Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing

The Case for a Consistent Cyberscam Classification Framework (CCCF)

Amber Stabek, Simon Brown, Paul A. Watters
Internet Commerce Security Laboratory (ICSL)
University of Ballarat
{a.stabek, s.brown, p.watters}@icsl.ballarat.edu.au

Abstract

Cyberscam classification schemes developed by international statistical reporting bodies, including the Bureau of Statistics (Australia), the Internet Crime Complaint Center (US), and the Environics Research Group (Canada), are diverse and largely incompatible. This makes comparisons of cyberscam incidence across jurisdictions very difficult. This paper argues that the critical first step towards the development of an inter-jurisdictional and global approach to identify and intercept cyberscams - and prosecute scammers - is a uniform classification system.

1. Introduction

Cyberscams operate in a continuum of change, and are extremely innovative. They have become endemic in society, damaging victim's lives and have the potential of reducing consumer confidence in internet commerce. Scams have had a significant impact on the Australian economy , costing an estimated $980 million during 2007 alone [2]. Cyberscams are a subset of technology-enabled crime, as defined by the Australian Institute of Criminology [3], which may be prosecuted at the Federal level, pursuant to the reforms made by the Cybercrime Act 2001 [11].

Cyberscams are internet assisted scams , and are considered a form of Financial Fraud as detailed by The Australasian Legal Information Institute [10]. The criminal community has been quick to realise the efficiency and effectiveness dividend of operating online. Through the internet, criminal agendas can be far-reaching, crossing borders and legal jurisdictions. A cyberscammer can operate in multiple countries on multiple victims in parallel. A single person or a unit of individuals can realise a large remuneration for the smallest possible investment of time and effort, even where such a syndicate might be loosely-coupled and geographically distributed.

Whilst there are a constellation of classification schemes available, a consistent classification framework is seemingly non-existent. Some themes seem to be agreed upon throughout current literature.

The problem can be demonstrated in the following way: the "Nigerian Letter Scam", "West African Fraud", "419 Scam", and "Advance Fee Fraud" all refer to the same type of scam, which involves an unsolicited email detailing a dramatic story and promise of good fortune, after a transfer of funds into a scammer's bank account. "The Nigerian Letter Scam", and "West African Fraud", are the different titles given to such a scam by State and Federal Authorities[1]. The "419 Scam" label refers to the article number of the Nigerian Criminal Code which accounts for these types of crimes, and is the term used by the State and Federal Governments[2]. "Advance Fee Fraud" is the umbrella term given for all fraud which requires the victim to pay a fee in advance, and is often used to describe various other forms of scams[3]. This profusion of names for the same underlying technique can lead to confusion, reducing the effectiveness of consumer education.

The monetary loss attributable to cyberscams throughout the United States has increased by $221.29 million since the first iC[3] Internet Crime Report was released in 2001 [7]. To coordinate[1] between industry, law enforcement, financial institutions, and government in a cohesive and operational manner on the issue of cyberscams, well-defined classifications need to be available. The importance of developing consistent and detailed cyberscam classifications for legislative implementation is described by the Parliamentary Joint Committee on the Australian Crime Commission

1 Queensland Police Service, West Australian Police Service, Victorian Police Service, New South Wales Police Force, Northern Territory Police Service, South Australian Police Department, Tasmanian Police Department, and Australian Federal Police

2 www.scamwatch.com.au
www.docep.wa.gov.au/ConsumerProtection/scamnet/default.html

3 Queensland Police Service, Australian Institute of Criminology, Australian Bureau of Statistics, and WA ScamNet

978-0-7695-3737-5/09 $25.00 © 2009 IEEE
DOI 10.1109/UIC-ATC.2009.77

Cybercrime Report [9], Recommendation 3 - the aim is to "ensure that priority is given to the development and implementation of consistent offence and evidence legislation in relation to cybercrime." Unfortunately, the geographically diverse nature of the technology allows all criminal groups to experiment in different jurisdictions and shift rapidly among them, which makes consistent description and enforcement difficult [3].

