Mass-marketing fraud: A growing concern

Monica T. Whitty

University of Leicester

IEEE Security & Privacy


http://www.computer.org/csdl/mags/sp/2015/04/index.html

End-users have more concerns than ever when it comes to cyber security. A growing international concern is mass-marketing fraud. In 2010 The ‘International Mass-Marketing Fraud Working Group’ (2010) reported that this crime had gradually transformed from a predominantly North American crime problem into a pervasive global criminal threat. In the UK approximately 2.6 million adults have fallen to these scams, with approximately 500,000 adults having fallen victim to a dating/romance scam, around 900,000 had been conned by a boiler room scam, 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 became a victim of mass-marketing fraud. Of further concern is the number of repeat victims of this crime, with almost a quarter of those scammed being scammed at least on one more occasion (Whitty, 2013a). The victims reported in Whitty’s representative samples are much closer to the ‘real’ number of victims in the UK. Reporting bodies in the UK, such as Action Fraud, estimate that less than 10% of the population report this types of crime – partly because of: the shame and embarrassment associated with becoming a victim; lack of knowledge of where/how to report; and because they are aware that it is unlikely that police will attempt to locate the criminal. In 2014 IC3, in
the USA, reported that 123,684 victims complained about financial losses to Internet crime, many of which were victims of mass-marketing fraud. The most common complaints they received included: auto fraud, government impersonation, intimidation/extortion, real estate, and confidence/romance scams. They estimate that only 10% of victims report the crime to the centre (IC3, 2014). In Australia in 2012 just over $94million (AUS) was reported as a loss to victims of mass-marketing fraud (ACCC, 2013).

Researchers, however, have yet to accurately measure the amount lost to individuals and as Florencio and Herley (2013) point out, we need to take results obtained about losses obtained from survey research given that outliers can distort the results. They provide the following examples: “A single individual who claims $50,000 loses, in an N= 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.” (p. 35). Anderson et al. (2012) argue that our response to cybercrime is so disproportionate that we overspend protecting against it. They note that: “As far as direct costs are concerned, we find 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, the indirect costs and defence 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. As a striking example, the botnet behind a third of the spam sent in 2010 earned its owners around US $2.7m, while worldwide expenditures on spam prevention probably exceeded a billion dollars. We are extremely inefficient at fighting cybercrime; or to put it another way, cyber-crooks are like terrorists or metal
thieves in that their activities impose disproportionate costs on society” (p.266). These points are important to consider when considering the costs of cybercrime; however, in addition to the financial losses, as this paper illustrates, it is critical that we consider the psychological costs to the well-being of an individual as well as the family and friends who are often impacted on by mass-marketing fraud (see, for example, Whitty & Buchanan, in press).

Fraud broadly can be defined as trickery used to gain a dishonest advantage, which is often financial, over another person or organisation. Mass-marketing fraud is a type of fraud that exploits mass communication techniques (e.g., email, Instant Messenger, bulk mailing, social networking sites) to con people out of money. The Internet has opened up 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 organised, crime. Examples include: foreign lotteries and sweepstakes (in which the person believes they have won money from a lottery and are told to pay a fee in order to release the funds), “419” scams (advance fee fraud, in which victims believe that for a small amount of money they will make a large fortune), and romance scams (taken in by a fake online dating persona, in which the victim sends the ‘fake persona’ money).

**Psychological impact**

There are both financial and psychological costs to victims of this crime. In fact, psychological effects can sometimes outweigh the financial impact, even when large sums of money are lost (Button, Lewis & Tapley, 2014; Whitty, 2013b). The Office of Fair Trading (2010) have 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” (p. 4). Psychological harm can include: shame, guilt, embarrassment, depression, feeling suicidal, grief, anxiety, and loss of trust (Whitty & Buchanan, 2012).

