View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Federation ResearchOnline

The Seven Scam Types: Mapping the Terrain of Cybercrime

Amber Stabek, Paul Watters and Robert Layton
Internet Commerce Security Laboratory
University of Ballarat
Mt Helen, Australia
a.stabek@icsl.ballarat.edu.au, p.watters@icsl.ballarat.edu.au, r.layton@ballarat.edu.au

Abstract*— Threat of cybercrime is a growing danger to the economy. Industries and businesses are targeted by cyber-criminals along with members of the general public. Since cybercrime is often a symptom of more complex criminological regimes such as laundering, trafficking and terrorism, the true damage caused to society is unknown. Dissimilarities in reporting procedures and non-uniform cybercrime classifications lead international reporting bodies to produce incompatible results which cause difficulties in making valid comparisons. A cybercrime classification framework has been identified as necessary for the development of an inter-jurisdictional, transnational, and global approach to identify, intercept, and prosecute cyber-criminals. Outlined in this paper is a cybercrime classification framework which has been applied to the incidence of scams. Content analysis was performed on over 250 scam descriptions stemming from in excess of 35 scamming categories and over 80 static features derived. Using hierarchical cluster and discriminant function analysis, the sample was reduced from over 35 ambiguous categories into 7 scam types and the top four scamming functions - identified as scamming business processes, revealed. The results of this research bear significant ramifications to the current state of scam and cybercrime classification, research and analysis, as well as offer significant insight into the business processes and applications adopted by scammers and cyber-criminals.

***Keywords*—Agglomerative, business process, classification, cybercrime, cyberscam, divisive, framework, static feature.**

I. INTRODUCTION

Many organisations affected by cybercrime have their own incident classification systems that operate using an agglomerative approach which involves breaking down events in order to understand their components. While this is useful to the parent organisation, these do not translate across platforms to allow for multi-party adoption which means that collaboration between sectors is near impossible. In contrast to this, the cybercrime classification framework outlined in this paper offers a combined agglomerative - divisive methodology which reconstructs deconstructed events in order to understand its processes. Unlike current criminological approaches, the method applied in the cybercrime classification framework is designed to be multidisciplinary and adaptable across sectors.

The objective of this research is to determine a classification system that can be used by various parties to refer to similar types of scams in international cybercrime. Inconsistencies in the cybercrime lexicon have regularly been reported as a reason behind insubstantial cross border liaisons [1], [2] incongruent transnational cooperation and unsuccessful investigations leading towards increasing cybercrime incidents [3]. This in turn causes congestion of law enforcement and industry resources [3], [6].

A cybercrime classification framework (CCF) would assist in formalising a language of cybercrime remaining consistent within jurisdictions and uniform across multi-national platforms. Such consistency would assist authorities by enhancing communication and cooperation between jurisdictions both at home and across national borders, as well as provide compatibility between cybercrime reporting agencies, allowing for a true representation of cybercrime incidence to be realised internationally.

By utilising the cybercrime classification framework outlined in this paper, 7 genres of scams were identified along with four primary scammer business processes. This information can be used by law enforcement agencies and dedicated cybercrime and fraud task forces in their identification, tracking and monitoring of cybercrimes and a contribution is made towards the utilisation of mixed methodologies for investigating cybercrime. This paper is divided into 6 subsequent sections; Motivation, where the motivation behind this research is discussed, Report Analysis, where an overview of cybercrime statistics and comparisons between reporting institutions and cybercrime research is presented, Methodology, where the methodology applied in this research is presented, Results, where the investigative results are detailed, Discussion, where a comprehensive discussion of the significance of the research and its results is considered, and Conclusion, where final remarks are made.

978-0-7695-4186-0/10 $26.00 © 2010 IEEE
DOI 10.1109/CTC.2010.14

IEEE computer society

II. MOTIVATION

Lack of uniformity and inconsistency in scam classification has been identified as an ongoing concern since the 1990's [1]. Strong evidence is presented [2] citing breadth of variation in scam classification among international and national scam reporting institutions, such as the Australian Bureau of Statistics (ABS), the Internet Crime Complaint Center (iC3), and the Environics Research Group (ERG). Further to this, large variation in scam classification is regularly identified as a primary cause of discrepancy in victim report data, and identified as an area in need of investigation [1], [2], [3], [4], [5]. These inconsistencies are reported as symptoms of ineffective scam identification and low rates of interception by law enforcement agencies resulting in the poor prosecution rates of scammers [6].

Confusion, uncertainty, and false negatives are the consequences of such discrepancy in scam classifications leading to more complex concerns, such as the under-reporting of scam incidence, reduced rates of successful follow up by investigative and law enforcement agencies and difficulty in making correct referrals [2], [6]. The blurred boundaries of scam classification are inherent throughout anti-fraud legislation, which the criminals seemingly exploit to their advantage [7]. While transnational investigative bodies dealing with the complexities of working beyond home borders and interacting with multiple jurisdictions face compounding challenges stemming from these issues [5], [6], [7].

During 1998 Glenn Wahlert from the Australian Federal Police (AFP) presented a paper at the Internet Crime Conference (ICC) where concerns surrounding the escalating adoption of computer technologies for business operations and personal use emerged [1]. During this time, technology based crimes were predominantly computer assisted crimes; these were crimes in which technology was the target of the attack, such as infecting an end-users machine with malicious code [1].

Wahlert [1] described technology based crimes beyond tech-as-target crimes by identifying areas of potential exploitation by cyber-criminals; the banking and finance sector, laundering, counterfeiting, trafficking, sexually related crimes, gambling, tactical intelligence, and scams [1]. Primary concerns surrounding the issues of anonymity, mass communicability, jurisdictional impedances, and cultural ambiguities were identified as high priority themes in need of committed research.

Effective mechanisms for the identification and monitoring of technology based crimes were identified as necessary for controlling technological exploitation. Further to this, it was suggested that the development of transnational agencies authorised to operate across jurisdictions were imperative to fight the phenomena [1].

The current lack of consistency in cyberscam classifications impede coordinated operations and make cross jurisdictional comparisons of scam incidence impossible [7], [2]. A cybercrime classification framework would aid in the detection, interception and prosecution of cyber-criminals.

The discrepancies between reporting institutions are briefly discussed in the next section

III. REPORT ANALYSIS

The iC3 2008 Internet Crime Report found that the reported incidence of cyberscams increased by 33.1% from 2007 [8]. Reports of scam incidence were recorded all throughout the United States with complaints received from as far abroad as Australia. Victim ages ranged from 10 years to 100 years and the total dollar loss was reported to be $264.6 million, an increase of $25.51 million from 2007 [8], [9].

The iC3 only reports on cases where a monetary loss was recorded, and as such only recognises instances of fraud as those where a financial loss has been incurred. The assumption that fraud encompasses only a monetary disadvantage is not representative of the broad and complex nature of cybercrime. The IC3 identified seven types of scams stemming from nine different categories of complaint.

During 2008, the ABS released the results from its first ever personal fraud survey [4]. A recorded dollar loss of $AUD980 million was attributable to incidences of personal fraud alone. While personal fraud remained undefined by the ABS, it was dissected into two categories of victimisation; these were 'scams' and 'identity fraud'. A person was recorded as being scammed if they responded to a scam by supplying information and/or money [4]. To become a victim of identity fraud, the victim must have had their personal details used by another person without their consent [4].

A distinction is identified between incidence of identity fraud and incidence of identity theft [2] and it is argued that before identity fraud can transpire, identity theft must first occur [10], this detail was not recorded by the ABS.

It is recorded that 23.5 million people within the UK were the target of a scamming event [11], this, represented 48% of all UK residents at the time of the mass marketing fraud report and an estimated total dollar loss per year is offered with the amount of £3.5 billion.

A detailed overview of the state of fraud in Australia describing a clear and present hierarchy of fraudster crimes [6] implies an interconnectedness between fraud and scam events. Prenzler and Hayes [6] suggest that jurisdictional inconsistencies and variations in fraud conceptualisation are responsible for the inadequate view of fraud present in society today. This inadequate view is fuelled by a sole-source research base which extends from published and incompatible victim report data collected from across the globe. It is recognised that without standardisation of estimation and calculation led by consistent classifications, an understanding of the true impact of fraudster crimes and in particular, cybercrime, cannot be realised.