The purpose of this paper is to highlight the current inconsistencies in cyberscam classification. A pathway to a new consistent system of cyberscam classification is outlined – such a scheme is required if success in fighting this crime type is to be achieved. The first step towards inter-jurisdictional and global approaches to fight cyberscammers is to develop a uniform classification system with which to identify and intercept cyberscams and prosecute cyberscammers.

2. Analysis of Classification Schemes

In this section, we review the classification schemes from several international bodies to demonstrate the variance and potential incompatibility of cyberscam classifications and definitions.

2.1 The Australian Institute of Criminology

During 2007, the Australian Institute of Criminology (AIC) released a report titled "Future Directions in Technology-Enabled Crime" [3]. This was the result of a comprehensive collaboration between the AIC and the Australian High Tech Crime Centre (AHTCC) of the Australian Federal Police (AFP). The report was designed to increase awareness of technology-enabled crime and forecast the path that such crimes might take over the period from 2007 to 2009.

'Technology-Enabled Crime' (TEC) is the term used by the AFP to refer to all crimes that are perpetrated by the use of information and communication technologies. This includes Computer Facilitated Fraud, such as Advance Fee Scams, Online Auction Fraud, Fraudulent Lottery Schemes, Modem and Webpage Hijacking and Identity Theft [3]. These crimes know neither borders nor jurisdictions, since a criminal perpetrating TEC can generally operate across legal borders. Choo et al. [3] began by drawing attention to the lack of uniformity in classification of TEC. While acknowledging that current ambiguous classifications are discipline dependant, it is implied that uniform legislation in fighting such criminal acts will be aided by a universal classification system for all TEC.

As we operate within an era where communication is instant and global connections are continuously maintained, criminals are embracing the opportunities that the digital age offers. By expanding the scope of their traditional operations, criminal individuals and groups have access to an international audience while enjoying the sanctity of pseudo-anonymity [3]. Since computer attackers perceive TEC to offer high margin with relatively low risk, some have suggested that TEC is an attractive and low risk addition to current criminal organisations [3].

As it is possible for TEC to be globally facilitated, giving cyber criminals the ability to "test" jurisdictions [3], law enforcement agencies must work collaboratively to effectively identify and intercept cyberscams, and prosecute these criminals. Current TEC task forces around the globe would benefit from a heightened collaborative methodology and shared pedagogy [5]. The necessity for collaboration and cooperation is supported by the Parliamentary Joint Committee on the Australian Crime Commission Recommendations 6, 7, 9, and 10 [9]. Further, the Australasian Centre for Policing Research Report [1] focuses on collaborative planning to bring consistency and standardisation to defining these crimes.

Choo et al. [3] insist that TEC values the use of tested and effective business models. Criminal individuals and groups are notable for their rapid adoption of innovative working business models. Since technology has become a key enabler for these criminal acts, and technology is continuously evolving, criminal individuals and organisations can derive direct benefits from being agile and adaptive to change. Online auction scams are an example of criminals operating their 'businesses' by exploiting a very successful business model used by online auction sites.

The divide that exists between technology-enabled criminals and current legislation is highlighted by Choo et al. [3] in their observation that criminal individuals and groups are flourishing from the free trade principles and transmutability that technology offers, while law enforcement bodies are hindered by geographical, legal and cultural constraints. To enable cohesive collaboration between law enforcement bodies around the globe, legislation and law enforcers must operate under the same free trade principles as those technology-enabled criminals [3], or acquire equal or greater agility. The first step towards global cross-jurisdiction cooperation and collaboration is a comprehensive and uniform classification system for cyberscams [9], which would allow authorities to identify and intercept cyberscams and prosecute

cyberscammers, particularly in collaboration with other law enforcement agencies.

The AIC [3] advise on a range of TEC in the area of cyberscams. Computer-Facilitated Frauds are made up of Advance-Fee Scams, Online Auction Frauds, Fraudulent Lottery Schemes, Modem and Webpage Hijacking, and Identity Theft which includes Phishing and Click Frauds. Online Auction Frauds include fourteen different types of scam. These are Seller Crimes - Shilling, Bid Shipping, Second Chance Offers, Shell Auction, Misrepresentation, Failure to Ship, Counterfeits / Pirated Software, Sale of non-Existent Merchandise, Fee Stacking, and Triangulation / Fencing, and Bidder Crimes – Bid Shielding, Failure to Pay, Buy and Switch, and False-Name Bids.