Unlike most other crimes, victims of mass-marketing fraud are often blamed for their victimisation. Family and friends, who are typically an important source of support for victims of crime, often blame victims – pointing out how they too have been affected (e.g., losing their inheritance). Victims are often viewed by society and depicted in the media as stupid or naïve – neither of which appears to be the case. This makes recovery from this crime even more difficult; especially given that it is highly unlikely that victims will ever have their funds recovered. Furthermore, preliminary findings suggest that after-care for victims needs to be long-term – which is another support often unavailable to victims given that they are unable to afford long-term counselling (Button et al., 2014; Whitty & Buchanan, 2012). Websites and online support groups have emerged where victims support other victims, although the effectiveness of this type of support is yet to be empirically tested (e.g., 


Vulnerability and persuasive techniques

Research that has considered the types of people who are most likely to be taken in by scams has mostly focused on ‘get rich quick scams’ (e.g., Lee & Soberon-Ferrer, 2005). Nonetheless, these studies provide some important insights into the sorts of individuals who are more vulnerable to mass-marketing fraud. Furnell (2005) argued that greedy and naive individuals are more likely to be conned. Lee and Soberon-Ferrer found that victims of fraud tend to be older, poorer, less educated and single. Holtfreter, Reisig and Pratt (2008) looked broadly at ‘consumer fraud’ victimisation
and found that fraud victims were more likely to have low self-control. In contrast, it has been found that those high in sensation seeking are not more likely to be scammed by the online dating romance scam; rather, high scores on the romantic belief subscale, ‘idealization’ is more associated with the likelihood of being a victim (Whitty & Buchanan, 2012, Buchanan & Whitty, 2014).

In explaining the success of mass-marketing fraud, scholars mostly draw from theories developed by social psychologists and adapt these to scams. Lea, Fischer and Evan (2009) offer the most comprehensive approach to explaining the psychology of scams. They argue that “falling for a scam comes down to errors in decision-making”, and “scammers create situations (with their scam offers) that increase the likelihood of poor decision-making” (p. 35). Lea et al. found that there were both cognitive (e.g., overconfidence in a specific topic) and motivational (e.g., the scam triggers positive emotions) processes to explain the psychological reasons for responding to scams. They found that the most consistent finding across their studies with regards to reasons why people are scammed included: ‘appeals to trust and authority’ (i.e., 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).

Although authority and visceral cues were the clearest findings in Lea et al.’s studies as a way of explaining why victims are drawn into scams, there are other persuasive techniques worthwhile considering. Scarcity has also been found to play a role; that is, presenting offers that have time limits (Whitty, 2013b). Classic marketing strategies such as the foot-in-the-door technique (i.e., 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 (i.e., asking for large amounts of money and
gradually decreasing the amount until the person is willing to comply) have also been found to be effective techniques (Whitty, 2013b). Stanjano & Wilson (2011) analysed face-to-face cons and found that attackers use a limited number of techniques to manipulate their victims.

In addition to considerations of classic persuasive techniques, I would argue that it is equally important to focus on the role the Internet might play in persuading individuals to part with their money. In the past, researchers have found that individuals develop very trusting, intimate relationships online (e.g., Walther, 1996). Given this, we might postulate that the Internet is the ideal place for criminals to target strangers in order to earn their trust. In my own work I have found that one-sided, ‘hyper-personal’ relationships develop between the victim and the scammer (Whitty, 2013b). Victims idealise the ‘fake persona’, believing they have found the perfect romantic partner. Given that much of the communication is asynchronous, criminals have time to write and consider the perfect response and develop the ideal person – making it easier to trick the victim into falling in love with them. Walther (1996) also found that when people are communicating via the Internet become much more focused on the online communications, blocking out other environments. In my own work, I have found victims of the romance scam report continuously re-reading emails and looking forward to the next romance email or IM chat session. Online a record is kept for individuals to revisit whenever they want – reinforcing the romantic messages being sent by criminals. Therefore, in my view, online communication helps strengthen the perceived emotional bond, making it difficult for victims to break away from the relationship. Although I have found this with the romance scam, this could potentially be found in other types of scams where the criminal spends time communicating with the victim prior to asking them for any money.
A Stage Theory Approach

Considering scams as a series of stages might also provide a useful method to gain greater insights into the anatomy of these scams. Again, in my work on the romance scam I have outlined a number of stages involved in this scam, which could potentially be applied to other types of mass-marketing frauds. The stages are as follows: Stage 1: potential victims need to be motivated to find the ‘ideal partner’; Stage 2: potential victims are presented with an ideal profile and the relationship is given the promise of exclusivity by the scammer; Stage 3: potential victims are groomed by the criminal to gain trust and love and the criminal test the waters to gauge whether the potential victim might be ready and willing to part with their money; Stage 4: the criminal employs techniques to persuade the potential victim to send money (e.g., a narrative about a crisis where money is urgently needed or the ‘foot-in-the-door’ technique described above); Stage 5: the criminal employs further techniques to keep the scam alive (e.g., inventing further crisis; employing the ‘door-in-the-face technique); Stage 6: might occur for some victims, where they believe the scam is over and are subsequently re-victimised (e.g., criminal admits to them scamming the victim, but nonetheless fell in love with them – and then asks the victim for more money; the victim receives an email from the criminal, pretending to be law enforcement, asking for a small amount of funds for them to release the money over to the victim) (Whitty 2013b).

