phishing detection', *ACM Transactions on Internet Technology (TOIT),* 10 (2), 5.

Cheng, C. I. (2009), 'The Extension and Tension of Internet Jurisdiction', *Socioeconomic Law and Institution Review,* 43, 127-60.

Cheng, C. W. (2001), 'Analysis of Electromagnetic Records Larceny', *Criminal Law Magazine*, 45 (6), 112-38.

Cheng, Fa-Chang (2011), 'The Law Enforcement in Cyberspace Criminal: Focusing on the Experience between Taiwan and the United States', *2011 Third International Conference on Multimedia Information Networking and Security (MINES)* (Shanghai, China: IEEE), 577-80.

Chien, Eric and O'Gorman, Gavin (2011), 'The Nitro Attacks, Stealing Secrets from the Chemical Industry', *Symantec Security Response*.

Chiou, W. T. (2009), 'Comments on the Constructional Problems of the Amendment Bill of the Computer-Processed Personal Data Protection Law – Based on the Ideologies of Information Autonomy and Information Privacy', *Yue-Dan Jurisprudence Magazine*, 168, 172-89.

Chou, Neil, et al. (2004), 'Client-Side Defense Against Web-Based Identity Theft', in Clifford Neuman, Michael Reiter, and Dan Boneh (eds.), *The 11th Annual Network and Distributed System Security Symposium (NDSS Symposium 2004)* (San Diego, California, USA).

Ciocchetti, Corey (2007), 'The Privacy Matrix', *Journal of Technology Law & Policy,* 12, 245.

Cisco (2011), 'Email attacks: this time it's personal', *Cisco Security White Paper*. <http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/targeted_attacks.pdf>, accessed September 8 2014.

Claburn, Thomas (2010), ''Tabnapping' attack simplifies phishing ', *InformationWeek,* 25 May 2010.

Clarke, Roger (2000), 'Beyond the OECD guidelines: privacy protection for the 21st century', *Canberra, Australia: Xamax Consultancy Pty Ltd. Retrieved August,* 5, 2009.

Comesongsri, Veti (2010), 'Motivation for the avoidance of phishing threat', (The University of Memphis).

Commission on Crime Prevention and Criminal Justice (2011), 'Requesting mutual legal assistance in criminal matters from G8 countries: A step-by-step guide, E/CN.15/2011/CPR.6', 20. <http://www.coe.int/t/DGHL/STANDARDSETTING/PC-OC/PCOC_documents/8_MLA%20step-by-step_CN152011_CRP.6_eV1182196.pdf>, accessed September 15 2014.

Creswell, John W (2013), *Research design: Qualitative, quantitative, and mixed methods approaches* (2 edn.: Sage).

Davinson, Nicola and Sillence, Elizabeth (2010), 'It won't happen to me: Promoting secure behaviour among internet users', *Computers in Human Behavior,* 26 (6), 1739-47.

Denscombe, Martyn (2010), *The Good Research Guide: For Small-Scale Social Research Projects: For small-scale social research projects* (4 edn.: McGraw-Hill International).

Dhamija, Rachna and Perrig, Adrian (2000), 'Deja vu: A user study using images for authentication', *Proceedings of the 9th conference on USENIX Security Symposium* (9: USENIX Association Berkeley), 45-58.

Dhamija, Rachna and Tygar, J Doug (2005), 'The battle against phishing: Dynamic security skins', *Proceedings of the 2005 symposium on Usable privacy and security (SOUPS)* (Pittsburgh, PA, USA: ACM), 77-88.

Dhamija, Rachna, Tygar, J Doug, and Hearst, Marti (2006), 'Why phishing works', in Rebecca Grinter, et al. (eds.), *Proceedings of the SIGCHI conference on Human Factors in computing systems* (Montreal, Canada: ACM), 581-90.

Dinna, NMN, et al. (2007), 'Managing legal, consumers and commerce risks in phishing', *Proceedings of World Academy of Science Engineering and Technology* (26: ACM Press), 562-7.

Dong, Xun, Clark, John A, and Jacob, Jeremy L (2010), 'Defending the weakest link: phishing websites detection by analysing user behaviours', *Telecommunication Systems,* 45 (2-3), 215-26.

Downs, Julie S, Holbrook, Mandy B, and Cranor, Lorrie Faith (2006), 'Decision strategies and susceptibility to phishing', *Proceedings of the second symposium on Usable privacy and security* (ACM), 79-90.

Dunn, John E. (2007), 'Do-it-Yorself Phishing Kit Found Online', *PCWorld*. <http://www.pcworld.com/article/128524/article.html>, accessed September 8 2014.

eBay 'Recognizing spoof (fake) eBay websites'. <http://pages.ebay.com/help/account/recognizing-spoof.html>, accessed September 8 2014.

Egelman, Serge, Cranor, Lorrie Faith, and Hong, Jason (2008), 'You've been warned: an empirical study of the effectiveness of web browser phishing warnings', in Mary Czerwinski, Arnie Lund, and Desney Tan (eds.), *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy: ACM), 1065-74.

Eisenstein, Eric M (2008), 'Identity theft: an exploratory study with implications for marketers', *Journal of Business Research,* 61 (11), 1160-72.

Ellison, Nicole B (2007), 'Social network sites: Definition, history, and scholarship', *Journal of Computer-Mediated Communication,* 13 (1), 210-30.

Emigh, Aaron (2005), 'Online identity theft: phishing technology, chokepoints and countermeasures', *ITTC Report on Online Identity Theft Technology and Countermeasures*.

--- (2007), 'Phishing attacks: Information flow and chokepoints', in Markus Jakobsson and Steven Myers (eds.), *Phishing and countermeasures: understanding the increasing problem of electronic identity theft* (John Wiley & Sons), 31-64.

Fang, Wen-Pinn (2007), 'Visual Cryptography in reversible style', *The Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2007)* (1: IEEE), 519-24.

FBI (2009), 'Operation Phish Phry - Major Cyber Fraud Takedown', *FBI*. <http://www.fbi.gov/news/stories/2009/october/phishphry_100709>, accessed September 10 2014.

Featherman, Mauricio S, Miyazaki, Anthony D, and Sprott, David E (2010), 'Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility', *Journal of Services Marketing,* 24 (3), 219-29.

Feily, Maryam, Shahrestani, Alireza, and Ramadass, Sureswaran (2009), 'A survey of botnet and botnet detection', in Rainer Falk, et al. (eds.), *The Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'09)* (Athens/Glyfada, Greece: IEEE), 268-73.

Felegyhazi, Mark, Kreibich, Christian, and Paxson, Vern (2010), 'On the potential of proactive domain blacklisting', *Proceedings of the Third USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET '10)* (San Jose, CA, USA).

Feng, Qingxiang, et al. (2011), 'New Anti-phishing Method with Two Types of Passwords in OpenID System', in Junzo Watada, et al. (eds.), *2011 Fifth International Conference on Genetic and Evolutionary Computing (ICGEC 2011)* (Kinmen, Taiwan; Xiamen, China: IEEE), 69-72.

Fette, Ian, Sadeh, Norman, and Tomasic, Anthony (2007), 'Learning to detect phishing emails', *Proceedings of the 16th international conference on World Wide Web* (Banff, Alberta, Canada: ACM), 649-56.

Finklea, Kristin M (2014), 'Identity theft: Trends and issues', *CRS report*. <http://fas.org/sgp/crs/misc/R40599.pdf>, accessed September 10 2014.

Fischer-Hübner, Simone (1998), 'Privacy and security at risk in the global information society', *Information Communication & Society,* 1 (4), 420-41.

Flaherty, David H (1992), *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States* (UNC Press Books).

Fogel, Joshua and Nehmad, Elham (2009), 'Internet social network communities: Risk taking, trust, and privacy concerns', *Computers in Human Behavior,* 25 (1), 153-60.

FormosaFoundation 'Taiwan's participation in international organizations', [Ambassador Program Issues 2013],

<http://www.formosafoundation.org/ambassador-program/documents/issues/TW-International-Participation.pdf>, accessed 15 July 2014.

Fox, Mark A. (2006), 'Phishing, pharming and identity theft in the banking industry', *Journal of International Banking Law and Regulation,* 21 (9), 548-52.

Frommer, Dan (2009), 'What a nigerian facebook scam looks like', *The Business Insider*. <http://www.businessinsider.com/2009/1/nigerian-scammers-still-roosting-on-facebook>, accessed September 11 2014.

Furnell, Steven (2007), 'Phishing: can we spot the signs?', *Computer Fraud & Security,* 2007 (3), 10-15.

Furnell, Steven M (2004), 'Getting caught in the phishing net', *Network Security,* 2004 (5), 14-18.

--- (2009), 'The irreversible march of technology', *Information Security Technical Report,* 14 (4), 176-80.

Görling, Stefan (2006), 'The myth of user education', *Virus Bulletin Conference* (11; Montreal, Canada), 13.

--- (2007), 'An overview of the Sender Policy Framework (SPF) as an anti-phishing mechanism', *Internet Research,* 17 (2), 169-79.

Gajek, Sebastian and Sadeghi, Ahmad-Reza (2008), 'A forensic framework for tracing phishers', in Simone Fischer-Hübner, et al. (eds.), *The Future of Identity in the Information Society* (Springer), 23-35.

Gan, Tian-Guei (2011), *The Specific Provisions of the Criminal Code -Part I* (2 edn.; Taipei: San Min Ltd).

Gannon, James, Morgan, Charles S., and Salzman, Lorne P. (2010), 'Canadian Government's proposed anti-spam and anti-spyware legislation', *World Data Protection Report,* 10 (9), 9-11.

Gao, W and Kim, J (2007), 'Robbing the cradle is like taking candy from a baby', *Proceedings of the Annual Conference of the Security Policy Institute (GCSPI)* (4; Amsterdam, The Netherlands), 23-37.

Garera, Sujata, et al. (2007), 'A framework for detection and measurement of phishing attacks', in Christopher Kruegel (ed.), *Proceedings of the 2007 ACM workshop on Recurring malcode* (Alexandria, VA, USA: ACM), 1-8.

Garfinkel, Simson L, et al. (2005), 'How to make secure email easier to use', in Wendy Kellogg, et al. (eds.), *Proceedings of the SIGCHI conference on Human factors in computing systems* (Portland, OR, USA: ACM), 701-10.