A Framework for Data Mining [12] discussed such approaches as association analysis, classification, prediction, and cluster analysis. The applied study was a supervised study which began by ranking crimes based on their perceived public harm. Fraud achieved fifth place while cybercrime gained first place in the ranking statistics. Pattern visualisation techniques were recommended as the best approach for analysis of cybercrimes [12].

Routine activities theory (RAT) re-emerged as a promising theoretical perspective during 2005 [13] and was applied to incidents of crime in hopes of understanding crime distributions. In 2008, it was proposed that RAT and lifestyle-exposure theory (LET) could be utilised for cybercrime by assessing computer crime victimisation rates [14]. The conclusion suggested that a hybrid of RAT and LET could be used to identify potential targets of computer crime based on online lifestyle and digital guardianship markers [14].

IV. METHODOLOGY

Hierarchical clustering analysis presents a method of modelling hierarchies within observed data. It has been suggested that a hierarchy of fraud exists [6] which implies that a hierarchy of scams also exists, this can also be inferred for the realm of cybercrime. These hierarchies can be investigated by applying hierarchical analytical techniques such as hierarchical cluster analyses on purpose driven data. The aim of this research is to investigate the presence of hierarchy within scam-based data and this is achieved through the derivation and analysis of scam static features. Following the pattern recognition phase of analysis, model verification is performed by applying discriminant function analysis to the clustering results.

The proposed method used in the divisively breaks the scams down into their static features and agglomeratively reconstructs scams based upon their identified static components, this allows for the determination of the business processes underlying cybercrimes. This approach takes into account each instance of cyber-crime in its whole form and through a process of deconstruction, static elements – the building blocks foundational to the processes and compilation of each crime are revealed. Once cybercrime cases are deconstructed to a state of static feature elements, cases are agglomeratively clustered based upon similarity of static features and cybercrime genres are revealed. This method has been applied to scam cases sourced from national and international institutions and a summary of the results of the CCF methodology appear below.

Over 250 scam cases sourced from 14 different scam reporting agencies and annual reports (see Table 1 in Appendix) were individually analysed for static features with each scam's resultant composition of static features recorded in the vector space. Following cluster and discriminant function analysis, similar scam cases were grouped according to similarity of static feature composition and it was determined that 7 scam genres exist, significantly less than the recorded 38 identified by the scam sources. Significant scam identifying features were recognised and these can be used to identify and classify new scams as they emerge.

Scam descriptions offer a rich source of information pertaining to the reporting institution's understanding of individual schemes. From analysing the content of a scam description, a detailed representation of scam processes can be understood. The purpose of the analysis performed here was to identify homogeneous subsets of scam cases. This was achieved through the use of hierarchical clustering analysis and discriminant function analysis. The aim of this research was to formulate clusters of scam cases derived from similarity matching principles based upon the purposely derived static features of scam descriptions. It was hypothesized that a smaller number of scam clusters could be found than the publicly acknowledged 38 which were recorded during the data collection phase.

Furthest neighbour hierarchical clustering using the Jaccard binary coefficient was used to partition similar scams. This method of clustering was selected for use because of its natural tendency to find homogeneous subsets within a data set [15].

The furthest neighbour is a method of complete linkage and a description of this appears below in Figure A. For complete linkage the distance between the furthest pair of cases from separate groups is considered. This approach is an agglomerative approach where data is partitioned according to Pn, Pn-1,…,P1. Where Pn is a single case or cluster and P1 contains all cases.

The Jaccard coefficient is a binary distance measure and is calculated by a / (a+b+c), where a = the presence of same features in both cases, b = the presence of features in case 1 and the absence of those same features in case 2, and c = the absence of features in case 1 and the presence of those same features in case 2.

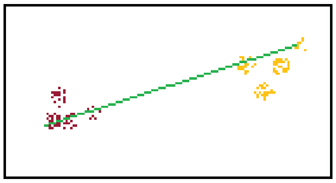


Figure A Complete Linkage

The memberships of scam clusters were recorded and a dendrogram and bar charts tabulating the frequencies within each cluster were created (see Figure 1 and 2 in the Appendix). The result of the hierarchical cluster model was evaluated and verified using a discriminant function analysis.

The goal of the discriminant function analysis was to assess the reliability of the model where a reliable model was defined as a model in which the (n-1) discriminant functions combined account for at least 95% of variability within the data. A model which accounted for at least 95% of variability could then be claimed to be at least 95% accurate. Another goal of the discriminant function analysis was to identify which scam static features were significant to cluster membership prediction.

V. RESULTS

The cluster solution which was accurate at least 95% of the time and contained the fewest number of clusters would satisfy the constraints of the investigation. Using the furthest neighbour Jaccard coefficient hierarchical cluster model and removing all insignificant static features, the 250+ scam cases from 38 scam categories could be clustered into only 7 clusters of scam types - called scam genres, whilst achieving 95% accuracy. Of the 82 scam static features derived, 68 were found to be significant to the variation in the model and thus impacted the placement of scam cases into scam clusters (see Table 3, 4, and 5 in the Appendix).

The validation of the furthest neighbour, Jaccard coefficient hierarchical clustering model for scam-based research carries implications for the usability of text-based publicly accessible data in mixed methodological analysis. These results also confirm the variability of scam descriptions across jurisdictions and provide evidence for the necessity for the standardisation of terminology.

These results confirm that the fewest number of clusters with the least number of scam memberships, inferring homogeneity across clusters and among cases is 7, and scam cases can be accurately allocated to a scam genre (cluster) 95% of the time using the furthest neighbour, Jaccard coefficient hierarchical clustering model.

Over two hundred and fifty individual scam cases and 82 purposely derived scam static features belonging to 38 separate source classified scam genre categories were analysed using an unsupervised agglomerative furthest neighbour, Jaccard coefficient hierarchical clustering model which was verified and tested for reliability by a discriminant function analysis.

This method achieved 95% accuracy in partitioning scam cases into scam genres. The 38 source classified scam genres were reduced down to only 7 scam genres which were Financial Gain through Low Level Trickery, Financial Gain and Information Gathering through Developed Story Based Applications, Participation and Information Gathering through Employment Based Strategies, Financial Gain through Implied Necessary Obligation, Information Gathering through Legitimate Looking Appeals, Financial Gain through Merchant and Customer Based Exploitation, and Financial Gain and Information Gathering through Marketing Opportunities.

It was discovered that only 68 of the 82 scam static features were required to achieve a 95% level of accuracy in scam membership and the most prominent of these static features were what the scam offered, the role of the victim, the goal of the scammer, and the method of scam introduction.

It is demonstrated that scams are currently over classified within current literature and that only 7 scam types or scam genres exist compared to the 38 recorded source-classified scam categories.

VI. DISCUSSION

1. Financial Gain through Low Level Trickery

The first scam genre contains 72 scam cases which are detailed in the appendix. This scam genre is made up of scam cases that involve the most basic forms of trickery. These involve scams that are not necessarily thorough in planning and detail. Victims falling for scam genre one scams would take people and communications at face value and not expend time or energy on investigating scam claims or the people behind them. These scams target the individual or company for once off transactions initially and where possible, if there were potential for the scam to be extended to elicit more funds from the victim, this may be pursued.

Scam genre 1 contains scams are at the most basic level after the victim's cash or ability to get loans. Door to door scams often involve the soliciting of services that are paid for and never performed. Psychic and clairvoyant scams involve the soliciting of services or merchandise that is paid for and is not what it had promised to be. Cheque overpayment scams involve the overpayment for a purchase and a request for the balance to be wired back to the sender. In this situation, the cheque is fraudulent and the scammer walks away with the victim's money after they have refunded the difference and financial advice scams involve soliciting supposed financial advice for an upfront fee. Whether or not the advice is useful is irrelevant since the victim has just paid a scammer and the scammer has walked away with the victim's money and possibly their personal and private details to use in a future identity based scam. Similarity among scams found in scam genre 1 emerge, the most obvious is the payment of funds to the scammer.

