ABSTRACT

Mass-marketing frauds (MMFs) are on the increase. Given the amount of monies lost and the psychological impact of MMFs there is an urgent need to develop new and effective methods to prevent more of these crimes. This paper reports the early planning of automated methods our interdisciplinary team are developing to prevent and detect MMF. Importantly, the paper presents the ethical and social constraints involved in such a model and suggests concerns others might also consider when developing automated systems.

Keywords

ACM proceedings, mass-marketing fraud, online scams, cybercrime, cybersafety

1. INTRODUCTION

Mass-marketing fraud (MMF) is a serious, complex, and organized crime. Examples include: foreign lotteries and sweepstakes (in which the victim 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) [10, 11]. Some MMFs are low-value one off scams on large numbers of victims, whilst others involve developing a relationship (e.g., romantic, business, friendship) where money is defrauded over time, again with multiple simultaneous or sequential victims.

Victims of MMF suffer both financial losses and psychological impacts, with psychological effects sometimes outweighing the financial impact, even when large sums of money are lost [12]. Psychological harm can include: shame, guilt, embarrassment, depression, feeling suicidal, grief, anxiety, and loss of trust. Catching and prosecuting MMF criminals is a difficult task. This is for three main reasons: (1) the criminals often live in a different country to the victims, (2) the methods the criminals use that 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.

Law enforcement and others have attempted to prevent the crime by using disruption tactics. Dating sites, for instance, have been asked to share known fake profiles in order to help reduce the number of criminal profiles. Facebook has attempted to take down known fake profiles. Anti-Money Laundering regulations increase the identifiability of transactions and recipients when money is transferred via money transfer companies, such as Western Union and MoneyGram.

There are also numerous guidelines, campaigns, websites, and phone apps available that attempt to educate users about scams in an attempt to prevent victimisation aris-
We also point out how these concerns might relate to the concerns related to the autonomous agent we are developing. The research being undertaken in our project: ‘DAPM: Detecting and Preventing Mass-Marketing Fraud’ is drawing from psychology, media and communications, criminology and linguistics to help identify deception and persuasive communication and evidence of grooming often evident in MMFs. We are also interested in identifying: the online identities, other communication and online behaviors typical of scammers as well as victims. We are also examining whether the psychological characteristics that are more typical of victims (e.g., romantic beliefs, impulsivity) [1] might be detected in victims’ online communications.

We are also examining socio-technical features to identify MMF. In particular, we are building on Huang et al.’s work [4] to investigate characteristics of scammer profiles, such as the utilization of same profile photographs, descriptions across multiple profiles and patterns of interaction and contact with other users (e.g., login times). We are also examining socio-technical characteristics typical of users, such as replying to any message they receive or immediately giving away their phone number. We will utilize supervised machine learning techniques such as random forests and clustering of profiles to this end.

In addition to identifying technical features we hope to uncover specific linguistic features: typical of a victim; indicative of scammers’ communication; and indicative of the interactions that take place between victims and scammers. For example, previous work has found that victims of romance scam are more likely to hold ‘idealized’ romantic beliefs – that is, believing that they can find a relationship with someone who will be their ‘true’ love and this person will be nearly perfect [1]. We might hypothesize, therefore, that someone who is more susceptible to the romance scam will write a profile specifying they are seeking out the perfect partner. We might also hypothesize that scammers will create profiles in a similar way and will communication em-
phrasing how ‘perfect’ they perceive the victim and that they believe that the victim is their ‘true love’.

We also hope to uncover deceptive communication. For example, previous work has found that liars tend to use more words, and these words are more informal and expressive, compared with people telling the truth. They also make more typographic errors [13]. It has also been found that word count is significantly higher in deceptive communication on Instant Messaging compared with when people speak the trust. Moreover, individuals who were lying were more likely to ask questions that they who were being honest [3]. Linguistic indicators of deception, therefore, might help us to automatically detect mass-marketing fraudsters.

Cultural indicators might also be useful for our agent. Given that it is believed that many scammers are West Africans, there may be some benefits into detecting West African communication in our model.

3. PERSONAL DATA USED FOR IDENTIFICATION

In the research for this project we will be drawing on personal data for our analysis. For example, we will be conducting analysis of profiles from dating sites, employment webpages and so forth. We will be conducting analysis of text produced by both the victim and the criminal. We might also wish to compare communication with the victim and non-criminals to examine any significant difference in stylistic features of this communication. Some of this text, we foresee, will be highly personal communication. In all instances, we will be able to anonymize the data – beyond simply taking out ‘real names’ (e.g., we will anonymize any occupational roles leak out identity information). Much of this anonymization we will conduct automatically rather than manually.