Gavison, Ruth (1980), 'Privacy and the Limits of Law', *Yale law journal*, 421-71.

George, Alison (2006), 'Living online: The end of privacy', *New Scientist,* 2569, 1-50.

Gercke, Marco (2007), 'Internet-Related Identity Theft', *Economic Crime Division, Directorate General of Human Rights and Legal Affairs, Strasbourg, France*.

Germain, Jack M. (2004), 'Will Antiphishing Legislation Be Effective?', *E-Commerce Times*. <http://www.ecommercetimes.com/story/38006.html>, accessed September 11 2014.

Google 'Google safe browsing for firefox', <http://www.google.com/tools/firefox/safebrowsing/>, accessed August 15 2014.

Gouda, Mohamed G, et al. (2007), 'SPP: An anti-phishing single password protocol', *Computer Networks,* 51 (13), 3715-26.

Granova, Anna and Eloff, JHP (2005), 'A legal overview of phishing', *Computer Fraud & Security,* 2005 (7), 6-11.

Grebb, Michael (2005), 'Crime: Crooks Get Behind Plow: 'Pharming' harvests a new crop of thieves', *Bank Technology News,* 1 March 2005.

Greenleaf, Graham (2005), 'APEC's privacy framework sets a new low standard for the Asia–Pacific', in Andrew T. Kenyon and Megan Richardson (eds.), *New dimensions in privacy law: international and comparative perspectives* (Cambridge: Cambridge University Press).

Gross, Grant (2005), 'Proposed Law Aims to Fight Phishing', *PCWorld*. <http://www.pcworld.com/article/119912/article.html>, accessed September 11 2014.

Gross, Ralph and Acquisti, Alessandro (2005), 'Information revelation and privacy in online social networks', *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (ACM), 71-80.

Gstöhl, Sieglinde (2007), 'Governance through government networks: The G8 and international organizations', *The Review of International Organizations,* 2 (1), 1-37.

Halderman, J Alex, Waters, Brent, and Felten, Edward W (2005), 'A convenient method for securely managing passwords', *Proceedings of the 14th international conference on World Wide Web* (ACM), 471-79.

Han, J. M. and Wu, J. F. (2000), *The Specific Provisions of the Criminal Code* (1 edn.).

He, Jianming, Chu, Wesley W, and Liu, Zhenyu Victor (2006), 'Inferring privacy information from social networks', in Sharad Mehrotra, et al. (eds.), *Intelligence and Security Informatics* (Springer), 154-65.

Herley, Cormac and Florencio, Dinei (2009), 'A profitless endeavor: phishing as tragedy of the commons', *Proceedings of the 2008 workshop on New security paradigms* (ACM), 59-70.

Herzberg, Amir (2009a), 'Why Johnny can't surf (safely)? Attacks and defenses for web users', *Computers & Security,* 28 (1), 63-71.

--- (2009b), 'DNS-based email sender authentication mechanisms: A critical review', *Computers & security,* 28 (8), 731-42.

Hidalgo, Amado (2007), 'A Monster Trojan', *Symantec Blog*. <http://www.symantec.com/connect/blogs/monster-trojan>, accessed August 17 2014.

Hipolito, Joahnna Marie 'Anatomy of a Data Breach', (updated November 15 2011) <http://about-threats.trendmicro.com/RelatedThreats.aspx?language=tw&name=Anatomy+of+a+Data+Breach>, accessed August 15 2014.

Holz, Thorsten, et al. (2008), 'Measuring and Detecting Fast-Flux Service Networks', *NDSS*.

Hong, Jason (2012), 'The state of phishing attacks', *Communications of the ACM,* 55 (1), 74-81.

Hornung, Gerrit and Schnabel, Christoph (2009), 'Data protection in Germany I: The population census decision and the right to informational self-determination', *Computer Law & Security Review,* 25 (1), 84-88.

Hsu, Cheng-Hsin, Wang, Polo, and Pu, Samuel (2011), 'Identify fixed-path phishing attack by STC', in Vidyasagar Potdar (ed.), *Proceedings of the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference* (Perth, Australia: ACM), 172-75.

Hsueh, Chih-Jen (2013), 'Criminal Penalties for Phishing', *Soochow Law Review,* 24 (3), 149-85.

Hsueh, Yi-Jing (2007), 'Averagely ten times hacker attackers daily', *Business Next*, 72.

Huang, Chang-Ren (2009), *The General Provisions of the Criminal Code* (2 edn.; Taipei: New Sharing Publishing Ltd).

Huang, Chun-Ying, et al. (2010), 'Mitigate web phishing using site signatures', *TENCON 2010-2010 IEEE Region 10 Conference* (Fukuoka, Japan: IEEE), 803-08.

Huang, Huajun, Tan, Junshan, and Liu, Lingxi (2009), 'Countermeasure techniques for deceptive phishing attack', *International Conference on New Trends in Information and Service Science (NISS'09)* (Beijing, China: IEEE), 636-41.

Huang, R. J. (2000), *The Limit of Penalty* (Yuan Jhao Publisher).

Huang, Yan-Fen (2012), 'The proposed suspension of the controversial provisions of the PIP Act', *iThome*. <http://www.ithome.com.tw/node/72444>, accessed September 7 2014.

Ianelli, Nicholas and Hackworth, Aaron (2005), 'Botnets as a vehicle for online crime', *CERT Coordination Center,* 1, 28.

ICANN, Security and Stability Advisory Committee (SSAC) (2008), 'SAC 028: SSAC Advisory on Registrar Impersonation Phishing Attacks '. <https://www.icann.org/en/system/files/files/sac-028-en.pdf>, accessed September 15 2014.

--- (2009), 'SAC 038: Registrar Abuse Point of Contact'. <https://www.icann.org/en/system/files/files/sac-038-en.pdf>, accessed September 15 2014.

Irani, Danesh, et al. (2008), 'Evolutionary study of phishing', *eCrime Researchers Summit, 2008* (IEEE), 1-10.

Irani, Danesh, et al. (2011), 'Reverse social engineering attacks in online social networks', in Thorsten Holz and Herbert Bos (eds.), *Detection of intrusions and malware, and vulnerability assessment* (6739: Springer), 55-74.

Islam, Rafiqul and Abawajy, Jemal (2013), 'A multi-tier phishing detection and filtering approach', *Journal of Network and Computer Applications,* 36 (1), 324-35.

ITU (2009), 'Understanding Cybercrime: A Guide for Developing Countries', *International Telecommunication Union Cybercrime Legislation Resources*. <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>, accessed September 7 2014.

Jagatic, Tom N, et al. (2007), 'Social phishing', *Communications of the ACM,* 50 (10), 94-100.

Jakobsson, Markus and Myers, Steven (2007), *Phishing and countermeasures: understanding the* *increasing problem of electronic identity theft* (John Wiley & Sons).

James, Divya and Philip, Mintu (2012), 'A Novel Anti phishing framework based on visual cryptography', *2012 International Conference on Power, Signals, Controls and Computation (EPSCICON)* (Thrissur, Kerala, India: IEEE), 1-5.

Jen, Wen-Yuan, Chang, Wei-ping, and Chou, Shih-chieh (2006), 'Cybercrime in Taiwan–an analysis of suspect records', in Hsinchun Chen, et al. (eds.), *Intelligence and Security Informatics* (Springer), 38-48.

Jeng, Y. J. (2003), 'Boost courage by whistling – comments on the augmentation of the Chapter 36 of the Criminal Code', *Ywe-Dan Jurisprudence*, 201, 104-15.

Jerram, Cate, et al. (2012), 'Why do some people manage phishing e-mails better than others?', *Information Management & Computer Security,* 20 (1), 18-28.

Johnson, Nathaniel A., Jakobsson, Markus, and Menczer, Filippo (2007), 'Social Phishing', *Communications of the ACM,* 50 (10), 94-100.

Juels, Ari, Stamm, Sid, and Jakobsson, Markus (2007), 'Combating click fraud via premium clicks', *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium* (Boston, MA. USA: USENIX Association), 1-10.

Kan, Michael (2011), 'Taiwan political party accuses China of hacking', *PCWorld*. <http://www.pcworld.com/article/237591/taiwan_political_party_accusses_china_of_hacking.html>, accessed September 7 2014.

Kang, JungMin and Lee, DoHoon (2007), 'Advanced white list approach for preventing access to phishing sites', in Yun Ji Na, et al. (eds.), *The 2007 International Conference on Convergence Information Technology (ICCIT 2007)* (Gyeongju, Korea: IEEE), 491-96.

Karlof, Chris, et al. (2007), 'Dynamic pharming attacks and locked same-origin policies for web browsers', *Proceedings of the 14th ACM conference on Computer and communications security* (Alexandria, VA, USA: ACM), 58-71.

Katyal, Neal Kumar (2001), 'Criminal law in cyberspace', *University of Pennsylvania Law Review*, 1003-114.

Ke, Y. C. (2003), 'The comments on the legislation relating computer (Internet) crimes of the Criminal Code', *Ywe-Dan Jurisprudence Classroom*, 11, 117-29.

Kennedy, Gabriela and Doyle, Sarah (2007), 'A snapshot of legal developments and industry issues relevant to information technology, media and telecommunications in key jurisdictions across the Asia Pacific–Co-ordinated by Lovells and contributed to by other leading law firms in the region', *Computer Law & Security Review,* 23 (2), 148-55.

Kirda, Engin and Kruegel, Christopher (2005), 'Protecting users against phishing attacks with antiphish', *29th Annual International Computer Software and Applications Conference (COMPSAC)* (1; Hong Kong, China: IEEE), 517-24.

--- (2006), 'Protecting users against phishing attacks', *The Computer Journal,* 49 (5), 554-61.

Klein, Amit (2010), 'The Golden Hour of Phishing Attacks', *Trusteer* <http://www.trusteer.com/blog/golden-hour-phishing-attacks>, accessed September 10

2014.

Konings, Marika (2009), 'Final report of the GNSO Fast Flux Hosting Working Group'. <http://gnso.icann.org/files/gnso/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf>, accessed September 20 2014.