2. Financial Gain and Information Gathering through Developed Story Based Applications

The second scam genre contains 74 scam cases. This scam genre is made up of scam cases that involve complex planning and detail. These scams hinge on the opportunistic nature of the general public as well as the scammer. In this sense a common bond is formed between the scammer and their victims and that is opportunity. The first scam in scam genre 2 is the charity scam. This scam relies on the poverty and necessity of others, this scam also emerges during natural or manmade disaster. These scams rely on assumed public knowledge of a cohort of individuals or a global tragedy. They are story based scams and offer to their victims the opportunity to make a difference in the world through financial assistance.

The ultimate goal of the scams found in scam genre 2 is money, the same as scam genre 1 however, the method of realising this goal is different. The grouping of unexpected prizes and chain letters together with charity scams and Nigerian 419 scams suggests some similarity in scam perpetrations; further investigation might prove useful in determining on what grounds these scams are alike. This may be due to the story based nature of all of these scams. Another goal which manifests in dating and romance scams, Nigerian 419 scams, and even spam offers is the collection of personal or private information.

3. *Participation and Information Gathering through Employment Based Strategies*

The third scam genre contains 22 scam cases. This scam genre is made up of scam cases that involve complex planning and detail, similar to that found in scam genre 2 however, the scams in scam genre 3 target the individual in the sense that they seek participation from victims. Each scam listed in scam genre three involves a level of victim 'employment' in which the victim participates in the scheme; normally a laundering scam, and for their participation they are financially rewarded. These scams can often lead to identity theft and other identity based crimes since in becoming involved in one of these scams the victim may have been an applicant for what they had believed was an authentic employment opportunity. With their application, the victim would have supplied the scammer/s with a full working and educational history, full name and date of birth as well as bank account details.

4. *Financial Gain through Implied Necessary Obligation*

The fourth scam genre contains 17 scam cases. This scam genre is made up of scam cases that require victim call backs or responses for the scam to be successful. The scams found here are different to those seen in scam genre one, two, and three. Most of these scams rely on alternative technologies to that of the Internet and World Wide Web for dissemination. There are a mixture of scams here that aim to trick the victim into a response and thus facing un-expected and unrealised charges. Regardless of the method of the scam, or the role of the victim, this scam genre contains scams that aim to make money from the victim in ways that would seem necessary or pertinent to the situation.

5. *Information Gathering through Apparently Authentic Appeals*

The fifth scam genre contains 38 scam cases. This scam genre is made up of scam cases that involve high level knowledge of how systems operate and contains those scams that are syntactically driven such as spyware and key logger scams. This scam genre also contains scams that seek information for the purpose of identity related crimes such as identity theft and credit/debit card fraud. The reason why syntactic scams using spyware and key loggers are clustered along with identity theft and credit/debit card scams is because syntactic attacks are dispersed with the goal of gathering victim identity credentials or other forms of information. Therefore, spyware and key logging scams are identified as a tool for the success of information gathering scams such as identity theft and credit/debit card scams. Also found in scam genre 5 are phishing scams which are also synonymous with identity theft and credit/debit card fraud.

6. *Financial Gain through Merchant and Customer Based Exploitation*

The sixth scam genre contains 24 scam cases. This scam genre is made up of scam cases that incorporate the roles of both the seller and buyer in the scam description. These scams are all transaction based scams involving a buyer and a seller; shill bidding, bid shielding, merchandise non-delivery, payment non-delivery, and product authenticity. The goal of this group of scams is financial gain which is achieved through various versions and applications of similarly styled scams. These scams are well researched and developed even though the victim and scammer only communicate for a short period of time.

7. *Financial Gain and Information Gathering through Marketing Opportunities*

The final scam genre is scam genre 7 which contains 30 scam cases. This scam genre is made up of scam cases that involve the exploitation of investment opportunities and contains a mixture of scam types including Ponzi and pyramid, identity theft, computer prediction software, investment seminars, charity fraud, affinity fraud, get rich quick scams and 419 advance fee fraud. Without further detailed analysis of the inter-connected nature of the suite of compiled static features fitting into this category, the presence of this mixture of scam titles is interpreted as hinging on the suggestion of investment opportunities within each scam case. The scams within scam genre 7 are marketed as money making opportunities, whether through investment, business opportunity, shares or gambling. However, the goal of the scammer is financial gain and in some instances this extends to information gathering.

8. The Top Four Scammer Business Processes

The top four cybercriminal business processes were identified and these account for the majority of the variation in scam genre placement which means that a scam's type can be identified early on in the scamming process by these 4 static features. By acknowledging these static features, the type of scam a scheme is can be confidently identified and future paths of communication and transaction flow can then be projected leading the way to the positive mapping of scam case progress and the identification of optimum paths of interception by law enforcement.

While it would be over confident to suggest that intercepting scam communications and transactions will lead to scammer prosecution, by identifying and projecting the business processes involved in scamming communications and transactions, optimum paths of interception causing the greatest damage to the scammer exhausting their time and funds can be realised.

The four most significant static features crucial to the successful scam campaign and therefore, the most important business processes that scammers build their schemes upon are: a) what the scam offers, b) the role of the victim, c) the goal of the scammer, and d) method of scam introduction.

If a cybercriminal were to begin planning a new scam campaign, these are the priority features that would need to be known and addressed by the scammer during the business development phase. Before launching a campaign, the scammer must know what he/she seeks, they must have an end goal decided, knowing this, the scammer develops a scam campaign which will deliver the desired outcome.

From knowledge of the desired outcome, the scammer must then decide on how he/she will introduce the scam to the target, further to this, contingencies would be made on how to reach as many targets as necessary to meet and exceed the intended goal. The scammer must know how to get the target involved in the scam, to do this, the scam must offer something of value to the target and finally, before the campaign can be finalised, the scammer must know what role he/she would play in the campaign, and therefore, what role the target will play.

By identifying these four key elements of the cybercriminal's business process, scams can be confidently identified and acted upon by the relevant authorities early on in the scamming campaign. Most importantly and in most cases, these key features can be identified from the very first scam communication, which means that the CCF methodology can be used as a tool for identifying possible scam communications before an incident of scamming even occurs. This can be demonstrated with the following example:

"Dear Beloved Friend, I am Mrs Lovelin Vincent, I was married to Late Chief Vincent Williams a government contractor I have the sum of US$5.5m which I inherited from my late husband before he was killed by unknown people on his way returning from a business trip. I want this money to be transfer in an account in your country for charity, widow's and church in your area.
God bless you and your family
Yours in the Lord."

The above is an example of what is usually termed a 419 scam. In this example, the scammer is pretending to be the widow of an influential man who was tragically killed and who now has a substantial sum of money that she wishes to donate to those charities within the intended victim's vicinity. This is the first communication of this 419 scam and the business processes used by the scammer can be identified as: a) what the scam offers – money, a chance to offer assistance, b) the role of the victim – randomly chosen and if the scam were to eventuate, the victim would assume the role of a third party or 'courier' to transfer and disseminate the supposed funds, c) the goal of the scammer – to gain access to the victim's bank account details and take their money, and d) method of scam introduction – email communication.

VII. Conclusion

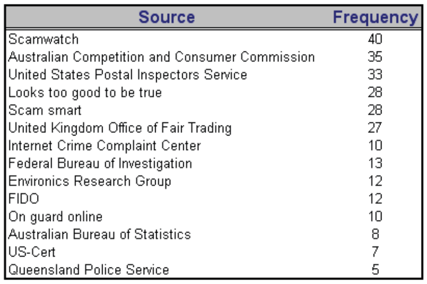
The cybercrime classification framework (CCF) can be expanded to incorporate all current and future forms of cybercrime. The ease with which the framework can be updated will assist authorities, industry and business in remaining constantly prepared with the most up to date and relevant information available on the instances of and types of cybercrimes circulating the Internet and targeting corporate operations and individuals.

Due to the user friendly nature of the CCF, it can easily be adopted by small to large businesses and the industrial sector to consistently and effectively manage and communicate their experiences of cybercrime to the authorities. Individual agencies can map their existing known schemes into the CCF and the authorities can use the CCF to develop consistent terms for further defining within the prosecution process as well as use the CCF to enhance transnational cooperation and coordination.