2.2 The Australian Bureau of Statistics and The MCLOC of SCAG

The Australian Bureau of Statistics (ABS) Personal Fraud Survey of 2007 [2] reports on Australian residents' exposure to fraud and cyberscams. The first of its kind in Australia, the Personal Fraud Survey was an addition to the Multi-Purpose Household Survey and contained a sample of 14,320 participants who agreed to be interviewed by phone. The report identified some scams and frauds as forms of Personal Fraud. No operational definition of Personal Fraud was supplied in the publication. The identified forms of Personal Fraud were [2]:

- Identity Fraud
  - Identity Theft
  - Credit / Debit Card Fraud
- Scams
  - Lotteries
  - Pyramid Schemes
  - Phishing and Related Scams
  - Financial Advice
  - Chain Letters
  - Advance Fee Fraud

The survey did not clearly link cyberscams to traditional scams, making true representation of this escalating problem impossible. A distinction is made between Scams and Identity Fraud, indicating that the ABS considers these forms of crime to be independent.

A Scam is defined by the report as "...a fraudulent invitation, request, notification or offer, designed to obtain someone's personal information or money or otherwise obtain financial benefit by deceptive means" ([2], p.5).

Identity Fraud is defined as "…the theft of a pre-existing identity without a person's consent, where the person's name[s], date of birth, address or other personal details are used to engage in fraudulent activities" ([2], p.5). This definition implies that Identity Fraud is considered to be one consequence of Identity Theft.

Identity Theft is defined as "the theft and fraudulent use of personal details or documents such as a driver's licence, tax file number or passport to conduct unauthorised transactions…or otherwise using a person's identity without permission" ([2], p5).

These definitions suggest that if a person had been a victim of Identity Fraud, they first must have been a victim of Identity Theft, where a scam may have been used as the method of obtaining targeted personal information. These definitions are in direct contrast to the 'Experience of Personal Frauds' chart which was published by the ABS [2]. The chart indicates that Identity Theft is viewed as a form of Identity Fraud. Based on this chart, if a person's identity is stolen, they are a victim of Identity Theft, while if a person's credit or bank card details are used without their consent; they are a victim of Credit / Bank Card Fraud.

Individuality and sense of self are what constitute 'Identity' [8], and three forms of information may be sought which represent Identity Theft. These may be physical (photographs, iris scans, fingerprints, voice prints), Government identifiers (drivers' license, passport), and financial information (bank account, credit card, employment information) ([8] p.3). Since the theft of financial information represents Identity Theft, a victim of Credit / Debit Card Fraud is a victim primarily of Identity Theft, before they become a Victim of Identity Fraud. The chart used by the ABS [2] suggests that a victim of Identity Theft or Credit / Debit Card Fraud is seen to be a victim of Identity Fraud. This contradicts the definitions given in the Final Report Identity Crime by the Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General [8]. If a person's identity is stolen, the stolen identity may not be used in fraudulent acts directly, or at all. Therefore, Identity Fraud does not result in Identity Theft, but Identity Theft may result in Identity Fraud and Identity Theft cannot always imply Identity Fraud.

Identity Fraud is defined by the Model Criminal Law Officers' Committee as "the gaining of money, goods, services or other benefits…through the use of a fabricated identity, a manipulated identity or a stolen / assumed identity" ([8], p.13). Identity Theft is defined as "the theft or assumption of a pre-existing identity…with or without consent" ([8], p.13). Based on these definitions, Identity Theft must occur before

Identity Fraud can be committed with regard to the use and / or assumption of a victim's personal details. If such details are deceptively gained through the use of cyberscamming, the theft of an identity has occurred. Once Identity Theft has been successful, a cyberscammer can sell the stolen identity onto a third party or use the identity to commit other crimes such as Identity Fraud and Debit / Credit Card Fraud. Identity Fraud and Credit / Debit Card Fraud are Identity Related Crimes and are resultant to Identity Theft Crimes. Since Identity Fraud involves the theft and use of personal details, a cyberscam may be seen as one of the primary mechanisms used by technology-enabled criminals to gain access to targeted information.

