Whitty, Monica T. (2015). *Mass-marketing fraud: A growing concern. IEEE Security & Privacy, 13* (4), pp. 84-87.

Mass-marketing fraud: A growing concern

Monica T. Whitty

University of Leicester

A growing international concern for end users is massmarketing fraud, which exploits mass communication techniques (such as email, instant messenging, bulk mailing, and social networking sites) to target victims for financial profit. The Internet has opened the floodgates to fraud, given that criminals can use it to target many more potential victims. Mass-marketing fraud is a serious, complex, and often organized crime. Examples include foreign lotteries and sweepstakes fraud, in which victims believe they have won money and are told to pay a fee to receive the funds; 419 scams or advance fee fraud, in which victims believe that for a small amount of money they will make a large fortune; and romance scams, in which victims send money to someone posing as a romantic interest on an online dating site.

In 2010, the International Mass- Marketing Fraud Working Group reported that this type of crime has gradually transformed from a predominantly North American problem into a pervasive global criminal threat.1 Since 2012, in the UK, approximately 2.6 million adults have fallen for these scams, with about 500,000 adults falling victim to a dating or romance scam; around 900,000 being conned by a boiler room scam (where victims are pressured into buying fake, overpriced, or worthless stocks) ; 700,000 by a charity scam; 900,000 by a “need funds for an

emergency" scam; 700,000 by an inheritance scam; and 800,000 by a lottery scam. In 2012 alone, some 800,000 UK adults were victims of this kind of fraud. Of further concern is that nearly a quarter of victims are scammed at least twice.[2]

Reporting bodies in the UK, such as Action Fraud, estimate that less than 10 percent of the population actually report this type of crime, partly because of the shame and embarrassment associated with becoming a victim, lack of knowledge of where and how to report the crime, and the awareness that it's unlikely that criminals will be located or prosecuted. In the US, the Internet Crime Complaint Center (IC3) reported that in 2014, 123,684 victims reported financial losses as a result of Internet crimes, many of which were mass-marketing fraud. The most common complaints included auto fraud, government impersonation, intimidation or extortion, real estate scams, and romance scams. It's estimated that only 10 percent of victims report the crime to IC3.[3] In Australia, just over AUS$94 million was reported lost by victims of mass-marketing fraud in 2012.[4]

Costs of Cybercrime

Researchers have yet to accurately measure the amount lost to individuals and as Dinei Florencio and Cormac Herley point out, we need to take a cautious approach to survey results about losses, because outliers can distort the results.5 For example, "a single individual who claims [US]$50,000 in losses, in a 1,000 person survey, is all it takes to generate a $10 billion loss over the population. One unverified claim of $7,500 in phishing losses translates into $1.5 billion."[5]

Ross Anderson and his colleagues argue that our response to cybercrime is so

disproportionate that we overspend protecting against it.[6] They note that "traditional offences such as tax and welfare fraud cost the typical citizen in the low hundreds of pounds/Euros/ dollars a year; transitional frauds cost a few pounds/Euros/dollars; while the new computer crimes cost in the tens of pence/cents." However, indirect and defense costs "are much higher for transitional and new crimes. For the former, they may be roughly comparable to what the criminals earn, while for the latter they may be an order of magnitude more." These points are important when considering the costs of cybercrime; however, in addition to financial losses, we must consider the costs to the psychological well-being of victims as well as family members and friends who are often impacted by mass-marketing fraud.[7]

Psychological Impact

The psychological effects of massmarketing fraud can sometimes outweigh the financial impact, even when large sums of money are lost.[8,9] The Office of Fair Trading reported that "in contrast to other types of crime, scams are a 'silent' crime for which victims may receive little support. Because there is usually not a visible perpetrator, it can also be difficult for victims to get closure."[10] Psychological harm can include shame, guilt, embarrassment, depression, suicidal feelings, grief, anxiety, and loss of trust.[11]

Unlike most other crimes, massmarketing fraud victims are often blamed for their victimization. Family and friends, who are typically an important source of support for victims, often blame the victims, pointing out how they too have been affected (such as losing their inheritance). Victims are often viewed by society and depicted in the media as stupid or naive. This makes recovery from this crime even more

difficult, especially given that victims aren't likely to have their funds recovered. Furthermore, preliminary findings suggest that aftercare for victims needs to be long term, which can be too expensive for victims.[8,11] Websites and online support groups such as www.romancescams.org and www.scamsurvivors.com have emerged where victims can support one another, although the effectiveness of this type of support is yet to be empirically tested.