The adoption of the cybercrime classification framework for state and federal reporting institutions would also encourage collaboration and useful interpretation of scam and cybercrime based statistics to give meaningful, accurate and up to date evaluations of cyber-based incidents and finally, the CCF methodology described here would improve the efficiency in identifying, tracking and monitoring cybercrimes.

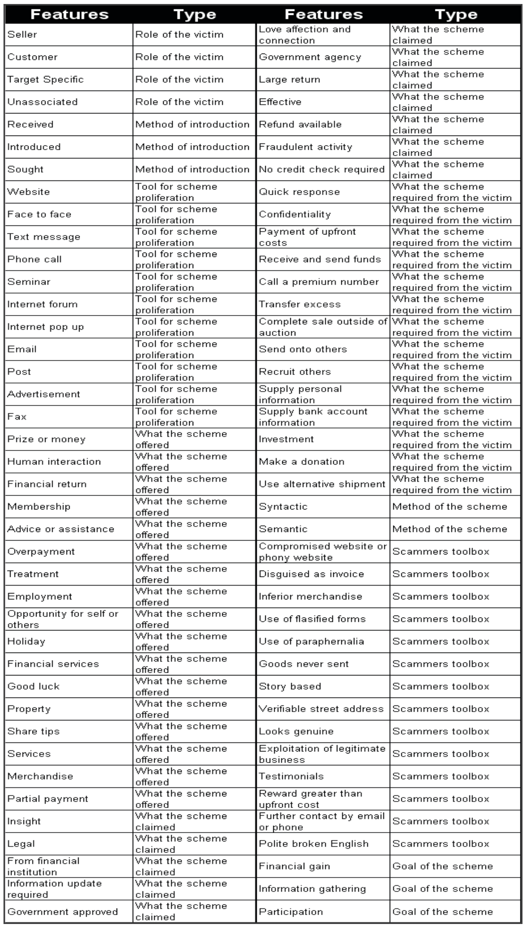
Appendix

Table 1: Scam source and its frequency contribution to the sample



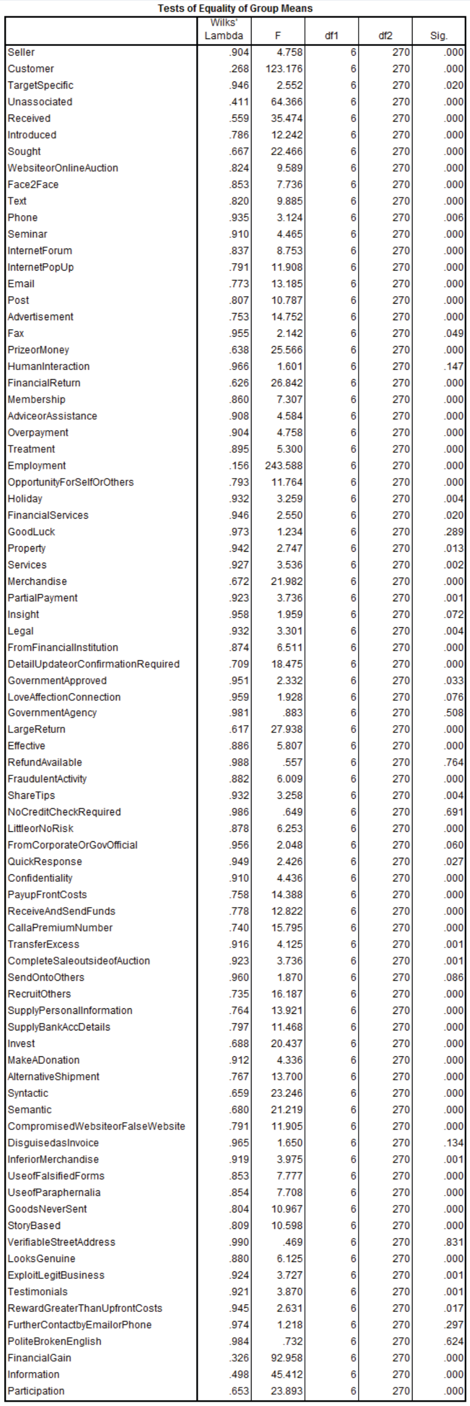
Source	Frequency
Scamwatch	40
Australian Competition and Consumer Commission	35
United States Postal Inspectors Service	33
Looks too good to be true	28
Scam smart	28
United Kingdom Office of Fair Trading	27
Internet Crime Complaint Center	10
Federal Bureau of Investigation	13
Environics Research Group	12
FIDO	12
On guard online	10
Australian Bureau of Statistics	8
US-Cert	7
Queensland Police Service	5

Table 2: List of derived scam static features



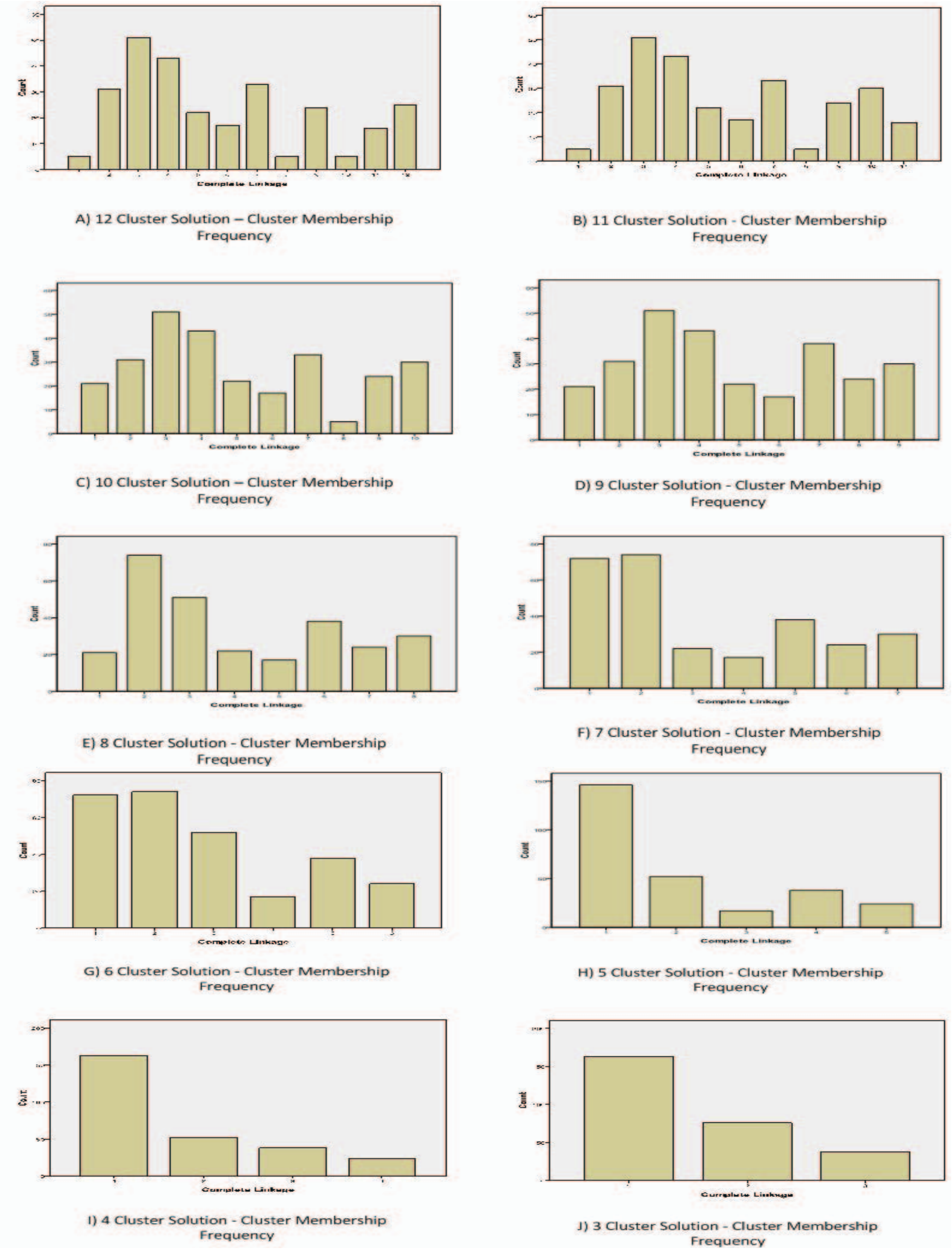
Features	Type	Features	Type
Seller	Role of the victim	Love affection and connection	What the scheme claimed
Customer	Role of the victim	Government agency	What the scheme claimed
Target Specific	Role of the victim	Large return	What the scheme claimed
Unassociated	Role of the victim	Effective	What the scheme claimed
Received	Method of introduction	Refund available	What the scheme claimed
Introduced	Method of introduction	Fraudulent activity	What the scheme claimed
Sought	Method of introduction	No credit check required	What the scheme claimed
Website	Tool for scheme proliferation	Quick response	What the scheme required from the victim
Face to face	Tool for scheme proliferation	Confidentiality	What the scheme required from the victim
Text message	Tool for scheme proliferation	Payment of upfront costs	What the scheme required from the victim
Phone call	Tool for scheme proliferation	Receive and send funds	What the scheme required from the victim
Seminar	Tool for scheme proliferation	Call a premium number	What the scheme required from the victim
Internet forum	Tool for scheme proliferation	Transfer excess	What the scheme required from the victim
Internet pop up	Tool for scheme proliferation	Complete sale outside of auction	What the scheme required from the victim
Email	Tool for scheme proliferation	Send onto others	What the scheme required from the victim
Post	Tool for scheme proliferation	Recruit others	What the scheme required from the victim
Advertisement	Tool for scheme proliferation	Supply personal information	What the scheme required from the victim
Fax	Tool for scheme proliferation	Supply bank account information	What the scheme required from the victim
Prize or money	What the scheme offered	Investment	What the scheme required from the victim
Human interaction	What the scheme offered	Make a donation	What the scheme required from the victim
Financial return	What the scheme offered	Use alternative shipment	What the scheme required from the victim
Membership	What the scheme offered	Syntactic	Method of the scheme
Advice or assistance	What the scheme offered	Semantic	Method of the scheme
Overpayment	What the scheme offered	Compromised website or phony website	Scammers toolbox
Treatment	What the scheme offered	Disguised as invoice	Scammers toolbox
Employment	What the scheme offered	Inferior merchandise	Scammers toolbox
Opportunity for self or others	What the scheme offered	Use of flasified forms	Scammers toolbox
Holiday	What the scheme offered	Use of paraphernalia	Scammers toolbox
Financial services	What the scheme offered	Goods never sent	Scammers toolbox
Good luck	What the scheme offered	Story based	Scammers toolbox
Property	What the scheme offered	Verifiable street address	Scammers toolbox
Share tips	What the scheme offered	Looks genuine	Scammers toolbox
Services	What the scheme offered	Exploitation of legitimate business	Scammers toolbox
Merchandise	What the scheme offered	Testimonials	Scammers toolbox
Partial payment	What the scheme offered	Reward greater than upfront cost	Scammers toolbox
Insight	What the scheme claimed	Further contact by email or phone	Scammers toolbox
Legal	What the scheme claimed	Polite broken English	Scammers toolbox
From financial institution	What the scheme claimed	Financial gain	Goal of the scheme
Information update required	What the scheme claimed	Information gathering	Goal of the scheme
Government approved	What the scheme claimed	Participation	Goal of the scheme