Scams are a method of tricking a potential victim into providing a criminal with access to something of value. Perceived value functions may be financial gain, personal information, or participation.

Financial gain may be the primary purpose driving a cyberscammer, which can be seen with scams requiring the potential victim to pay a fee in advance to collect a non-existent prize or paying for tickets to an event which is deceptively represented online. (One recent example of this is the 2008 Beijing Olympics Ticketing Scam).

Personal information involves gaining access to selected personal details. Phishing is an example of one method that cyberscammers use to facilitate their scams and gain access to targeted information. The scams focused around gaining access to personal information often lead to other crimes against the individual, such as Identity Theft and Identity Fraud.

Participation refers to scams which act as a cover for more elaborate schemes. Cyberscams - with the main goal of recruiting potential participants for other criminal activities such as laundering of goods or money (money mules) - require the potential victim to participate in these activities. Work from home scams can evolve into laundering schemes, and are an example of the participation-focused cyberscam.

Phishing and spoofing are popular methods used by cybercriminals to scam potential victims and gain access to their personal information. Since phishing and spoofing are mechanisms for the facilitation of cyberscams, they should not be regarded as cyberscams, rather the method by which some cyberscams may be actuated. The difficulties encountered with the definitions used by the ABS [2] are explained in part by the authors' admission that for this report, victims of identity fraud "...were not required to be exposed to a scam" ([2], p.27) since the report "was not designed to capture the level of complexity" ([2], p.37) that represents the current operational processes of cyberscams and technology-enabled crimes. This single-dimensional view of these definitions and resultant statistics raises concerns about the broader applicability of the information presented in the ABS Personal Fraud Survey of 2007 [2].

2.3 The Internet Crime Complaint Center

The 2007 Internet Crime Complaint Center (iC^3) Internet Crime Report [6] represents a collaboration between the National White Collar Crime Center, Bureau of Justice Assistance and the Federal Bureau of Investigation, which reports complaints of internet crime, and has been actively involved in reporting in this area since 2001. The iC^3 Internet Crime Report [6] reports on complaints regarding internet crime in nine key areas of cyberscam: Auction Fraud, Non-delivery of Goods, Confidence Fraud, Credit / Debit Card Fraud, Check Fraud, Computer Fraud, Identity Theft, Financial Institution Fraud, and Nigerian Letter Fraud.

The Report shows some discrepancies in its classifications of cyberscams. Identity Theft, Credit / Debit Card Fraud, and Financial Institution Fraud are identified within the report as separate categories of cyberscam and statistics are provided for each: 6.3% of complaints were Credit / Debit Card Fraud related, 2.9% of cases were Identity Theft related, and 2.7% of cases were classified as Financial Institution Fraud ([7], p.5). Financial Institution Fraud is defined as a "knowing misrepresentation of the truth or concealment of a material fact by a person to induce a business, organisation, or other entity that manages money, credit, or capital to perform a fraudulent activity" ([7], p.18).

The separate categorisation suggests independence between the three forms of cyberscam, whose relationship may be logically formalised in the following way. Let U = the universe which is made up of all technology-enabled crime. Let F = Financial Institution Fraud. Let I = Identity Theft. C = Credit / Debit Card Fraud. Let S represent all other forms of cyberscam.

$$U = S + F + I + C$$

Even though statistically reported on as a separate form of cyberscam, Financial Institution Fraud is regarded as the umbrella term for Identity Theft and Credit / Debit Card Fraud throughout the body of the iC^3 report [7] which correlates with the recommendations provided by The Australasian Legal Information Institute [10]. This implies that in the universe of TEC *(U)* there exists a finite set of crimes

known as Financial Institution Fraud *(F)*. Since Identity Theft *(I)* and Credit / Debit Card Fraud *(C)* are considered to be forms of Financial Institution Fraud *(F)*, then *F* is composed of *I* and *C* which exists in *U*.