Koops, Bert-Jaap and Leenes, Ronald (2006), 'Identity theft, identity fraud and/or identity-related crime', *Datenschutz und Datensicherheit-DuD,* 30 (9), 553-56.

Koops, Egbert Jakob and Brenner, Susan W (2006), 'Cybercrime jurisdiction - an introducation', in Egbert Jakob Koops and Susan W Brenner (eds.), *Cybercrime and Jurisdiction; A Global Survey* (Hague: T.M.C. Asser Press), 3-4.

Kornblum, Janet and Marklein, Mary Beth (2006), 'What you say online could haunt you', *USA Today*. <http://usatoday30.usatoday.com/tech/news/internetprivacy/2006-03-08-facebook-myspace_x.htm?csp=N007>, accessed September 7 2014.

Krebs, Brian (2004), 'Companies Forced to Fight Phishing', *The Washington Post*. <http://www.washingtonpost.com/wp-dyn/articles/A61916-2004Nov19.html>, accessed September 15 2014.

Kshetri, Nir (2010), 'The Economics of Click Fraud', *IEEE Security & Privacy,* 8 (3), 45-53.

Kueter, Jeff (2009), 'The missile defense mission', *Journal of International Security Affairs,* 16, 33-40.

Kumaraguru, Ponnurangam (2009), *Phishguru: a system for educating users about semantic attacks* (ProQuest).

Kumaraguru, Ponnurangam, et al. (2008), 'Lessons from a real world evaluation of anti-phishing training', *eCrime Researchers Summit, 2008* (IEEE), 1-12.

--- (2010), 'Teaching Johnny not to fall for phish', *ACM Transactions on Internet Technology (TOIT),* 10 (2), 7.

Kumaraguru, Ponnurangam, et al. (2009), 'School of phish: a real-world evaluation of anti-phishing training', *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS)* (Google in Mountain View, CA, USA: ACM), 3.

Lam, Tony (2005), 'An Overview of the Principles Established by the APEC Privacy Framework', *APEC Technical Assistance Seminar: Domestic Implementation*. <https://www.pcpd.org.hk/english/files/infocentre/1tonylam1_ppt.pdf>, accessed September 27 2014.

Larkin, Erik (2010), 'Browser Fingerprints: A Big Privacy Threat', *PCWorld*. <http://www.pcworld.com/article/192648/browser_fingerprints_a_big_privacy_threat.html>, accessed September 16 2014.

Layton, Robert and Watters, Paul (2009), 'Determining provenance in phishing websites using automated conceptual analysis', *eCrime Researchers Summit, 2009* (IEEE), 1-7.

Lee, Che-Fu (1997), 'China's Perception of the Taiwan Issue', *New Eng. L. Rev.,* 32, 695.

Lee, Lung-Hao, et al. (2013), 'User-Centric Phishing Threat Detection', *In Poster Session of the 34th*

IEEE Symposium on Security and Privacy (San Francisco, California, USA).

Lee, Lung-Hao, et al. (2014), 'Users' behavioral prediction for phishing detection', in Chin-Wan Chung, et al. (eds.), *Proceedings of the companion publication of the 23rd international conference on World wide web companion* (Seoul, Korea: International World Wide Web Conferences Steering Committee), 337-38.

Lee, Lung-Hao, et al. (2012), 'Context-aware web security threat prevention', in Ting Yu, George Danezis, and Virgil Gligor (eds.), *Proceedings of the 2012 ACM conference on Computer and communications security* (Raleigh, North Carolina, USA: ACM), 992-94.

Lee, Wei-Bin, et al. (2011), 'An Anti-phishing User Authentication Scheme without Using a Sensitive Key Table', in Xiamu Niu, et al. (eds.), *2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)* (Dalian, China: IEEE), 141-44.

Legon, Jeordan (2004), 'Phishing'scams reel in your identity', *CNN*. <http://edition.cnn.com/2003/TECH/internet/07/21/phishing.scam/>, accessed September 16 2014.

Lessig, L (2006), *Code: version 2.0* (2 edn.: New York: Basic Books).

Levi, Michael and Burrows, John (2008), 'Measuring the Impact of Fraud in the UK A Conceptual and Empirical Journey', *British Journal of Criminology,* 48 (3), 293-318.

Li, Linfeng and Helenius, Marko (2007), 'Usability evaluation of anti-phishing toolbars', *Journal in Computer Virology,* 3 (2), 163-84.

Li, Mao-San (1998), *Authority, Subject, and Criminal Laws* (Taipei: Han-Lu Publisher).

--- (2001), 'The virtual image and actual features of computer crimes in Taiwan', *Collection of Papers on Criminal Policies and Research of Crimes* (4: Ministry of Justice), 1-16.

Li, Xingan (2007), 'International actions against cybercrime: Networking legal systems in the networked crime scene', *Webology,* 4 (3), 1-45.

Liang, H. C. (1994), *Research of Living Examples of the Criminal Code* (Taipei: Wu-Nan Book Co. Ltd.).

Liang, Huigang and Xue, Yajiong (2010), 'Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective', *Journal of the Association for Information Systems,* 11 (7).

Liao, Y. L. and Li, S. C. (2003), *Computer Crime –Theory and Practice* (Taipei: Wu-Nan Book Co. Ltd).

Liao, Y. L. and Jin, M. C. (2006), 'A comparatively study of two reenactment of Penal Code on computer crime', *Journal of Information, Technology and Society,* 2006 (2), 56-76.

Liao, You-lu and Tsai, Cynthia (2006), 'Analysis of computer crime characteristics in Taiwan', in Hsinchun Chen, et al. (eds.), *Intelligence and Security Informatics* (Springer), 49-57.

Lillibridge, Mark D, et al. (2001), 'Method for selectively restricting access to computer systems', (Google Patents).

Lin, Chia-Chen and Chiang, Po-Hsuan (2009), 'A Novel Mutual Authentication Based on Data Embedding Technique', in Jeng-Shyang Pan, Yen-Wei Chen, and Lahmi C. Jain (eds.), *Fifth*

International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'09) (Kyoto, Japan: IEEE), 274-77.

Lin, Chun-Li and Cheng, Ming-Her (2008), 'The one-time Password Authentication Protocol of against Phishing Attack', *2008 Management and Application of Information Communication Technologies Conference* (Kaohsiung, Taiwan: Shu Te Univeristy), 216-25.

Lin, Dung-Mau (2012), *The overview of the Criminal Code* (7 edn.; Taipei: Yi-Pin Publisher).

Lin, Guan-Hong (2006a), 'A research on the Chapter 'Offences against Computer Use' of the Criminal Code ', *Criminal Law Magazine*, 50: 6, 82-118.

Lin, Min-Sheng, et al. (2013), 'Malicious URL filtering—A big data application', in Xiaohua Hu, et al. (eds.), *2013 IEEE International Conference on Big Data* (Santa Clara, CA, USA: IEEE), 589-96.

Lin, Shun-Jie (2011a), 'The Introduction of the Taiwan Anti-Phishing Reporting Mechanism and Platform', *TWCERT/CC Newsletter,* 6.

Lin, Sian-Tian (2006b), *The Specific Provisions of the Criminal Code* (5 edn., 1; Taipei: Angel Publisher).

Lin, Yi-Long (2010), 'The Relay Position of the TWNIC to Enable the TWCERT/CC to Transform and Restart', *TWCERT/CC Newsletter,* 1.

Lin, Yu-Shiung (2011b), *New General Provisions of the Criminal Code* (3 edn.).

Lindamood, Jack, et al. (2009), 'Inferring private information using social network data', *Proceedings of the 18th international conference on World wide web* (Madrid, Spain: ACM), 1145-46.

Lininger, Rachael and Vines, Russell Dean (2005), *Phishing: cutting the identity theft line* (John Wiley & Sons).

Liou, Guang-San (1999), *The Theory of Computer Crimes* (Beijing: The Publisher of the People’s University of China) 4.

Liou, J. Y. (2010), 'Unsatisfying Progress of Legislation: Initial Comments on the Personal Information Protection Act.', *Yue-Dan Jurisprudence Magazine*, 183, 147-64.

Lipson, Howard F (2002), 'Tracking and tracing cyber-attacks: Technical challenges and global policy issues', (DTIC Document).

Litan, Avivah (2005), 'Increased phishing and online attacks cause dip in consumer confidence', *Gartner Study (June 2005)*.

Liu, Jin-Han (2010), 'The Activation of the Taiwan Information Security Strategic Alliance', *TWCERT/CC Newsletter - Special Periodical for the Taiwan Information Security Strategic Alliance*. <http://www.myhome.net.tw/cert01/cont04.htm>, accessed September 16 2014.

Liu, Wenyin, et al. (2006), 'An antiphishing strategy based on visual similarity assessment', *Internet Computing, IEEE,* 10 (2), 58-65.

Lloyd, Ian J (2000), *Legal aspects of the information society* (Butterworths).

Longstaff, Thomas A, et al. (1997), 'Security of the Internet', *The Froehlich/Kent Encyclopedia of Telecommunications,* 15, 231-55.

Lovet, Guillaume (2009), 'Fighting Cybercrime: Technical, juridical and ethical challenges', *Virus*

Bulletin Conference (Geneva, Switzerland), 63-76.

Lu, Chi-Chao, et al. (2006), 'Cybercrime & cybercriminals: An overview of the Taiwan experience', *Journal of Computers,* 1 (6), 11-18.

Ludl, Christian, et al. (2007), 'On the effectiveness of techniques to detect phishing sites', in Bernhard M. Hämmerli and Robin Sommer (eds.), *Detection of Intrusions and Malware, and Vulnerability Assessment* (4579: Springer), 20-39.

Lynch, Jennifer (2005), 'Identity theft in cyberspace: crime control methods and their effectiveness in combating phishing attacks', *Berkeley Tech. LJ,* 20, 259.

Ma, Justin, et al. (2009), 'Beyond blacklists: learning to detect malicious web sites from suspicious URLs', *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining* (Paris, France: ACM), 1245-54.

MacEwan, Neil (2013), 'A Tricky Situation: Deception in Cyberspace', *The Journal of Criminal Law,* 77 (5), 417-32.

Marsoof, Althaf (2011), 'Online social networking and the right to privacy: The conflicting rights of privacy and expression', *International Journal of Law and Information Technology*, eaq018.