Table 3: DFA equality of group means



Tests of Equality of Group Means

	Wilks' Lambda	F	df1	df2	Sig.
Seller	.904	4.758	6	270	.000
Customer	.268	123.176	6	270	.000
TargetSpecific	.946	2.552	6	270	.020
Unassociated	.411	64.366	6	270	.000
Received	.559	35.474	6	270	.000
Introduced	.786	12.242	6	270	.000
Sought	.667	22.466	6	270	.000
WebsiteorOnlineAuction	.824	9.589	6	270	.000
Face2Face	.853	7.736	6	270	.000
Text	.820	9.885	6	270	.000
Phone	.935	3.124	6	270	.006
Seminar	.910	4.465	6	270	.000
InternetForum	.837	8.753	6	270	.000
InternetPopUp	.791	11.908	6	270	.000
Email	.773	13.185	6	270	.000
Post	.807	10.787	6	270	.000
Advertisement	.753	14.752	6	270	.000
Fax	.955	2.142	6	270	.049
PrizeorMoney	.638	25.566	6	270	.000
HumanInteraction	.966	1.601	6	270	.147
FinancialReturn	.626	26.842	6	270	.000
Membership	.860	7.307	6	270	.000
AdviceorAssistance	.908	4.584	6	270	.000
Overpayment	.904	4.758	6	270	.000
Treatment	.895	5.300	6	270	.000
Employment	.156	243.588	6	270	.000
OpportunityForSelfOrOthers	.793	11.764	6	270	.000
Holiday	.932	3.259	6	270	.004
FinancialServices	.946	2.550	6	270	.020
GoodLuck	.973	1.234	6	270	.289
Property	.942	2.747	6	270	.013
Services	.927	3.536	6	270	.002
Merchandise	.672	21.982	6	270	.000
PartialPayment	.923	3.736	6	270	.001
Insight	.958	1.959	6	270	.072
Legal	.932	3.301	6	270	.004
FromFinancialInstitution	.874	6.511	6	270	.000
DetailUpdateorConfirmationRequired	.709	18.475	6	270	.000
GovernmentApproved	.951	2.332	6	270	.033
LoveAffectionConnection	.959	1.928	6	270	.076
GovernmentAgency	.981	.883	6	270	.508
LargeReturn	.617	27.938	6	270	.000
Effective	.886	5.807	6	270	.000
RefundAvailable	.988	.557	6	270	.764
FraudulentActivity	.882	6.009	6	270	.000
ShareTips	.932	3.258	6	270	.004
NoCreditCheckRequired	.986	.649	6	270	.691
LittleorNoRisk	.878	6.253	6	270	.000
FromCorporateOrGovOfficial	.956	2.048	6	270	.060
QuickResponse	.949	2.426	6	270	.027
Confidentiality	.910	4.436	6	270	.000
PayupFrontCosts	.758	14.388	6	270	.000
ReceiveAndSendFunds	.778	12.822	6	270	.000
CallaPremiumNumber	.740	15.795	6	270	.000
TransferExcess	.916	4.125	6	270	.001
CompleteSaleoutsideofAuction	.923	3.736	6	270	.001
SendOntoOthers	.960	1.870	6	270	.086
RecruitOthers	.735	16.187	6	270	.000
SupplyPersonalInformation	.764	13.921	6	270	.000
SupplyBankAccDetails	.797	11.468	6	270	.000
Invest	.688	20.437	6	270	.000
MakeADonation	.912	4.336	6	270	.000
AlternativeShipment	.767	13.700	6	270	.000
Syntactic	.659	23.246	6	270	.000
Semantic	.680	21.219	6	270	.000
CompromisedWebsiteorFalseWebsite	.791	11.905	6	270	.000
DisguisedasInvoice	.965	1.650	6	270	.134
InferiorMerchandise	.919	3.975	6	270	.001
UseofFalsifiedForms	.853	7.777	6	270	.000
UseofParaphernalia	.854	7.708	6	270	.000
GoodsNeverSent	.804	10.967	6	270	.000
StoryBased	.809	10.598	6	270	.000
VerifiableStreetAddress	.990	.469	6	270	.831
LooksGenuine	.880	6.125	6	270	.000
ExploitLegitBusiness	.924	3.727	6	270	.001
Testimonials	.921	3.870	6	270	.001
RewardGreaterThanUpfrontCosts	.945	2.631	6	270	.017
FurtherContactbyEmailorPhone	.974	1.218	6	270	.297
PoliteBrokenEnglish	.984	.732	6	270	.624
FinancialGain	.326	92.958	6	270	.000
Information	.498	45.412	6	270	.000
Participation	.653	23.893	6	270	.000