The research will, of course, strictly follow ethical guidelines set out by the British Psychological Society and the UK Research Councils – and so we don’t foresee any specific ethical concerns regarding the research. Participants will be giving informed consent and can withdraw from the research without penalty. Participants’ confidentiality will be respected and their personal data will be stored securely.

Given we are conducting our research following ethical guidelines and principles we are not concerned with the ethics or moral issues regarding our research practice. The ethics and social challenges, however, which do concern us, are in the next stages of the project – which will be undertaken should we reveal effective identification of scammers in our research studies.

4. DEVELOPING A SYSTEM TO AUTOMATICALLY DETECT AND WARN POTENTIAL VICTIMS OF MMF

In addition to the identification platform, should our research successfully detect fraudsters, we intend to develop a proof of concept application to warn users about scam accounts. This application will be composed of a web browser extension to be installed on user computers. In addition, the tool will collect information about the accounts that our backend will detect belong to scammers.

In brief, the system would need to analyze personal data on the end-user’s machine (e.g., online profiles, emails, Instant Messaging, etc.). This could possibly be all data created and sent to their personal computers or there might be a reason to bracket some of these data. In addition to analyzing the data to make decisions about the probability that the user is communicating with a fraudster the system would need to feedback this information to the user – and would need to do so in a convincing and persuasive manner (especially given that victims often do not believe others, including those in authority positions, such as the police, when they are informed that they have been scammed [10].) We will be drawing from expertise in HCI to develop different types of warning messages and test their effectiveness (e.g., visually wording of the messages) [9, 8]. We would therefore need to build a system that end-users might trust and that could win the trust over from criminal to the autonomous system.

5. ETHICAL AND SOCIAL CHALLENGES WITH OUR AUTOMATED SYSTEM

The benefits of an automatic detection system are obvious. Should it be able to detect end-users’ communication with scammers, it has the potential to prevent victims from sending money, downloading harmful malware on their computers used later for identity fraud; prevent victims from forming intimate relationships with a criminal – only later to be traumatized by the end of the relationship; prevent victims from creating compromising material (e.g., naked photographs, cybersex videos) that might be used at a later date as blackmail.

Despite these benefits, there are nonetheless ethical and social challenges associated with such a system. The proposed detection system would need to be making decisions regarding ‘genuine’ people compared with ‘fraudsters’. There is, of course, the possibility of false positives. False positives with such an agent have different ramifications compared with an email that is mistakenly filtered out into the junk box. Imagine the hypothetical scenario described below:

The end user might be seeking out a partner on a dating site and the person they are communicating with (referred to as unknown) might be a good match, with genuine similar interests and outlook in life. The unknown exaggerates their attributes (slightly more than users would normally exaggerate). They are also somewhat socially clumsy and are rarely given attention and so flatter the end-user in an exaggerated manner, more akin to a scammer. The end-user is also a General in the American Army. Given this combination of factors, the system warns the end-user communicating that the unknown is most likely a scammer and so the end-user decides to end the relationship. In this scenario both parties have found dating difficult and rarely opportunities present themselves to each person. Moreover, the unknown was unaware that their data had been analyzed by an automated detection system and warned the end-user that they could be communicating with a criminal.

In the above scenario we are left with the difficult choice of wanting to protect the end-user from potential harm, at
6. CONCLUSIONS

In summary, software programs are becoming a part of our everyday lives, with systems built to automate e-commerce, medical decisions and vehicles. Despite the popularity of these systems and the advancement of science to create these systems, there remains the concern as to how to create ethical autonomous systems – or how to implement such systems in an ethical manner. It has been argued that software engineers often “do not cater for the ‘messiness’ of social life and social research and its continuous impact on design choices” (p.523) [7]. Different ethical, social and psychological concerns might be related to different types of automated programs. Previous work, for example, has raised concerns with drones lowering the thresholds to fire when in warfare. This paper, we believe raises an important concern about needing to balance the need to help and support individuals, whilst still allowing the end user the opportunities they would have otherwise had in their lives. Moreover, like other research on automated programs it raises the concern of privacy. The work we present here will guide our own research as we develop our autonomous agent to prevent MMF and we hope will be considered and guide future development of autonomous agents.

Acknowledgements

The work reported in this paper is supported by award EP/K028112/1 ‘DAPM: Detecting and Preventing Mass-Marketing Fraud (MMF)’, from the UK Engineering and Physical Sciences Research Council.

7. REFERENCES