Prevention

Preventing mass-marketing fraud is a difficult task. Catching and prosecuting attackers is challenging given that: (1) the criminals often live in a different country
to the victims, (2) the methods the criminals use make them difficult to trace, and (3) prosecution is very time consuming, owing to the large amounts of online data that need to be analysed to establish evidence against the criminals and gain intelligence about their whereabouts and operating tactics. Given the difficulties involved in catching criminals, other methods are also needed in order to help prevent this crime.

Law enforcement and others have attempted to prevent the crime by using disruption tactics. Dating sites, for instance, have been encouraged to share known fake profiles in order to help reduce the amount of criminal profiles on their sites. Law enforcement have 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 (this would make it easier to catch criminals and, in consequence, deter criminals). Moreover, these transfer countries have been encouraged to enter Suspicious Activity Reports for any transaction that appears to have been conducted with a scammer. However, even if such a strategies were successful, criminals could potentially find a way around this (e.g., another means of transferring money is to persuade victims to, unknowingly, transfer money into other victims accounts, making the money more difficult to trace back to the criminal as well as involving the victim, typically unknowingly, in money laundering).

Unfortunately awareness of mass-marketing fraud does not necessarily prevent individuals from becoming victims. Researchers have found that many victims that fall for mass-marketing frauds have heard of these scams, some having detailed knowledge (Lea et al., 2009; Whitty & Buchanan, 2012b). Lea et al., (2009) argue that detailed knowledge of a scam can, in fact, increases vulnerability as these individuals often develop an ‘illusion of invulnerability’. Moreover, once a victim is hooked into a scam, it is very difficult to draw them out of the scam, making them
believe it was a hoax. In my own work I have found that even when authority figures (e.g., police, law enforcement, bank managers) attempt to alert a person to that fact (knowledge garnered from intelligence) that they have become a victim of a romance scam, the victim often has difficulties believing this person. Moreover, when the victim questions the criminal about his/her authenticity the criminal will employ persuasive techniques to convince the victim (Whitty, 2012). Given that knowledge about a scam, therefore, may not be enough to prevent individuals from becoming defrauded other types of interventions are also needed. Stajano & Wilson (2011) also argued that – given that attackers consistently use a small number of well-established tricks – system designers could to more to prevent exploitation. “Our message for the system-security architect is that it is naïve 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.”

Conclusions
As cyber-criminals refine and develop their techniques it is likely that a greater proportion of the population will be susceptible to mass-marketing fraud. Research to date has provided some detail as to the anatomy of these scams and the techniques employed by criminals to persuade victims to part with their money. New methods need to be developed to trace criminals and co-operation is needed across international boundaries (given that often the victim and the criminal reside in different countries). Among the technical solutions advocated by Stajano & Wilson (2011), computer scientists could develop programmes to assist law enforcement in
tracing criminals online (akin to technologies developed to trace paedophiles), or develop software that detects fake profiles and deceptive communication and alerts the user in real time when they are communicating with a known fraudster. In addition, new methods are needed to help prevent victims from sending money – in Germany, for instance, a combination of automatic detection techniques and training of bank and Post Office counter staff have dramatically reduced the number of successful 419 attacks. Many of the scams require mules to monetize the proceeds of attacks, so detection and increasing awareness of typical mule recruitment techniques can be fruitful. Moreover, since an increasing number of scams are conducted over a mixture of channels – for instance online and phone – and involve impersonation of bank or law enforcement staff, we urgently need to develop solutions that provide reliable signals to users that they talking to a legitimate, rather than an imposter.

References


Office of Fair Trading, Helping people affected by scams: A toolkit for practitioners. 2010 Retrieved from:


http://www.policeprofessional.co.uk/


http://www2.le.ac.uk/departments/media/people/monica-whitty/Whitty_romance_scam_report.pdf