Martin, Tim (2009), 'Phishing for answers: Factors influencing a participant's ability to categorize email', *Comput. Changing World, Portland, OR*.

Mazanec, Brian M (2009), 'The art of (cyber) war', *Journal of International Security Affairs,* 16, 81-90.

McAfee 'McAfee SiteAdvisor', <http://www.siteadvisor.com/howitworks/index.html>, accessed August 16 2014.

McConnel (2000), 'Cybercrime…and punishment? Archaic Laws Threaten Global Information'. <http://www.witsa.org/papers/McConnell-cybercrime.pdf>, accessed September 21 2014.

McGowan, Laura (2006), 'Criminal Law Legislation Update', *J. Crim. L.,* 71, 184.

McGrath, D Kevin and Gupta, Minaxi (2008), 'Behind Phishing: An Examination of Phisher Modi Operandi', *LEET,* 8, 4.

McGrath, D Kevin, Kalafut, Andrew, and Gupta, Minaxi (2009), 'Phishing infrastructure fluxes all the way', *IEEE Security & Privacy,* 7 (5), 0021-28.

McMillan, Robert (2006), 'Who or what is 'Rock Phish' and why should you care?', *PCWorld*. <http://www.pcworld.com/article/128175/article.html>, accessed September 16 2014.

McNealy, Jasmine E (2008), 'Angling for phishers: legislative responses to deceptive e-mail', *Comm. L. & Pol'y,* 13 (2), 275-300.

McRae, Craig M and Vaughn, Rayford B (2007), 'Phighting the phisher: Using web bugs and honeytokens to investigate the source of phishing attacks', in Jr. Ralph H. Sprague (ed.), *40th Annual Hawaii International Conference on System Sciences 2007 (HICSS 2007)* (Big Island, Hawaii: IEEE), 270c-70c.

Medvet, Eric, Kirda, Engin, and Kruegel, Christopher (2008), 'Visual-similarity-based phishing detection', *Proceedings of the 4th international conference on Security and privacy in communication netowrks* (Istanbul, Turkey: ACM), 22.

Menon, Sundaresh and Siew, Teo Guan (2012), 'Key challenges in tackling economic and cyber crimes: Creating a multilateral platform for international co-operation', *Journal of Money Laundering Control,* 15 (3), 243-56.

Mercuri, Rebecca T (2006), 'Scoping identity theft', *Communications of the ACM,* 49 (5), 17-21.

MessageLabs (2009), 'Cutwail's bounce-back; instant messages can lead to instant malware'.

Microsoft 'SmartScreen Filter', <http://www.microsoft.com/en-gb/security/online-privacy/smartscreen.aspx>, accessed August 15 2014.

Mill, John Stuart (1848), 'Principles of Political Economy With Some of Their Applications to Social Philosophy. 1857', *George Routledge and Sons, Manchester*.

Milletary, Jason (2005), 'Technical trends in phishing attacks', (CERT Coordination Center, Carnegie Mellon University).

Mitnick, Kevin D and Simon, William L (2001), *The art of deception: Controlling the human element of security* (John Wiley & Sons).

MOJ (2010), 'The Passing of the Personal Information Protection Act after Three-reading Procedure of the Legislative Yuan', (The Department of Legal Affairs of the Ministry of Justice, Taiwan).

Moore, Tyler and Clayton, Richard (2007), 'Examining the impact of website take-down on phishing', *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (Pittsburgh, PA, USA: ACM), 1-13.

--- (2008), 'The consequence of non-cooperation in the fight against phishing', *eCrime Researchers Summit, 2008* (IEEE), 1-14.

--- (2009), 'The impact of incentives on notice and take-down', in M. Eric Johnson (ed.), *Managing Information Risk and the Economics of Security* (Springer), 199-223.

Moscaritolo, Angela (2010), 'FBI warns of SMS and phone-based phishing scams', *SC MAGAZINE*. <http://www.scmagazine.com/fbi-warns-of-sms-and-phone-based-phishing-scams/article/191565/>, accessed November 12 2014.

Moynahan, Moynahan (2005), 'Three ways to fight back against phishing', *COMPUTERWORLD*. <http://www.computerworld.com/article/2568318/security0/three-ways-to-fight-back-against-phishing.html>, accessed September 16 2014.

Mozilla 'Mozilla Firefox built-in phishing and malware protection', <https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work>, accessed August 15 2014.

Myers, Steven (2006), 'Introduction to Phishing', in Markus Jakobsson and Steven Myers (eds.), *Phishing and countermeasures: understanding the increasing problem of electronic identity theft* (John Wiley & Sons).

Namestnikov, Yuri (2009), 'The economics of botnets', *Analysis on Viruslist. com, Kaspersky Lab*.

Naor, Moni and Shamir, Adi (1995), 'Visual cryptography', in Alfredo De Santis (ed.), *Advances in Cryptology EUROCRYPT'94 - Workshop on the Theory and Application of Cryptographic Techniques)* (Perugia, Italy: Springer), 1-12.

Nappinai, NS (2009), 'Cyber crime law in india: Has law kept pace with emerging trends? an empirical study', *Journal of International Commercial Law and Technology,* 5 (1), 22-28.

Nazario, Jose and Holz, Thorsten (2008), 'As the net churns: Fast-flux botnet observations', *3rd International Conference on Malicious and Unwanted Software 2008 (MALWARE 2008)* (IEEE), 24-31.

Nero, Philip J, et al. (2011), 'Phishing: Crime that pays', *eCrime Researchers Summit, 2011* (San Diego, USA: IEEE), 1-10.

NETCRAFT 'Netcraft anti-phishing toolbar', <http://toolbar.netcraft.com/>, accessed August 15 2014.

--- 'Phishing Site Takedown & Countermeasures', *Netcraft Inc.* <http://www.netcraft.com/anti-phishing/phishing-site-takedown/>, accessed August 15 2014.

Nielsen, Jakob (2004), 'User education is not the answer to security problems', *Nielsen Norman Group*. <http://www.nngroup.com/articles/security-and-user-education/>, accessed September 17 2014.

Nirmal, K, Ewards, SE Vinodh, and Geetha, K (2010), 'Maximizing online security by providing a 3 factor authentication system to counter-attack'Phishing'', *2010 International Conference on Emerging Trends in Robotics and Communication Technologies (INTERACT)* (IEEE), 388-92.

Nykodym, Nick, et al. (2010), 'Cybercrime and Business: How to not Get Caught by the Online Phisherman', *J. Int'l Com. L. & Tech.,* 5, 252.

OECD (2006), *OECD Anti-Spam Toolkit of Recommended Policies and Measures* (OECD Publishing).

Oussayef, Karim Z (2008), 'Selective privacy: Facilitating market-based solutions to data breaches by standardizing internet privacy policies', *BUJ Sci. & Tech. L.,* 14, 104.

Paget, François (2007), 'Identity theft', *McAfee Avert Labs technical white paper*. <http://www.pubblicaamministrazione.net/file/whitepaper/000042.pdf>, accessed September 17 2014.

Pan, Ying and Ding, Xuhua (2006), 'Anomaly based web phishing page detection', in Bob Werner (ed.), *22nd Annual Computer Security Applications Conference (ACSAC'06)* (Miami Beach, Florida, USA IEEE), 381-92.

Pao, Hsing-Kuo, Chou, Yan-Lin, and Lee, Yuh-Jye (2012), 'Malicious URL Detection Based on Kolmogorov Complexity Estimation', *Proceedings of the The 2012 IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technology - Volume 01* (1: IEEE Computer Society), 380-87.

Parmar, Bimal (2012), 'Protecting against spear-phishing', *Computer Fraud & Security,* 2012 (1), 8-11.

Pfanner, Eric (2011), 'G-8 Leaders to Call for Tighter Internet Regulation', *New York Times*. <http://www.nytimes.com/2011/05/25/technology/25tech.html?_r=2&>, accessed September 17 2014.

Prakash, Pawan, et al. (2010), 'Phishnet: predictive blacklisting to detect phishing attacks', *2010*

Proceedings IEEE INFOCOM (San Diego, California, USA: IEEE), 1-5.

Prosser, William L. (1960), 'Privacy', *California Law Reivew,* 48 (3), 383-423.

Purkait, Swapan (2012), 'Phishing counter measures and their effectiveness - literature review', *Information Management & Computer Security,* 20 (5), 382-420.

Radnor, Hilary (2001), *Researching your professional practice* (Buckingham: Open).

Randall, Kenneth C (1987), 'Universal jurisdiction under international law', *Tex. L. Rev.,* 66, 785.

Reidenberg, Joel R (1997), 'Lex informatica: The formulation of information policy rules through technology', *Tex. L. Rev.,* 76, 553.

Rivner, Uri (2011), 'Anatomy of Attack', *RSA Blog*. <http://blogs.rsa.com/rivner/anatomy-of-an-attack/>, accessed 17 September 2014.

Roberts, Paul (2004), 'More Scam Artists Go Phishing', *PCWorld*. <http://www.pcworld.com/article/116330/article.html>, accessed September 17 2014.

Robila, Stefan A and Ragucci, James W (2006), 'Don't be a phish: steps in user education', *ACM SIGCSE Bulletin* (38: ACM), 237-41.

Robson, William Alexander (1962), *Nationalized industry and public ownership* (G. Allen & Unwin).

Rodenbaugh, Mike (2009), 'ICANN policy developments on abusive domain name registrations', *The IP Litigator: Devoted to Intellectual Property Litigation and Enforcement,* 15, 9-15.

Ronda, Troy, Saroiu, Stefan, and Wolman, Alec (2008), 'Itrustpage: a user-assisted anti-phishing tool', *ACM SIGOPS Operating Systems Review - EuroSys '08* (42; Glasgow, UK: ACM), 261-72.

Rosenberg, Richard S (1992), *The social impact of computers* (Academic Press Professional, Inc.).

Ross, Blake, et al. (2005), 'Stronger Password Authentication Using Browser Extensions', *Proceedings of the 14th conference on USENIX Security Symposium* (14: USENIX Association Berkeley, CA, USA), 17-32.

Roth, Brad (2005), 'State sovereignty, international legality, and moral disagreement', *The annual meeting of the American Political Science Association* (Washington, DC, USA).