Vulnerability and Persuasive Techniques

Research on the types of people most likely to be victims of scams has mostly focused on "get rich quick" schemes.[12] Nonetheless, these studies provide some important insights into the sorts of individuals who are more vulnerable to mass-marketing fraud. Steve Furnell argued that greedy and naive individuals are more likely to be conned.[13] Jinkook Lee and Horacio Soberon-Ferrer found that victims of fraud tend to be older, poorer, less educated, and single.[12] Kristy Holtfreter and her colleagues looked broadly at consumer fraud victimization and found that victims were more likely to have low self-control.[14] In contrast, it's been found that those who are considered sensation seekers aren't more likely to be scammed by the online dating romance scam; rather, for those who score high on the Romantic Belief Scale, idealization is more associated with the likelihood of being a victim.[7,11]

In explaining the success of mass-marketing fraud, scholars mostly draw from social psychological theories and apply them to these scams. An Office of Fair Trading report offers the most comprehensive explanation of the psychology of scams.[15] The report argues that "falling for a scam comes down to errors in decision-making," and that "scammers create situations (with their scam offers) that increase the likelihood

of poor decision-making." The authors found that both cognitive (overconfidence in a specific topic) and motivational (the scam triggers positive emotions) processes explained the psychological reasons for responding to scams. Across their studies, the most consistent reasons people were drawn into scams were "appeals to trust and authority" (the use of people or institutions of authority to make the scam appear legitimate) and "visceral triggers" (triggers employed to make potential victims focus on huge prizes and imagined positive future emotional states).

However, other persuasive techniques are worth considering. For example, scarcity has been found to play a role; that is, presenting offers that have time limits.[9] Classic marketing strategies such as the foot-in-the-door technique (asking for small amounts of money first and gradually increasing the requests as the person continues to comply) and the door-in-the-face technique (asking for large amounts of money and gradually decreasing the amount until the person is willing to comply) have also been found effective.[9] Frank Stanjano and Paul Wilson analyzed face-to-face cons and found that attackers use a limited number of techniques to manipulate their victims.[16]

In addition to classic persuasive techniques, I would argue that it' equally important to focus on the role the Internet plays in persuading individuals to part with their money. In the past, researchers have found that individuals develop very trusting, intimate relationships online.[17] Given this, we might postulate that the Internet is the ideal place for criminals to target strangers to earn their trust.

I've found that one-sided, hyperpersonal relationships often develop between victims and scammers. [9] Victims idealize the fake persona, believing they have found the

perfect romantic partner. Given that much of the communication is asynchronous, criminals have time to develop the illusion of the ideal person, making it easier to trick victims into falling in love with them. Joseph Walther also found that when people are communicating via the Internet, they become much more focused on their online communications, blocking out other environments.[17]

I've also found that victims of the romance scam report continuously re-reading emails and looking forward to the next email or chat session. When communicating online, a record is kept for individuals to revisit whenever they want, reinforcing the romantic messages being sent by criminals.

Therefore, I believe online communication helps strengthen the perceived emotional bond, making it difficult for victims to escape the relationship. The same idea could apply to other types of scams in which criminals spend time communicating with victims before asking them for money.

A Stage Theory Approach

Thinking of scams as a series of stages is a useful method of gaining greater insight into their anatomy. I've outlined six stages involved in the romance scam, which could potentially be applied to other types of mass-marketing fraud:

■ stage 1—potential victims need to be motivated to find the "ideal" partner;

■ stage 2—potential victims are presented with the profile of an ideal partner and promised an exclusive relationship;

■ stage 3—potential victims are groomed to trust and love the criminal, who then gauges whether potential victims are ready and willing to part with their money;

■ stage 4—the criminal employs techniques to persuade potential victims to send money (such as a narrative about a crisis where money is urgently needed or the foot-in-the-door technique);

■ stage 5—the criminal employs further techniques to keep the scam alive, such as inventing another crisis or employing the door-in-the-face technique; and

■ stage 6—victims might believe the scam is over and are subsequently revictimized (the criminal admits to the scam but claims to be in love and then asks for more money, or victims receive an email from the criminal pretending to be law enforcement asking for a small amount of money to return their funds).[9]

Prevention

Preventing mass-marketing fraud is a difficult task. Catching and prosecuting attackers is challenging given that the criminals often live in a different country than the victims; the methods the criminals use make them difficult to trace; and prosecution is very time consuming, owing to the large amounts of online data that needs to be analyzed to establish evidence and gain intelligence on the criminals' whereabouts and operating tactics. Other methods are needed to help prevent these crimes.

Law enforcement and others have attempted to prevent these crimes by using disruption tactics. Users of dating sites, for instance, have been encouraged to report known fake profiles to help reduce the number of criminal profiles on these sites. Law enforcement has also tried to influence a change in the way money is transferred via money transfer companies, such as Western Union and MoneyGram, so that users are traceable. Doing so would make catching criminals easier and could deter other

criminals. Moreover, these transfer companies have been encouraged to enter suspicious activity reports for any transaction that appears to have been conducted by a scammer. However, even if such strategies were successful, criminals could potentially find a loophole (for example, persuading victims to unknowingly transfer money into other victims' accounts, making the money more difficult to trace back to criminals as well as involving victims in money laundering).