A) 12 Cluster Solution – Cluster Membership Frequency

B) 11 Cluster Solution - Cluster Membership Frequency

C) 10 Cluster Solution – Cluster Membership Frequency

D) 9 Cluster Solution - Cluster Membership Frequency

E) 8 Cluster Solution - Cluster Membership Frequency

F) 7 Cluster Solution - Cluster Membership Frequency

G) 6 Cluster Solution - Cluster Membership Frequency

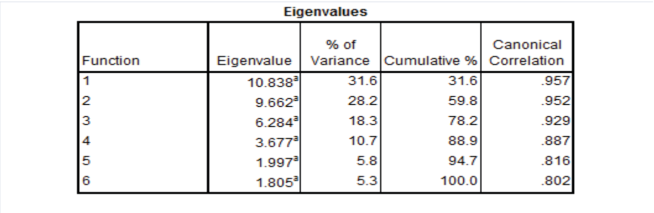
H) 5 Cluster Solution - Cluster Membership Frequency

I) 4 Cluster Solution - Cluster Membership Frequency

J) 3 Cluster Solution - Cluster Membership Frequency

Figure 1: Frequency bar charts of scam cluster memberships

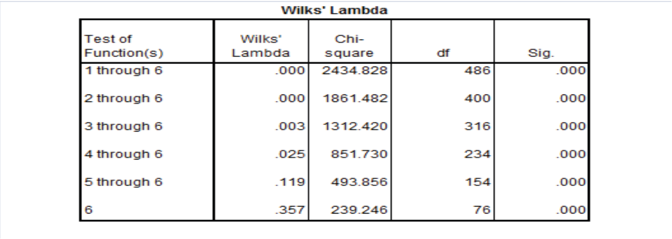
Table 4: DFA Eigenvalues



Eigenvalues

Function	Eigenvalue	% of Variance	Cumulative %	Canonical Correlation
1	10.838[a]	31.6	31.6	.957
2	9.662[a]	28.2	59.8	.952
3	6.284[a]	18.3	78.2	.929
4	3.677[a]	10.7	88.9	.887
5	1.997[a]	5.8	94.7	.816
6	1.805[a]	5.3	100.0	.802

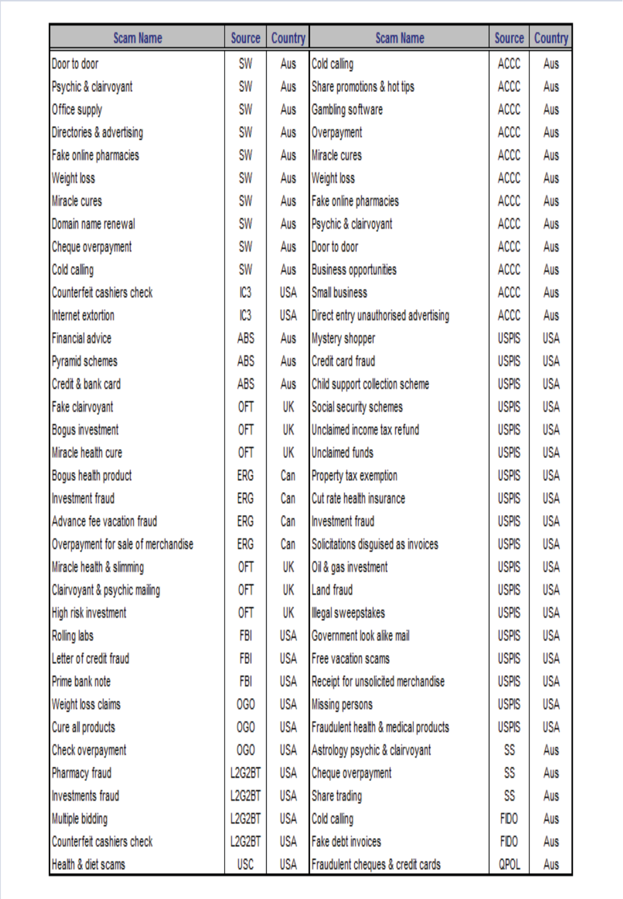
Table 5: DFA Tests of significance



Wilks' Lambda

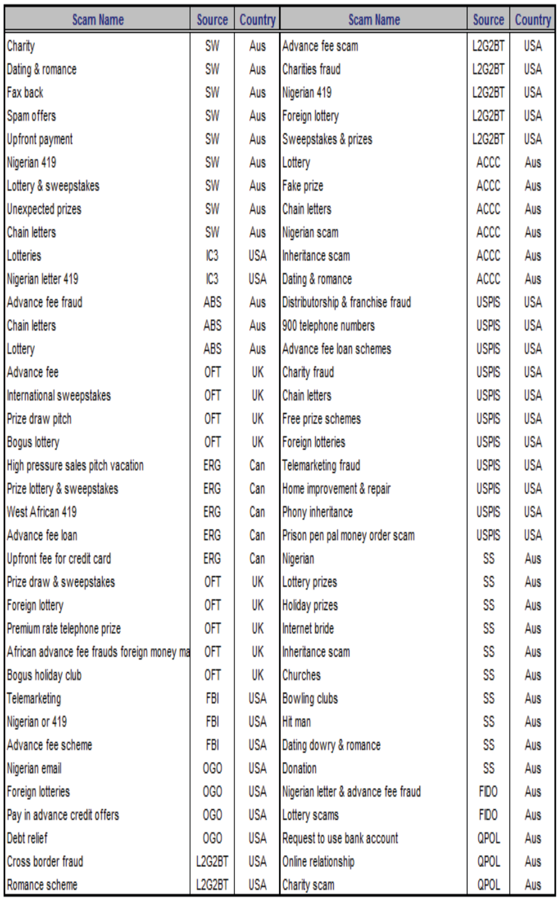
Test of Function(s)	Wilks' Lambda	Chi-square	df	Sig.
1 through 6	.000	2434.828	486	.000
2 through 6	.000	1861.482	400	.000
3 through 6	.003	1312.420	316	.000
4 through 6	.025	851.730	234	.000
5 through 6	.119	493.856	154	.000
6	.357	239.246	76	.000

Table 6: Scam genre 1



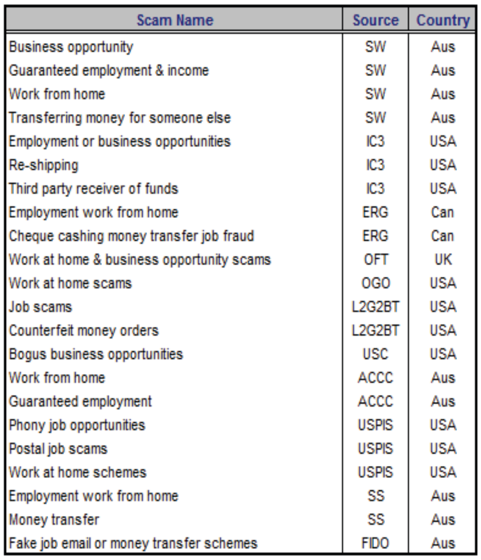
Scam Name	Source	Country	Scam Name	Source	Country
Door to door	SW	Aus	Cold calling	ACCC	Aus
Psychic & clairvoyant	SW	Aus	Share promotions & hot tips	ACCC	Aus
Office supply	SW	Aus	Gambling software	ACCC	Aus
Directories & advertising	SW	Aus	Overpayment	ACCC	Aus
Fake online pharmacies	SW	Aus	Miracle cures	ACCC	Aus
Weight loss	SW	Aus	Weight loss	ACCC	Aus
Miracle cures	SW	Aus	Fake online pharmacies	ACCC	Aus
Domain name renewal	SW	Aus	Psychic & clairvoyant	ACCC	Aus
Cheque overpayment	SW	Aus	Door to door	ACCC	Aus
Cold calling	SW	Aus	Business opportunities	ACCC	Aus
Counterfeit cashiers check	IC3	USA	Small business	ACCC	Aus
Internet extortion	IC3	USA	Direct entry unauthorised advertising	ACCC	Aus
Financial advice	ABS	Aus	Mystery shopper	USPIS	USA
Pyramid schemes	ABS	Aus	Credit card fraud	USPIS	USA
Credit & bank card	ABS	Aus	Child support collection scheme	USPIS	USA
Fake clairvoyant	OFT	UK	Social security schemes	USPIS	USA
Bogus investment	OFT	UK	Unclaimed income tax refund	USPIS	USA
Miracle health cure	OFT	UK	Unclaimed funds	USPIS	USA
Bogus health product	ERG	Can	Property tax exemption	USPIS	USA
Investment fraud	ERG	Can	Cut rate health insurance	USPIS	USA
Advance fee vacation fraud	ERG	Can	Investment fraud	USPIS	USA
Overpayment for sale of merchandise	ERG	Can	Solicitations disguised as invoices	USPIS	USA
Miracle health & slimming	OFT	UK	Oil & gas investment	USPIS	USA
Clairvoyant & psychic mailing	OFT	UK	Land fraud	USPIS	USA
High risk investment	OFT	UK	Illegal sweepstakes	USPIS	USA
Rolling labs	FBI	USA	Government look alike mail	USPIS	USA
Letter of credit fraud	FBI	USA	Free vacation scams	USPIS	USA
Prime bank note	FBI	USA	Receipt for unsolicited merchandise	USPIS	USA
Weight loss claims	OGO	USA	Missing persons	USPIS	USA
Cure all products	OGO	USA	Fraudulent health & medical products	USPIS	USA
Check overpayment	OGO	USA	Astrology psychic & clairvoyant	SS	Aus
Pharmacy fraud	L2G2BT	USA	Cheque overpayment	SS	Aus
Investments fraud	L2G2BT	USA	Share trading	SS	Aus
Multiple bidding	L2G2BT	USA	Cold calling	FIDO	Aus
Counterfeit cashiers check	L2G2BT	USA	Fake debt invoices	FIDO	Aus
Health & diet scams	USC	USA	Fraudulent cheques & credit cards	QPOL	Aus