Rouse, Margaret (2007), 'Honeynet', *TechTarget*. <http://searchsecurity.techtarget.com/definition/honeynet>, accessed September 17 2014.

Rouvroy, Antoinette and Poullet, Yves (2009), 'The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy', in Serge Gutwirth, et al. (eds.), *Reinventing Data Protection?* (Springer), 45-76.

Saha, Basudev and Gairola, Ashish (2005), 'Botnet: an overview', *CERT-In White Paper, CIWP-2005-05,* 240.

Savirimuthu, Joseph (2008), 'Identity theft and the gullible computer user: what Sun Tzu in the art of war might teach', *J. Int'l Com. L. & Tech.,* 3, 120.

Schechter, Stuart E, et al. (2007), 'The emperor's new security indicators', *2007 IEEE Symposium on Security and Privacy* (Oakland, California, USA: IEEE), 51-65.

Schjolberg, Stein and Ghernaouti-Helie, Solange (2011), 'A global treaty on cybersecurity and cybercrime', *Cybercrime Law*.

SearchITChannel (2006), 'Ready for some spear phishing', *TechTarget*.

<http://searchitchannel.techtarget.com/feature/Ready-for-some-spear-phishing>, accessed September 17 2014.

Sengar, PK and Kumar, Vijay (2010), 'Client-side defense against phishing with pagesafe', *International Journal of Computer Applications,* 4 (4), 6-10.

Seybold, Patrick (2011), 'Update on PlayStation Network and Qriocity', *PlayStation.Blog*. <http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/>, accessed September 19 2014.

Sheng, Steve, et al. (2009a), 'Improving phishing countermeasures: An analysis of expert interviews', *Proceedings of the 4th APWG eCrime Researchers Summit,* 2, 4.

Sheng, Steve, et al. (2010), 'Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, USA: ACM), 373-82.

Sheng, Steve, et al. (2009b), 'An empirical analysis of phishing blacklists', *CEAS 2009: Sixth Conference on Email and Anti-Spam* (Mountain View, California, USA).

Sheng, Steve, et al. (2007), 'Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish', *Proceedings of the 3rd symposium on Usable privacy and security* (Pittsburgh, PA, USA: ACM), 88-99.

Shiu, Nai-Wen (2011a), 'The Report of the Current Status of the Taiwan Information Security Strategic Alliance', *TAIS International Conference 2011* (TWNIC).

Shiu, Tze-Tian (2011b), 'The provisions and debates of the offence of fraud', *Ywe-Dan Jurisprudence Magazine*, 197, 197-200.

Shiu, Wen-Yi (1991), *The Theory of Personal Data Protection Law* (Taipei: San-Min Book Co. Ltd).

Silverman, David (2001), *Interpreting qualitative data: methods for analyzing talk, text and interaction* (London: Sage).

Sofaer, Abraham D and Goodman, Seymour E (2001), 'Cyber Crime and Security. The Transnational Dimension', in Abraham D Sofaer and Seymour E Goodman (eds.), *The transnational dimension of cyber crime and terrorism* (Stanford: Hoover Institution Press), 1-34.

Sophos (2004), 'Do-it-yourself phishing kits found on the internet, reveals Sophos', *Sophos*. <http://www.sophos.com/en-us/press-office/press-releases/2004/08/sa_diyphishing.aspx>, accessed September 19 2014.

Spitzner, Lance (2010), 'Honeytokens: The Other Honeypot', *Symantec* <http://www.symantec.com/connect/articles/honeytokens-other-honeypot>, accessed September 20 2014.

Stamm, Sid, Ramzan, Zulfikar, and Jakobsson, Markus (2007), 'Drive-by pharming', in Hideki Imai and Gullin Wang (eds.), *Information and Communications Security* (Springer), 495-506.

Stebila, Douglas (2010), 'Reinforcing bad behaviour: the misuse of security indicators on popular websites', *Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction* (Brisbane, Australia: ACM), 248-51.

Stevenson, Robert Louis B (2005), 'Plugging the" Phishing" Hole: Legislation Versus Technology', *Duke L. & Tech. Rev.,* 2005, 6-26.

Su, Wen-Bin (2009), 'Taipei becomes the headquarters of bots in the Asia and Pacific Region', *iThome*. <http://www.ithome.com.tw/itadm/article.php?c=54571>, accessed September 20 2014.

Sullins, Lauren L (2006), 'Phishing for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft', *Emory Int'l L. Rev.,* 20, 397.

Sun, Hung-Min, Chen, Yao-Hsin, and Lin, Yue-Hsun (2012), 'oPass: A user authentication protocol resistant to password stealing and password reuse attacks', *Information Forensics and Security, IEEE Transactions on,* 7 (2), 651-63.

Svantesson, Dan Jerker B (2005), 'The characteristics making Internet communication challenge traditional models of regulation–What every international jurist should know about the Internet', *International Journal of Law and Information Technology,* 13 (1), 39-69.

Symantec (2007), 'Symantec Internet Security Threat Report –Trend for July-December 2006', XI. <http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf>, accessed August 30 2014.

--- (2008), 'Symantec APJ Internet Security Threat Report – Trend for July-December 07', XIII. <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_apj_internet_security_threat_report_xiii_04-2008.en-us.pdf>, accessed August 31 2014.

--- (2009a), 'The State of Phishing: A Monthly of Report – May 2009'. <http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_report_05-2009.en-us.pdf>, accessed August 30 2014.

--- (2009b), 'Symantec APJ Internet Security Threat Report – Trend for 2008', XIV. <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_apj_internet_security_threat_report_04-2009.en-us.pdf>, accessed August 29 2014.

--- (2009c), 'The State of Phishing: A Monthly of Report – August 2009'. <http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_report_08-2009.en-us.pdf>, accessed August 31 2014.

--- (2010), 'Symantec Global Internet Security Threat Report –Trend for 2009', XV. <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf>, accessed August 20 2014.

--- (2011), 'SMB Threat Awareness Poll – Global Results'. <http://www.symantec.com/content/en/us/about/media/pdfs/symc-smb-threat-awareness-poll.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Nov_worldwide_SMBflashpoll/>, accessed August 29 2014.

--- (2014), 'Internet Security Threat Report 2014', 19. <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf>, accessed August 31 2014.

Taiwan Network Information Center (2010), 'Wireless Internet Usage in Taiwan – A summary

Report of the January Survey of 2010'. <http://www.twnic.net.tw/download/200307/1001c.pdf>, accessed August 27 2014.

The US President's Identity Theft Task Force (2007), 'Combating Identity Theft: A Strategic Plan'. <http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/downloadabledocuments/combating_identity_theft_a_strategic_plan.pdf>, accessed September 17 2014.

Thomson, K and Van Niekerk, Johan (2012), 'Combating information security apathy by encouraging prosocial organisational behaviour', *Information Management & Computer Security,* 20 (1), 39-46.

TrendMicro 'Tabnapping: new phishing attack works through imposter browser tabs', (updated July 2010) <http://www.trendmicro.com/ftp/documentation/general/TRENDMICRO_JUL10/trendsetter_july10_tabnap.html>, accessed 16 June 2014.

Trubek, David M and Trubek, Louise G (2007), 'New Governance & Legal Regulation: Complementarity, Rivalry, and Transformation', *Columbia Journal of European Law, Summer*.

Trusteer (2008), 'In session phishing attacks', *Trusteer Research Paper*.

Tsai, H. F. (2003), 'The regulations of the Criminal Law of the unauthorised acquirement act of electromagnetic records', *The Jurisprudence Collected Papers of the Chung Cheng University,* 13, 1-196.

Tseng, Shian-Shyong, et al. (2011), 'Automatic content generation for anti-phishing education game', *2011 International Conference on Electrical and Control Engineering (ICECE)* (Yichang, China: IEEE), 6390-94.

Tseng, Shian-Shyong, et al. (2013), 'Building a Frame-Based Anti-Phishing Model based on Phishing Ontology', *The 7th International Conference on Advanced Information Technology* (Chaoyang University of Technology, Taichung, Taiwan).

Tsukayama, Harley (2011), 'Cyber attack on RSA cost EMC $66 million', *The Washington Post*. <http://www.washingtonpost.com/blogs/post-tech/post/cyber-attack-on-rsa-cost-emc-66-million/2011/07/26/gIQA1ceKbI_blog.html>, accessed September 17 2014.

UN (2005), 'Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice', (Bangkok, Tailand: The 11th UN Congress on Crime Preventation and Criminal Justice).

United Kingdom Cabinet Office (2002), 'Identity Fraud: A Study'. <http://www.statewatch.org/news/2004/may/id-fraud-report.pdf>, accessed September 17 2014.

Varghese, Thomas 'Phishing Site Takedown Services – Does this really prevent identity theft?', (updated 31 August 2008) <https://blogs.oracle.com/BornIdentity/entry/phishing_site_takedown_service>, accessed 10 July 2014.

Veljanovski, Cento (2010), 'Economic approaches to regulation', in Robert Baldwin, Martin Cave, and Martin Lodge (eds.), *The Oxford Handbook of Regulation* (Oxford: Oxford University Press), 17-38.

Vijayalekshmi, S and Rabara, S Albert (2010), 'Fending finanicial transaction from phishing attack', *The 2nd International Conference on Trendz in Information Sciences & Computing (TISC), 2010* (Chennai, India: IEEE), 171-75.

Vijayan, Jaikumar (2011), 'Sony Pictures falls victim to major data breach', *COMPUTERWORLD*. <http://www.computerworld.com/s/article/9217273/Sony_Pictures_falls_victim_to_major_data_breach>, accessed September 15 2014.

Volio, Fernando (1981), 'Legal personality, privacy and the family', in Louis Henkin (ed.), *The International Bill of Rights* (New York: Columbia University Press).

Von Ahn, Luis, et al. (2003a), 'CAPTCHA: Using hard AI problems for security', in Eli Biham (ed.), *Advances in Cryptology - EUROCRYPT 2003 (International Conference on the Theory and Applications of Cryptographic Techniques)* (Warsaw, Poland: Springer), 294-311.

Von Ahn, Luis, et al. (2003b), 'Captcha: Telling humans and computers apart automatically', *Proceedings of Eurocrypt*.

von Solms, R. (2013), 'Phishing for phishing awareness', *Behaviour & Information Technology,* 32 (6), 584-93.