Unfortunately, awareness of mass-marketing fraud doesn't necessarily prevent individuals from becoming victims. Researchers have found that many victims who fall for mass-marketing frauds have heard of these scams, and some even have detailed knowledge of them.[11,15] The 2009 Office of Fair Trading report argues that detailed knowledge of a scam can, in fact, increase vulnerability because these individuals often develop an "illusion of invulnerability." [15] Moreover, once victims are hooked into a scam, it's very difficult to make them believe it was a hoax. I've found that even when authority figures (such as police, law enforcement, and bank managers) alert people to the fact that they are victims of a romance scam, victims often have difficulty believing it. Moreover, when victims question criminals about their authenticity, criminals will employ persuasive techniques to convince victims otherwise.18 Given that knowledge about a scam might not be enough to prevent individuals from becoming defrauded, other types of interventions are needed. Stajano and Wilson contend that because attackers consistently use a small number of well-established tricks, system designers could do more to prevent exploitation: "Our message for the system-security architect is that it is naive to lay blame on users and whine, 'The system I designed would be secure, if only users were less gullible.' The wise security designer seeking a robust solution will acknowledge the existence of

these vulnerabilities as an unavoidable consequence of human nature and actively build safeguards that prevent their exploitation."[16]

As cybercriminals develop and refine their techniques, a greater proportion of the population will likely be susceptible to mass-marketing fraud. Research to date has provided some detail as to the anatomy of these scams and the techniques criminals use to persuade victims to part with their money. New methods of tracing criminals are needed, as is cooperation across international boundaries. Among the technical solutions advocated by Stajano and Wilson is that computer scientists should develop programs to help law enforcement trace criminals online (akin to technologies developed to trace pedophiles) or software that detects fake profiles and deceptive communication and alerts users in real time.16 In addition, new methods are needed to help prevent victims from sending money. In Germany, for instance, automatic detection techniques and bank and post office staff training has dramatically reduced the number of successful 419 attacks. Many of these scams require mules to monetize the proceeds of attacks, so detection and increasing awareness of typical mule recruitment techniques might be fruitful. Moreover, because an increasing number of scams are conducted via mixed channels—online and telephone—and involve impersonation of bank or law enforcement staff, we urgently need reliable ways to signal users when they are talking to a legitimate person, rather than an imposter.

References

1. "Mass-Marketing Fraud: A Threat Assessment," Int'l Mass-Marketing Fraud Working Group, 2010; www.ice.gov/doclib/cornerstone/pdf/immfta.pdf.

2. M.T. Whitty, Mass-Marketing Fraud in the UK, report, 2013.

3. "2014 Internet Crime Report," ann. report, Internet Crime Complaint Center, 2014.

4. "Targeting Scams: Report of the ACCC on Scam Activity 2012," Australian

Competition & Consumer Commission, 2013; www.accc.gov.au/system/files/Targeting %20scams%202012.pdf.

5. D. Florencio and C. Herley, "Sex, Lies and Cyber-Crime Surveys," Economics of Information Security and Privacy III, B. Schneier, ed., Springer, 2013, pp. 35–53.

6. R. Anderson et al., "Measuring the Cost of Cybercrime," Economics of Information Security and Privacy, R. Böhme, ed., Springer, 2013, pp. 265–300.

7. M.T. Whitty and T. Buchanan, "The Online Dating Romance Scam: The Psychological Impact on Victims— Both Financial and Non-financial," to be published in Criminology Criminal Justice, Sage Publications, 2015.

8. M. Button, C. Lewis, and J. Tapley, "Not a Victimless Crime: The Impact of Fraud on Individual Victims and Their Families," Security J., vol. 27, no. 1, 2014, pp. 36–54.

9. M.T. Whitty, "The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam," British J. Criminology, vol. 53, no. 4, 2013, pp. 665–684.

10. "Helping People Affected by Scams: A Toolkit for Practitioners," Office of Fair Trading, 2010.

11. M.T. Whitty and T. Buchanan, "The Psychology of the Online Dating Romance Scam Report," Univ. of Leicester, 2012; www2.le.ac.uk /departments/media/people /monica-whitty/Whitty_romance _scam_report.pdf.

12. J. Lee and H. Soberon-Ferrer, "Consumer Vulnerability to Fraud: Influencing Factors," J. Consumer Affairs, vol. 31, no. 1, 2005, pp. 70–89.

13. S. Furnell, "Internet Threats to End- Users: Hunting Easy Prey," Network Security, vol. 2005, no. 7, 2005, pp. 5–9.

14. K. Holtfreter, M.D. Reisig, and T.C. Pratt, "Low Self-Control, Routine Activities and Fraud Victimization," Criminology, vol. 46, no. 1, 2008, pp. 189–220.

15. "Provoking and Committing Errors of Judgment," Office of Fair Trading, 2009; http://fraudresearchcenter .org/2012/03/the-psychology-of -scams-provoking-and-committing -errors-of-judgment.

16. F. Stajano and P. Wilson, "Understanding Scam Victims: Seven Principles for Systems Security," Comm. ACM, vol. 54, no. 3, 2011, pp. 70–75.

17. J.B. Walther, "Computer-Mediated Communication: Impersonal, Interpersonal and Hyperpersonal Interaction," Comm. Research, vol. 23, no. 1, 1996, pp. 3–43.

18. M.T. Whitty. "True Romance?," PoliceProfessional.com, 19 July 2012; www.policeprofessional.com /news.aspx?id=14829.