Table 7: Scam genre 2



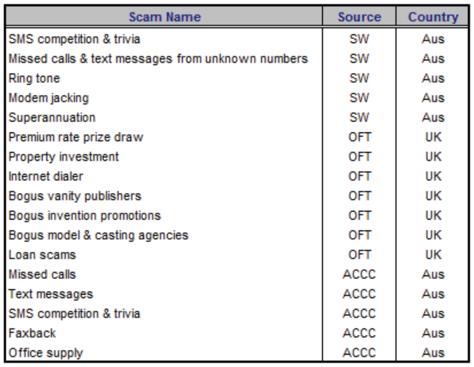
Scam Name	Source	Country	Scam Name	Source	Country
Charity	SW	Aus	Advance fee scam	L2G2BT	USA
Dating & romance	SW	Aus	Charities fraud	L2G2BT	USA
Fax back	SW	Aus	Nigerian 419	L2G2BT	USA
Spam offers	SW	Aus	Foreign lottery	L2G2BT	USA
Upfront payment	SW	Aus	Sweepstakes & prizes	L2G2BT	USA
Nigerian 419	SW	Aus	Lottery	ACCC	Aus
Lottery & sweepstakes	SW	Aus	Fake prize	ACCC	Aus
Unexpected prizes	SW	Aus	Chain letters	ACCC	Aus
Chain letters	SW	Aus	Nigerian scam	ACCC	Aus
Lotteries	IC3	USA	Inheritance scam	ACCC	Aus
Nigerian letter 419	IC3	USA	Dating & romance	ACCC	Aus
Advance fee fraud	ABS	Aus	Distributorship & franchise fraud	USPIS	USA
Chain letters	ABS	Aus	900 telephone numbers	USPIS	USA
Lottery	ABS	Aus	Advance fee loan schemes	USPIS	USA
Advance fee	OFT	UK	Charity fraud	USPIS	USA
International sweepstakes	OFT	UK	Chain letters	USPIS	USA
Prize draw pitch	OFT	UK	Free prize schemes	USPIS	USA
Bogus lottery	OFT	UK	Foreign lotteries	USPIS	USA
High pressure sales pitch vacation	ERG	Can	Telemarketing fraud	USPIS	USA
Prize lottery & sweepstakes	ERG	Can	Home improvement & repair	USPIS	USA
West African 419	ERG	Can	Phony inheritance	USPIS	USA
Advance fee loan	ERG	Can	Prison pen pal money order scam	USPIS	USA
Upfront fee for credit card	ERG	Can	Nigerian	SS	Aus
Prize draw & sweepstakes	OFT	UK	Lottery prizes	SS	Aus
Foreign lottery	OFT	UK	Holiday prizes	SS	Aus
Premium rate telephone prize	OFT	UK	Internet bride	SS	Aus
African advance fee frauds foreign money ma	OFT	UK	Inheritance scam	SS	Aus
Bogus holiday club	OFT	UK	Churches	SS	Aus
Telemarketing	FBI	USA	Bowling clubs	SS	Aus
Nigerian or 419	FBI	USA	Hit man	SS	Aus
Advance fee scheme	FBI	USA	Dating dowry & romance	SS	Aus
Nigerian email	OGO	USA	Donation	SS	Aus
Foreign lotteries	OGO	USA	Nigerian letter & advance fee fraud	FIDO	Aus
Pay in advance credit offers	OGO	USA	Lottery scams	FIDO	Aus
Debt relief	OGO	USA	Request to use bank account	QPOL	Aus
Cross border fraud	L2G2BT	USA	Online relationship	QPOL	Aus
Romance scheme	L2G2BT	USA	Charity scam	QPOL	Aus

Table 8: Scam genre 3



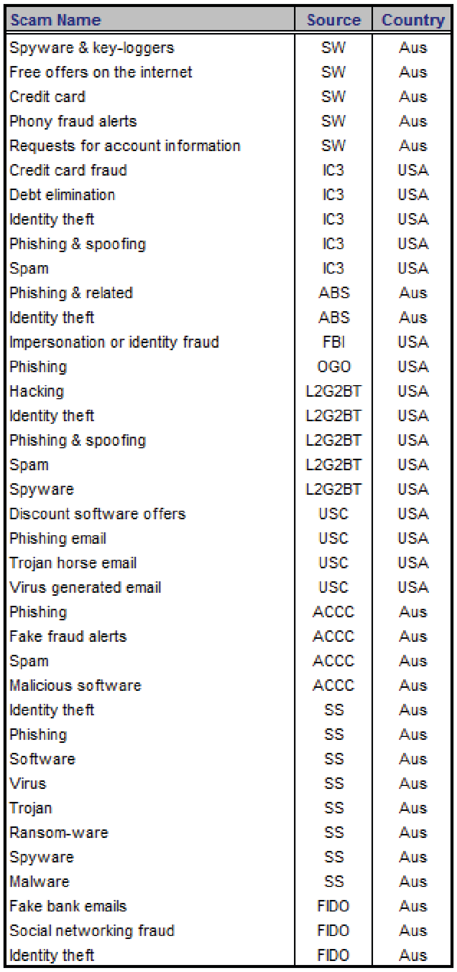
Scam Name	Source	Country
Business opportunity	SW	Aus
Guaranteed employment & income	SW	Aus
Work from home	SW	Aus
Transferring money for someone else	SW	Aus
Employment or business opportunities	IC3	USA
Re-shipping	IC3	USA
Third party receiver of funds	IC3	USA
Employment work from home	ERG	Can
Cheque cashing money transfer job fraud	ERG	Can
Work at home & business opportunity scams	OFT	UK
Work at home scams	OGO	USA
Job scams	L2G2BT	USA
Counterfeit money orders	L2G2BT	USA
Bogus business opportunities	USC	USA
Work from home	ACCC	Aus
Guaranteed employment	ACCC	Aus
Phony job opportunities	USPIS	USA
Postal job scams	USPIS	USA
Work at home schemes	USPIS	USA
Employment work from home	SS	Aus
Money transfer	SS	Aus
Fake job email or money transfer schemes	FIDO	Aus