U = *S* + *F*, where *F* = *I* + *C*

? ? S, *F* ? *U* : *I* ? *C* ? *F where S = all other cyberscams.*

By reporting statistics of Financial Institution Fraud as well as the subsets that exist within the set of Financial Institution Fraud as exclusive and independent events, an incorrect and potentially biased story is told.

Confidence Fraud was responsible for only 6.7% of all reported cyberscams. Confidence Fraud is defined as "the reliance on another's discretion and / or breach in a relationship of trust resulting in financial loss and a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment" ([7], p.18). This generic classification describes all forms of cyberscams, TEC as well as more traditional crimes. All cyberscams involve a knowing misrepresentation of the truth on behalf of the cyberscammer as well as concealment of information which may otherwise deter potential victims from falling prey. The iC^3 report [7] selectively defines Auction Fraud, Non-Delivery of Goods, and the Nigerian Letter Scam under the one umbrella term "Confidence Fraud".

Another type of cyberscam described is Computer Fraud which is defined as "…a violation of law involving a computer." ([7], p.18). Since all cyberscams use computer technology as their key distribution and operational mechanism, all cyberscams fall under this category. Other serious crimes, such as child pornography and online gambling rackets, can also represent Computer Fraud, as defined in this way. Thus, the definition is quite broad, and limited in its application to cyberscams and technology-enabled crimes.

2.4 The Environics Research Group

The 2007 Canadian Consumer Mass Marketing Fraud (CMMF) Survey by the Environics Research Group [4] identified twelve types of Consumer Mass Marketing Fraud and Advance Fee Frauds. The survey targeted citizen awareness and exposure to the following scams [4]: Prize / Lottery and Sweepstakes Fraud, West African / 419 Fraud, Employment / Work From Home Fraud, Cheque Cashing / Money Transfer Job Fraud, Overpayment for Sale of Merchandise Fraud, Advance Fee Loan Fraud, Upfront Fee for Credit Card Fraud Bill for Unsuitable Merchandise Fraud, Bogus Health Product / Cure Fraud, Advance Fee Vacation Fraud, High Pressure Sales Pitch Vacation Fraud, and Investment Fraud.

Consumer Mass Marketing Fraud is defined as "fraud committed via mass communication media using the telephone, mail, and the internet (including deceptive email, but NOT identity theft or so called phishing activities)" ([4], p.i.). Again, like the ABS Personal Fraud Survey [2], there appears to be a lack of connection between traditional crimes and TEC. The authors acknowledge use of an insufficient pool of national data in the area of CMMF. This consensus is transferable across oceans, boarders and jurisdictions.

Included in these classifications of scams are four types of Advance Fee Fraud: West African / 419 Fraud, Advance Fee Loan Fraud, Upfront Fee for Credit Card Fraud, and Advance Fee Vacation Fraud. Two forms of Vacation Fraud are recognized: Advance Fee Vacation Fraud and High Pressure Sales Pitch Vacation Fraud. Advance Fee Vacation Fraud has been included in both categories demonstrating the ease at which a scam can be associated with multiple categories.

The report specified that the focus of CMMF for this survey was Canadian residents. A sample of 3,520 participants was obtained [4]. The statistics suggest that once a person became a victim of a scam, they were recurring targets of such crimes, with a 31% increase in the number of contacts from scammers in a twelve month period (non victims = 16, victims = 21) [4]. This suggests that, in the current climate of increasing and exploitive cyberscams, an intermediary plan for combating these crimes may be required. Increasing the frequency and impact of educational advertising campaigns which highlight the severity of cyberscams in the community may be a practical approach to cultivating awareness. Using sophisticated campaigns which make individuals aware of how they might become a victim to a cyberscam would empower them to make informed choices. Such education may come from a coalition of government and commercial organisations, and must be focused on increasing consumer confidence in internet commerce.