Wagner, R Polk (2005), 'On software regulation', *U of Penn. Law School, Public Law Working Paper,* 57.

Wall, David (2003), *Crime and the Internet* (Routledge).

--- (2007), *Cybercrime: The transformation of crime in the information age* (4: Polity).

Wang, Jau-Hwang, et al. (2006), 'Technology-based Financial Frauds in Taiwan: Issues and Approaches', *IEEE International Conference on Systems, Man and Cybernetics, 2006* (6; Taipei, Taiwan: IEEE), 1120-24.

Wang, Jingguo, et al. (2009), 'Visual e-mail authentication and identification services: An investigation of the effects on e-mail use', *Decision Support Systems,* 48 (1), 92-102.

Wang, Jisi (2004a), 'China's Changing Role in Asia', *The Rise of China and a Changing East Asian Order, Tokyo, Japan: Japan Center for International Exchange*.

Wang, Ming-Yong (2004b), 'Criminal Jurisdiction over Computer Crimes', *The Online Symposium of the Academic Research and Practical Deliberation Conference 'Cyberspace: Information, Law and Society* (6), 25-34.

Wang, Te-Yu and Liu, I-Chou (2004), 'Contending identities in Taiwan: Implications for cross-strait relations', *Asian Survey,* 44 (4), 568-90.

Wardman, Brad and Warner, Gary (2008), 'Automating phishing website identification through deep MD5 matching', *eCrime Researchers Summit, 2008* (IEEE), 1-7.

Warren, Samuel D and Brandeis, Louis D (1890), 'The right to privacy', *Harvard law review*, 193-220.

Warrner, Gary (2007), 'Report on the criminal 'Rock Phish' domains registered at Nic.at', *SPAMHAUS*. <http://www.spamhaus.org/organization/statement/7/>, accessed September

15 2014.

Watson, Brett (2004), 'Beyond Identity: Addressing Problems that Persist in an Electronic Mail System with Reliable Sender Identification', *The First Confernece on Email and Anti-Spam (CEAS)* (Mountain view, California, USA).

Watson, David, Holz, Thorsten, and Mueller, Sven (2008), 'Know your Enemy: Phishing', *The Honeynet Project*. <http://www.honeynet.org/papers/phishing/>, accessed September 15 2014.

Waugh, Rob (2010), 'Watch your wall: New Facebook attack has stolen passwords from 45,000 users - and could be spreading through infected links', *Daily Mail*. <http://www.dailymail.co.uk/sciencetech/article-2083118/Facebook-hacked-Ramnit-worm-stolen-passwords-45-000-users.html>, accessed September 13 2014.

Wenyin, Liu, et al. (2005), 'Detection of phishing webpages based on visual similarity', *Special interest tracks and posters of the 14th international conference on World Wide Web* (Chiba, Japna: ACM), 1060-61.

Westin, Alan F (1970), *Privacy and freedom* (London: Bodley Head).

--- (2003), 'Social and political dimensions of privacy', *Journal of social issues,* 59 (2), 431-53.

Whitaker, Reginald (1999), *The end of privacy: How total surveillance is becoming a reality* (The New Press).

Wilson, Carly and Argles, David (2011), 'The fight against phishing: Technology, the end user and legislation', *2011 International Conference on Information Society (i-Society)* (IEEE), 501-04.

Wilson, Clay (2008), 'Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress', *CRS Report for Congress*. <http://fas.org/sgp/crs/terror/RL32114.pdf>, accessed September 20 2014.

Workman, Michael (2008), 'Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security', *Journal of the American Society for Information Science and Technology,* 59 (4), 662-74.

Wu, Ling-Jun (2001), 'The current role and future adjusment of Taiwan in APEC', *NPF Research Report* (National Policy Foundation).

Wu, Min, Miller, Robert C, and Little, Greg (2006a), 'Web wallet: preventing phishing attacks by revealing user intentions', *Proceedings of the second symposium on Usable privacy and security (SOUPS '06)* (Pittsburgh, PA, USA: ACM), 102-13.

Wu, Min, Miller, Robert C, and Garfinkel, Simson L (2006b), 'Do security toolbars actually prevent phishing attacks?', in Rebecca Grinter, et al. (eds.), *Proceedings of the SIGCHI conference on Human Factors in computing systems* (Montreal, Canada: ACM), 601-10.

Xiang, Guang and Hong, Jason I (2009), 'A hybrid phish detection approach by identity discovery and keywords retrieval', *Proceedings of the 18th international conference on World wide web* (Madrid, Spain: ACM), 571-80.

Xu, Shao Xuan (2009), 'Over 3,100 cyber attacks towards Taiwanese government system were originated by Chinese cyber army', *Liberty Times,* 24 March 2009.

Xu, Wanhong, Zhou, Xi, and Li, Lei (2008), 'Inferring privacy information via social relations', *IEEE 24th International Conference on Data Engineering Workshop, 2008 (ICDEW 2008)* (Cancun, Mexico: IEEE), 525-30.

Yang, Che-Ching, et al. (2012), 'Building an Anti-phishing Game to Enhance Network Security Literacy Learning', in Ignacio Aedo, et al. (eds.), *2012 IEEE 12th International Conference on Advanced Learning Technologies (ICALT)* (Rome, Italy: IEEE), 121-23.

Yang, Phillip Y. M. (1997), 'Taiwan's approaches to APEC: economic cooperation, political significance, and international participation', *International Conference on Canada-Taiwan Relations in the 1990s* (National ChengChi Univeristy, Taipei, Taiwan).

Ye, C. S. (2003), 'The comparison of legislation amendments to the Criminal Code in relation to computer crime and the research on practical problems', in Ministry of Justice (ed.), *Collection of Papers on Criminal Policies and Research of Crimes* (6:4), 1-17.

Yee, Ka-Ping and Sitaker, Kragen (2006), 'Passpet: convenient password management and phishing protection', *Proceedings of the second symposium on Usable privacy and security (SOUPS '06)* (Pittsburgh, PA, USA: ACM), 32-43.

Yenurkar, Mr Bhushan and Zade, Mr Shrikant (2014), 'An anti-phishing framework with new validation scheme using visual cryptography ', *International Journal of Computer Science and Mobile Computing (IJCSMC),* 3 (2), 739-44.

Yu, Eileen (2011), 'China dispatches online army', *ZDNet*. <http://www.zdnet.com/china-dispatches-online-army-2062300502/>, accessed September 12 2014.

Yue, Chuan and Wang, Haining (2008), 'Anti-phishing in offense and defense', *Annual Computer Security Applications Conference, 2008 (ACSAC 2008)* (Anaheim, California, USA: IEEE), 345-54.

--- (2010), 'BogusBiter: A transparent protection against phishing attacks', *ACM Transactions on Internet Technology (TOIT),* 10 (2), 6.

Zaid, Mark S (1997), 'Taiwan: It Looks like It, It Acts like It, but Is It a State-The Ability to Achieve a Dream through Membership in International Organization', *New Eng. L. Rev.,* 32, 805.

ZAMYATIN, Evgeny Ivanovich, GLENNY, Michael V, and GUERNEY, Bernard Guilbert (1972), *We... Translated [from the Russian MS.] by Bernard Guilbert Guerney. Introduction by Michael Glenny* (Penguin).

ZDNet (2007), 'Taipei has beceome the principal setting location of phishing web sites within the Asia-Pacific region', (ZDNet).

Zhang, Haijun, et al. (2011), 'Textual and visual content-based anti-phishing: a Bayesian approach', *Neural Networks, IEEE Transactions on,* 22 (10), 1532-46.

Zhang, Jian, Porras, Phillip A, and Ullrich, Johannes (2008), 'Highly Predictive Blacklisting', in Paul Van Oorschot (ed.), *17th USENIX Security Symposium* (San Jose, CA), 107-22.

Zhang, Yue, Hong, Jason I, and Cranor, Lorrie F (2007a), 'Cantina: a content-based approach to detecting phishing web sites', *Proceedings of the 16th international conference on World*

Wide Web (Banff, AB, Canada: ACM), 639-48.

Zhang, Yue, et al. (2007b), 'Phinding phish: Evaluating anti-phishing tools', *Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS 2007)* (San Diego, CA, USA).

Zheleva, Elena and Getoor, Lise (2009), 'To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles', *Proceedings of the 18th international conference on World wide web* (Madrid, Spain: ACM), 531-40.

APPENDIX A – LIST OF INTERVIEWEES

CODE NAME	POSITION
Interviewee A	Police officer from the specialized investigation unit for Internet crime
Interviewee B	Police officer from the specialized investigation unit for Internet crime
Interviewee C	Lawmaker for the cybercrime laws of Taiwan Executive of an online merchant
Interviewee D	Expert from the information security department of the leading ISP of Taiwan
Interviewee E	Expert from TWNIC
Interviewee F	Expert from information security industry
Interviewee G	Official from the Resources and Technologies Department of NCC
Interviewee H	Expert from information security industry

APPENDIX B – TAIWANESE LEGISLATION

Constitution

Art. 22 –

All other freedoms and rights of the people that are not detrimental to social order or public welfare shall be guaranteed under the Constitution.

Art. 23 –

All the freedoms and rights enumerated in the preceding Articles shall not be restricted by law except by such as may be necessary to prevent infringement upon the freedoms of other persons, to avert an imminent crisis, to maintain social order or to advance public welfare.

Civil Code

Art. 184 -

A person who, intentionally or negligently, has wrongfully damaged the rights of another is bound to compensate him for any injury arising therefrom. The same rule shall be applied when the injury is done intentionally in a manner against the rules of morals.

A person, who violates a statutory provision enacted for the protection of others and therefore prejudice to others, is bound to compensate for the injury, except no negligence in his act can be proved.

Civil Procedure Code

Art. 1.1 –

A defendant may be sued in the court for the place of the defendant's domicile or, when that court cannot exercise jurisdiction, in the court for the place of defendant's residence. A defendant may also be sued in the court for the place of defendant's residence for a claim arising from transactions or occurrences taking place within the jurisdiction of that court.

Art.15.1 –

In matters relating to torts, an action may be initiated in the court for the location where the tortious act occurred.

Art. 22 –
When several courts may have jurisdiction over an action, a plaintiff may choose to initiate the action in any one of those courts.

Application Laws for Foreign-related Civil Law

Art. 25-
Claims grounded on tort shall be governed by the law of the State in which the tort was committed.

Art. 28.1-
Claims grounded on tort committed by disseminative means, such as the press, radio, television, computer Internet or other media methods shall be governed by the following three choices of laws at the option of the injured party:

a. The law of the State in which the tort was committed or the law of the State of domicile of the tortfeasor if the place of commitment cannot be identified;
b. The law of the State in which the injuries or the infringement have occurred if the tortfeasor should have foreseen that the injuries would occur in that State; and
c. The law of the State of the injured party if the act caused an infringement of personality rights.

Copyright Act

Art. 3.1(1) and (5) –
For the purposes of this Act the following definitions shall apply:

1."Work" means a creation that is within a literary, scientific, artistic, or other intellectual domain.
5."Reproduce" means to reproduce directly, indirectly, permanently, or temporarily a work by means of printing, reprography, sound recording, video recording, photography, handwritten notes, or otherwise. This definition also applies to the sound recording or video recording of scripts, musical works, or works of similar nature during their performance or broadcast, and also includes the construction of an architectural structure based on architectural plans or models.

Art. 84 –
The copyright holder or the plate rights holder may demand removal of infringement of its rights. Where there is likelihood of infringement, a demand may be made to prevent such infringement.

Art. 88.1 –
A person who unlawfully infringes on another person's economic rights or plate rights out of intention or negligence shall be liable for damages. Where multiple persons engage in unlawful

infringement, they shall bear joint and several liability for damages.

Art. 91-1.2 –
A person who distributes or with intent to distribute publicly displays or possesses a copy knowing that it infringes on economic rights shall be imprisoned not more than three years and, in addition thereto, may be fined not less than seventy thousand and not more than seven hundred and fifty thousand New Taiwan Dollars.

Trademark Act

Art. 70.2 –
Any of the following acts, without consent of the proprietor of a registered trademark, shall be deemed infringement of the right of such trademark:
[…] (2) knowingly using words contained in another person’s well-known registered trademark as the name of a company, business, group or domain or any other name that identifies a business entity, and hence there exists a likelihood of confusion on relevant consumers or a likelihood of dilution of the distinctiveness or reputation of the said well-known trademark; […]

Art. 69.1 –
A proprietor of a registered trademark is entitled to demand a person who infringes or is likely to infringe the trademark right to stop or prevent such infringement.

Art. 69.3 –
The proprietor is entitled to demand the infringer who knowingly, or with reasonable grounds to know, infringed such trademark rights to pay the proprietor damages.

Personal Information Protection Act (PIP Act)

Art. 1 –
Personal Information Protection Act（hereinafter “this Law”）is enacted to govern the collection, processing and use of personal information so as to prevent harm on personality rights, and to facilitate the proper use of personal information.

Art. 2 –
The terms used herein denote the following meanings:
1. Personal information: the name, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, social activities and other information which may be used to identify a natural person,

both directly and indirectly;

2. Personal information file: A collection of personal information built to allow information retrieval and management by automatic or non-automatic measures;

3. Collection: To collect personal information in any form and way;

4. Processing: To record, input, store, compile, correct, duplicate, retrieve, delete, output, connect or internally transmit information for the purpose of establishing or using a personal information file;

5. Use: All methods of personal information use other than processing;

6. International transmission: The cross-border processing or use of personal information;

7. Government agency refers to a government agency or administrative juridical person at the central or local government level which is empowered to exercise sovereign power;

8. Non-government agency refers to the natural persons, juridical persons or groups other than those stated in the proceeding item;

9. The Party means an individual of whom the personal information has been collected, processed or used in accordance with this Law.

Art. 5 –

The rights and interests of the Party should be respected in collecting, processing or using personal information and the information should be handled in accordance with the principle of bona fide. It should not go beyond the purpose of collection and should be reasonable and fair.

Art. 6 (suspended) –

Personal information of medical treatment, genetic information, sexual life, health examination and criminal record should not be collected, processed or used. However, the following situations are not subject to the limits set in the preceding sentence:

1. when in accordance with law;

2. when it is necessary for the government agency to perform its duties or for the non- government agency to fulfill the legal obligation, and when there are proper security measures.

3. when the Party has disclosed such information by himself, or when the information concerned has been publicized legally;

4. when the personal information is collected, processed or used under certain methods by a government agency or an academic research institution based on the purpose of medical treatment, personal hygiene or crime prevention statistics and/or study.

The rules of the range, procedure and any other items to be followed concerning Item 4 of the preceding Paragraph should be set by the government authority in charge of subject industry at the central government level in conjunction with the Ministry of Justice.

Art. 8 –

The following items should be told precisely to the Party by a government agency or non-government agency, in accordance with Article 15 or Article 19:

1. the name of the government agency or the non government agency;
2. purpose of collection;
3. classification of the personal information;
4. time period, area, target and way of the use of personal information;
5. rights of the Party and ways to exercise them as prescribed in Article 3;
6. the influence on his rights and interests while the Party chooses not to provide his personal information;
The following situations may be exempted from the notice prescribed in the preceding Paragraph:
1. when in accordance with law;
2. when the collection of personal information is necessary for the government agency to perform its official duties or the non government agency to fulfill the legal obligation;
3. when the notice will impair the government agency in performing its official duties;
4. when the notice will impair the interests of a third person;.
5. when the Party should have known the content of the notification already.

Art. 9 –
A government agency or non-government agency should notify the Party of the source of information and Item 1 to 5 of Paragraph 1 of the preceding Article, before processing or using personal information collected in accordance with Article 15 or 19 which was not provided by the Party.
The notification mentioned in the preceding Paragraph may not be given for the followings:
1. Under one of the situations listed in Paragraph 2 of the preceding Article;
2. When the Party has disclosed such information by himself or when the information has been publicized legally;
3. When the notification may not be made to the Party or his legal representative;
4. When it is necessary for public interests on statistics or the purpose of academic research. The information may not be used to identify a certain person after a treatment of the provider or the disclosure of the collector;
5. Personal information collected by the mass media for the purpose of news reporting on the basis of public interests;
The notification mentioned in Paragraph 1 may be undertaken when the personal information is used against the Party for the first time.

Art. 11 –
The government agency or the non government agency should ensure the accuracy of personal information, and correct or supplement it, ex officio or upon the request of the Party.
In the event of a dispute regarding the accuracy of personal information, the agency should discontinue processing or using the information, ex officio or upon the request of the Party. However, the preceding sentence may not be applicable when it is necessary for the performance of

an official duty or fulfillment of a legal obligation and has been recorded, or when it is agreed by the Party in writing.

The information collected should be deleted, discontinued to process or use, ex officio or upon the request of the Party when the specific purpose no longer exists or time period expires. However, the preceding sentence may not be applicable when it is necessary for the performance of an official duty or fulfillment of a legal obligation and has been recorded, or when it is agreed by the Party in writing.

The information collected should be deleted, discontinued to process or use, ex officio or upon the request of the Party in the cases where a violation of this Law occurred during collecting, processing or using that information.

In the cases where the government agency or the non-government agency should be attributed to of not correcting or supplementing personal information, persons to whom the personal information was provided should be notified after correction or supplement.

Art. 12 –

When the personal information is stolen, disclosed, altered or infringed in other ways due to the violation of this Law, the government agency or non-government agency should notify the Party after an inspection.

Art. 15 –

Except the information stated in Paragraph 1 of Article 6, the government agency should not collect or process personal information unless there is a specific purpose and should comply with one of the following conditions:

1. it is within the scope of job functions provided by laws and regulations;
2. a written consent has been made by the Party; and
3. the rights and interests of the Party may not be harmed.

Art. 16 –

Except the information stated in Paragraph 1 of Article 6, the government agency should use the personal information in accordance with the scope of its job functions provided by laws and regulations, and in compliance with the specific purpose of collection. However, the information may be used outside the scope upon the occurrence of one of the following conditions:

1. Where in accordance with law;
2. Where it is for national security or to promote public interests;
3. Where it is to prevent harm on the life, body, freedom or property of the Party;
4. Where it is to prevent harm on the rights and interests of other people;
5. Where it is necessary for public interests on statistics or the purpose of academic research conducted by a government agency or an academic research institution, respectively. The information may not lead to the identification of a certain person after the treatment of the provider

or the disclosure of the collector;
6. Where such use may benefit the Party; and
7. A written consent of the Party has been obtained.

Art. 18 –
The government agency which keeps personal information files should assign personnel(s) on security and maintenance of those files to prevent them from being stolen, altered, damaged, destroyed or disclosed.

Art. 19 –
Except the information stated in Paragraph 1 of Article 6, the non-government agency should not collect or process personal information unless there is a specific purpose and should comply with one of the following conditions:
1. Where in accordance with law;
2. Where there is a contract or quasi-contract between the Party and the agency;
3. Where the Party has disclosed such information by himself or when the information has been publicized legally;
4. Where it is necessary for public interests on statistics or the purpose of academic research conducted by a research institution. The information may not lead to the identification of a certain person after the treatment of the provider or the disclosure of the collector;
5. Where a written consent has been made by the Party;
6. Where the public interest is involved; and
7. Where the personal information is obtained from publicly available resources. However, it is exempted if the information is limited by the Party on the processing or use and the interests of the Party should be protected.
By the time when the collector or processor realizes or has been notified of the provision in Item 7 of the preceding Paragraph by the Party, he should delete, stop processing or using the personal information, ex officio or upon the request of the Party.

Art. 20 –
Except the information stated in Paragraph 1 of Article 6, the non-government agency should use the personal information in accordance with the scope of the specific purpose of collection provided. However, the information may be used outside the scope upon the occurrence of one of the following conditions:
1. Where in accordance with law;
2. Where it is to promote public interests;
3. Where it is to prevent harm on the life, body, freedom or property of the Party;
4. Where it is to prevent harm on the rights and interests of other people;
5. Where it is necessary for public interests on statistics or the purpose of academic research

conducted by a government agency or an academic research institution, respectively. The information may not lead to the identification of a certain person after the treatment of the provider or the disclosure of the collector;

6. Where a written consent of the Party has been obtained.

When the non-government agency uses the personal information for the purpose of marketing pursuant to the preceding Paragraph and has been turned down by the Party, the agency should stop its action.