3. Conclusion

In this paper, a significant amount of variation has been found in the way that cyberscams are classified internationally. This variance makes it difficult for sensible transnational comparisons to be made, or co-ordinated operations to be conceived.

To aid in the detection and interception of cyberscams, and prosecution of cyberscammers, a clear

and consistent classification scheme needs to be developed. Such a scheme may be derived "bottom-up", using text mining techniques, or "top-down", based on a business process analysis for each type of cyberscam. A search of similarities and commonalities between scams, based on selected characteristics, would provide an objective basis for classification.

Future work will require the development of detailed process trees for each type of cyberscam, as well as business models identified for each cluster. The statistical clustering, subsequent process tree analysis and formalised business process models will form the basis for a common taxonomy of cyberscams , allowing for accurate, concise and consistent classifications of current and future cyberscams. Cross-over effects may be seen in other areas of technology-enabled crime including more traditional crimetypes .

The primary benefit of a business analysis approach in identifying and classifying cyberscams is a level playing field allowing law enforcement bodies to operate under similar principles, identified as 'free trade principles' by Choo et al. [3], as criminal individuals and groups can. This would aid in the detection, interception and prosecution of cyberscammers.

A purpose-driven classification system for cyberscams could be utilised by industry, law enforcement, financial institutions, and government, as it could be tailored to the desired necessities of the user.

It is clear from the reports cited in this document that the awareness and identification of cyberscams as a national concern, independent from scams in general is in the distant future. The development of a purpose-driven classification system would highlight the possible need for a different strategy to those used currently in tackling cyberscams. This could lead to greater recognition of cyberscams as a national and international priority.

Such a classification system may also act as a stepping stone towards building more fluid channels for collaboration and cooperation between organisations at State, Federal and international levels which is a prerequisite for effectively fighting these crimes.

The establishment of a uniform cyberscam classification system should be seen as a priority for all government, industry and law enforcement bodies.

4. Acknowledgements

This research is funded by the State Government of Victoria, IBM, Westpac, the Australian Federal Police and the University of Ballarat.

5. References

[1] Australasian Centre for Policing Research. (2006). *Standardisation of definitions of Identity crime terms: a step towards consistency.* (No. 145.3). Payneham, South Australia, Commonwealth of Australia. Retrieved on October 12, 2008 from www.acpr.gov.au

[2] Australian Bureau of Statistics. (2008). *Personal fraud* (No. 4528.0). Canberra, Australian Capital Territory: Author. Retrieved September 22, 2008, from AusStats database.

[3] Australian Institute of Criminology. (2007). *Future directions in technology-enabled Crime: 2007-2009* (no. 78). Canberra, Australian Capital Territory: Choo, K.R, Smith, R.G., McCusker, R.

[4] Environics Research Group. (2008). *2007 Canadian Consumer Mass Marketing Fraud Survey* (No. 459-06). Canada: Author

[5] Federal Bureau of Investigation. (2009, January 14). *Combating cyber crime global Network operates 24/7.* [Headline Archives]. United States: FBI, U.S. Federal Government, U.S. Department of Justice. Retrieved January 14, 2009. from http://www.fbi.gov/page2/jan09/fordham_011409.html

[6] Internet Crime Complain Center. (2007). *2007 Internet crime report.* United States of America: The National White Collar Crime Center, Bureau of Justice Assistance, Federal Bureau of Investigation.

[7] Internet Fraud Complaint Center. (2002). *2001 Internet fraud report* United States of America: The National White Collar Crime Center.

[8] Model Criminal Law Officers' Committee of the Standing Committee of Attorneys – General. (2008). *Final report identity crime.* Barton, Australian Capital Territory, Commonwealth of Australia: Author.

[9] Parliament of the Commonwealth of Australia. (2004). *Cybercrime* Senate Printing Unit, Parliament House, Canberra, Australian Capital Territory: Parliamentary Joint Committee on the Australian Crime Commission.

[10] The Australasian Legal Information Institute www.austlii.edu.au accessed January 3, 2009.

[11] Legislation

Cybercrime Act 2001 (Cwlth). Retrieved December 10, 2008, from The Australian Legal Information Institute database austli