The non-government agency should notify the Party the measures of refusal at the first marketing action and should pay for fees necessary.

Art. 27.1, 27.2–

The non-government agency which keeps personal information files should adopt proper security measures to prevent them from being stolen, altered, damaged, destroyed or disclosed.

The government authority in charge of subject industry at the central government level may designate a non-government agency for setting up the plan of security measures for the personal information file or the disposal measures for the personal information after termination of business.

Art. 28 –

A government agency should be liable for damages and compensation caused by illegal collection, processing and using of personal information, or other ways of infringement on the rights of the Party due to violation of this Law. However, it does not apply to damages caused by natural disaster, incident or other force majeure.

A proper amount of monetary compensation may be requested for damage not to properties. A proper rehabilitation action may be requested upon infringement to reputation.

The total amount of compensation for the damages referred to in the two preceding Paragraphs shall be no less than NT$500 but no more than NT$20,000 for each case of damages per person in the cases where the victims in the two preceding Paragraphs may not or cannot provide evidence for actual damage amount.

With regard to damages caused to multi parties by the same cause and fact, the total amount of compensation should not exceed NT$200 million. However, if the interests involved are over the amount in the preceding sentence, the amount of interests should be set as the limit.

If the total amount of damage caused by the same cause and fact exceeds the amount mentioned in the preceding Paragraph, the compensation amount to the victim should not be limited by the baseline（NT$500）set in Paragraph 3 of this Article.

The right of claim referred to in the second Paragraph above should not be transferred or inherited. However, it does not apply to the situation where the monetary compensation has been undertaken according to an agreement or the case has been brought to the court.

Art. 29 –

A non-government agency should be liable for damages and compensation caused by illegal collection, processing and using of personal information, or other ways of infringement on the rights of the Party due to violation of this Law. However, it does not apply to the situation where the non-government agency can be proved to be unintentional or non-negligent.

The provisions of Paragraphs 2 to 6 of the preceding Article are applicable to claims for damages made in accordance with the provisions of the preceding Paragraph.

Art. 41 –

A violation to Paragraph 1 of Article 6, Articles 15, 16, 17, 19 and Paragraph 1 of Article 20, or an order or disciplinary action of the limitation on international transmission made by the government authority in charge of subject industry at the central government level in accordance with Article 21 which may harm other people's rights should be imposed of a sentence or custody of no more than 2 years, or a fine of no more than NT$200,000, or both.

A person who intends to commit the crime in the preceding Paragraph should be imposed of a sentence of no more than 5 years and a fine of no more than NT$1,000,000.

Art. 54 (suspended) –

For the personal information which is not provided by the Party before the amendment of this Law and is subject to a notice to the Party prior to processing or use in accordance with Article 9, the personal information controller should fulfill its notice duty within one year after the effective date of this Law Amendment. Any processing or use of the personal information without notification in the overdue period of time is regarded as violation of Article 9.

Enforcement Rules of the Personal Information Protection Act

Art. 3 –

"Other information which may be used to identify a natural person indirectly" referred to in Item 1 of Article 2 of the Act shall mean that the government agency or the non-government agency possessing the information can not directly identify the specific person without comparing to, combining with or connecting to other information.

Art. 12 –

"Proper security measures" referred to in Item 2 of Paragraph 1 of Article 6, "security and maintenance" referred to in Article 18, and "proper security measures" referred to in Paragraph 1 of Article 27 of the Act shall mean the technical or organizational measures taken by the government agency or the non-government agency for the purpose of preventing personal information from being stolen, altered, damaged, destroyed or disclosed.

The measures prescribed in the preceding paragraph may include the following matters and shall

follow the principle of appropriate proportionality to achieve the objective of personal information protection:
(1) allocating management personnel and substantial resources;
(2) defining the scope of personal information;
(3) establishing the mechanism of risk evaluation and management of personal information;
(4) establishing the mechanism of preventing, giving notice of, and responding to accidents;
(5) establishing an internal management procedure of collecting, processing, and using personal information;
(6) managing information security and personnel;
(7) promoting acknowledgement, education and training;
(8) managing facility security;
(9) establishing a mechanism of auditing information security;
(10) keeping records of the use, locus information and proof; and
(11) Integrated persistent improvements on the security and maintenance of personal information.

Art. 19 –
When requesting the government agency or the non-government agency to correct or supplement his/her personal information, the Party shall make an appropriate explanation.

Art. 22 –
“Appropriate methods of notification” referred to in Article 12 of the Act shall mean prompt words, written document, telephone, text message, email, facsimile, electronic record or other manners which will be sufficient to make or likely make the Party know such notification. However, if the notification costs too much, in consideration of the technical feasibility and privacy protection of the Party, such notification may be made via internet, news media or other appropriate manners to notice.
The contents of “notification to the Party” referred to in Article 12 of the Act shall include the fact that personal information has been infringed and the responding measures which have been taken.

Art. 25.1 –
“Personnel(s)” referred to in Article 18 of the Act shall mean personnel with the ability to manage and maintain personal information files and to sufficiently perform the regular task of securing and maintaining personal information for the agency.

Art. 28 –
“Publicly available resources” referred to in Item 7 of Paragraph 1 of Article 19 of the Act shall mean mass media, internet, news, magazine, government gazette and other accesses through which the general public may be aware of or contact, and thus obtain personal information.

Criminal Code

Art. 3 –

This Code shall apply to an offense committed within the territory of the Republic of China. An offense committed on board a vessel or aircraft of the Republic of China outside the territory of the Republic of China shall be considered an offense committed within the territory of the Republic of China.

Art. 4 –

Where either the conduct or the result of an offense takes place within the territory of the Republic of China, the offense shall be considered as committed within the territory of the Republic of China.

Art. 5 –

This Code shall apply to any of the following offenses outside the territories of the Republic of China:

1. The offense of sedition specified in Article 100.
2. The offense of treason specified in Article 103.
3. The offense of obstructing governmental operation specified in Article 135, 136 or 138.
4. The offenses against public safety specified in Article 185-1 or 185-2.
5. The offenses of counterfeiting currency specified in Article 195 to 199.
6. The offenses of counterfeiting securities specified in Articles 201 to 202.
7. The offenses of forgery specified in Articles 211, 214, 218 or 216, in which only includes using forged official documents as specified in Articles 211, 213 and 214.
8. The drug offenses specified in Chapter 20, except for the offenses of drug abuse or possession of drugs, seeds or application tools or drug.
9. The offenses against personal freedom specified in Articles 296 and 296-1
10. The offenses of piracy specified in Articles 333 and 334.

Art. 6 –

This Code shall apply to any of the following offenses committed by a public official of the Republic of China outside the territory of the Republic of China：

1. The offenses of malfeasance specified in Articles 121 to 123, 125, 126, 129, 131, 132, or 134.
2. The offense of facilitating escape specified in Article 163.
3. The offenses of forgery specified in Article 213.
4. The offenses of embezzlement specified in Article 336,paragraph 1.

Art. 7 –

This Code shall apply where any national of Republic of China commits an offense which is not specified in one of the two preceding articles but is punishable for not less than 3 years of imprisonment outside the territory of the Republic of China; unless the offense is not punishable by the law of the place where the offense is committed.

Art. 10.6 –

The term electromagnetic recording means records for computer process made through the use of electronic, magnetic, optical or other similar means.

Art. 320 –

A person who for purpose to exercise unlawful control over other’s property for himself or for a third person unlawfully takes movable property of another commits larceny and shall be sentenced to imprisonment for not more than five years, short-term imprisonment, or a fine of not more than five hundred yuan.

A person who for purpose to gain unlawful benefit of himself or of a third person unlawfully occupies the real property of another shall be punished in accordance with provisions of the preceding paragraph.

An attempt to commit an offense specified in one of the two preceding paragraphs is punishable.

Art. 339 –

A person who by fraud causes another to deliver to him property belonging to such other or to a third person for purpose to exercise unlawful control over other’s property for himself or for a fourth person shall be sentenced to imprisonment for not more than five years or short-term imprisonment; in lieu thereof, or in addition thereto, a fine of not more than one thousand yuan may be imposed.

A person who by the means specified in the preceding paragraph takes an illegal benefit for himself or for a third person shall be subject to the same punishment.

An attempt to commit an offense specified in one of the two preceding paragraphs is punishable.

Art. 358 –

A person who without reason by entering another’s account code and password, breaking his computer protection, or taking advantage of the system loophole of such other accesses his computer or relating equipment shall be sentenced to imprisonment for not more than three years or short-term imprisonment; in lieu thereof, or in addition thereto, a fine of not more than one hundred thousand yuan may be imposed.

Art. 359 –

A person without reason obtains, deletes or alters the magnetic record of another’s computer or relating equipment and causes injury to the public or others shall be sentenced to imprisonment of no more than five years or short-term imprisonment; in lieu thereof, or in addition thereto, a fine of not more than two hundred thousand yuan may be imposed.

Art. 360 –

A person who without reason interferes, through the use of computer programs or other electromagnetic methods, with the computer or relating equipment of another person and causes injury to the public or another shall be sentenced to imprisonment for not more that three years or short-term imprisonment; in lieu thereof, or in addition thereto, a fine of not more than one hundred thousand yuan may be imposed.

Art. 361 –

A person who commits the offenses specified in the three preceding articles against the computers and relating equipment of a public office shall be punished by increasing the punishment up to one half.

Art. 362 –

A person who makes computer programs specifically for himself or another to commit the offenses specified in this Chapter and causes injury to the public or another shall be punished for imprisonment for not more than five years or short-term imprisonment; in lieu thereof, or in addition thereto, a fine of not more than two hundred thousand yuan may be imposed.

Art. 363 –

The prosecution of the offenses specified in articles, 358 through 360, may be instituted only upon complaint.

Criminal Procedure Code

Art. 5 –

A court of the place where an offense is committed or where an accused is domiciled, resides, or is located shall have jurisdiction over the case.

If an offense is committed on a vessel or an aircraft of the Republic of China outside the territory of the Republic of China, the court of the place where the vessel is registered or from which the aircraft departed or landed after the commission of the offense shall also have jurisdiction.