Table 9: Scam genre 4



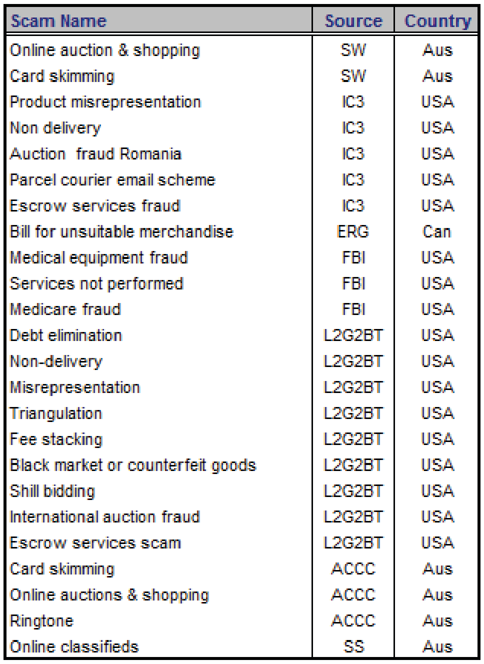
Scam Name	Source	Country
SMS competition & trivia	SW	Aus
Missed calls & text messages from unknown numbers	SW	Aus
Ring tone	SW	Aus
Modem jacking	SW	Aus
Superannuation	SW	Aus
Premium rate prize draw	OFT	UK
Property investment	OFT	UK
Internet dialer	OFT	UK
Bogus vanity publishers	OFT	UK
Bogus invention promotions	OFT	UK
Bogus model & casting agencies	OFT	UK
Loan scams	OFT	UK
Missed calls	ACCC	Aus
Text messages	ACCC	Aus
SMS competition & trivia	ACCC	Aus
Faxback	ACCC	Aus
Office supply	ACCC	Aus

Table 10: Scam genre 5



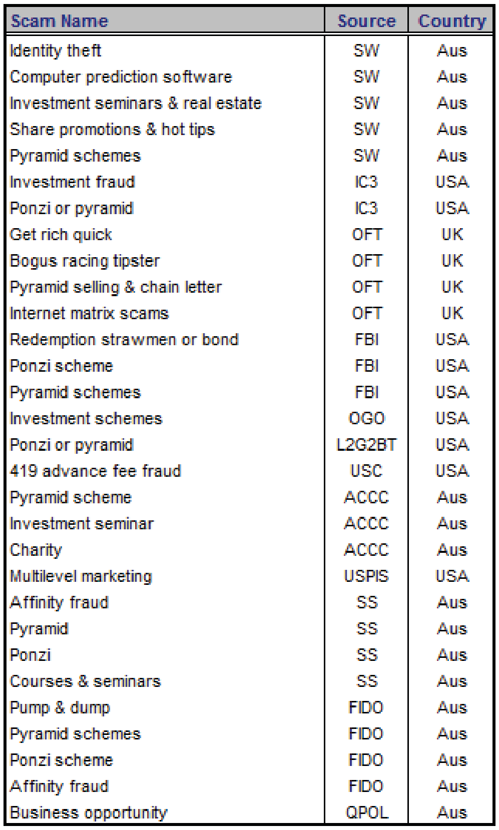
Scam Name	Source	Country
Spyware & key-loggers	SW	Aus
Free offers on the internet	SW	Aus
Credit card	SW	Aus
Phony fraud alerts	SW	Aus
Requests for account information	SW	Aus
Credit card fraud	IC3	USA
Debt elimination	IC3	USA
Identity theft	IC3	USA
Phishing & spoofing	IC3	USA
Spam	IC3	USA
Phishing & related	ABS	Aus
Identity theft	ABS	Aus
Impersonation or identity fraud	FBI	USA
Phishing	OGO	USA
Hacking	L2G2BT	USA
Identity theft	L2G2BT	USA
Phishing & spoofing	L2G2BT	USA
Spam	L2G2BT	USA
Spyware	L2G2BT	USA
Discount software offers	USC	USA
Phishing email	USC	USA
Trojan horse email	USC	USA
Virus generated email	USC	USA
Phishing	ACCC	Aus
Fake fraud alerts	ACCC	Aus
Spam	ACCC	Aus
Malicious software	ACCC	Aus
Identity theft	SS	Aus
Phishing	SS	Aus
Software	SS	Aus
Virus	SS	Aus
Trojan	SS	Aus
Ransom-ware	SS	Aus
Spyware	SS	Aus
Malware	SS	Aus
Fake bank emails	FIDO	Aus
Social networking fraud	FIDO	Aus
Identity theft	FIDO	Aus

Table 11: Scam genre 6



Scam Name	Source	Country
Online auction & shopping	SW	Aus
Card skimming	SW	Aus
Product misrepresentation	IC3	USA
Non delivery	IC3	USA
Auction fraud Romania	IC3	USA
Parcel courier email scheme	IC3	USA
Escrow services fraud	IC3	USA
Bill for unsuitable merchandise	ERG	Can
Medical equipment fraud	FBI	USA
Services not performed	FBI	USA
Medicare fraud	FBI	USA
Debt elimination	L2G2BT	USA
Non-delivery	L2G2BT	USA
Misrepresentation	L2G2BT	USA
Triangulation	L2G2BT	USA
Fee stacking	L2G2BT	USA
Black market or counterfeit goods	L2G2BT	USA
Shill bidding	L2G2BT	USA
International auction fraud	L2G2BT	USA
Escrow services scam	L2G2BT	USA
Card skimming	ACCC	Aus
Online auctions & shopping	ACCC	Aus
Ringtone	ACCC	Aus
Online classifieds	SS	Aus

Table 12: Scam genre 7



Scam Name	Source	Country
Identity theft	SW	Aus
Computer prediction software	SW	Aus
Investment seminars & real estate	SW	Aus
Share promotions & hot tips	SW	Aus
Pyramid schemes	SW	Aus
Investment fraud	IC3	USA
Ponzi or pyramid	IC3	USA
Get rich quick	OFT	UK
Bogus racing tipster	OFT	UK
Pyramid selling & chain letter	OFT	UK
Internet matrix scams	OFT	UK
Redemption strawmen or bond	FBI	USA
Ponzi scheme	FBI	USA
Pyramid schemes	FBI	USA
Investment schemes	OGO	USA
Ponzi or pyramid	L2G2BT	USA
419 advance fee fraud	USC	USA
Pyramid scheme	ACCC	Aus
Investment seminar	ACCC	Aus
Charity	ACCC	Aus
Multilevel marketing	USPIS	USA
Affinity fraud	SS	Aus
Pyramid	SS	Aus
Ponzi	SS	Aus
Courses & seminars	SS	Aus
Pump & dump	FIDO	Aus
Pyramid schemes	FIDO	Aus
Ponzi scheme	FIDO	Aus
Affinity fraud	FIDO	Aus
Business opportunity	QPOL	Aus

Acknowledgment

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

References

[1] G., Wahlert, "Crime in cyberspace: Trends in computer crime in Australia," presented at the Internet Crime Conference, Melbourne, Australia, 1998.

[2] A., Stabek, S., Brown, and P., Watters, "The case for a consistent cyberscam classification Framework," in First Cybercrime and Trustworthy Computing Workshop, 2009.

[3] Australian Centre for Policing Research and the Australian Transaction Reports and AnalysisCentre Proof of Identity Steering Committee, "Standardisation of definitions of identity crime terms: A step towards consistency," 145.3, Commonwealth of Australia, 2006.

[4] Australian Bureau of Statistics, "Personal fraud, 2007," No. 4528.0, Australian Capital Territory, 2008.

[5] Parliamentary Joint Committee on the Australian Crime Commission, "Cybercrime," Australian Capitol Territory, 2004.

[6] H., Hays, and T., Prenzler, "Profiling fraudsters Queensland case study in fraudster crimes," Final Report to Crime Prevention Queensland, 2002.

[7] K.R., Choo, R.G., Smith and R. McCusker, "Future directions in technology-enabled crime: 2007-2009," the Australian Institute of Criminology, No. 78, Australian Capitol Territory, 2007.

[8] Internet Crime Complaint Center, "2007 Internet Crime Report," USA: National White Collar Crime Center, Bureau of Justice Assistance, and the Federal Bureau of Investigation, 2008.

[9] Internet Crime Complaint Center, "2008 Internet Crime Report," USA: National White Collar Crime Center, Bureau of Justice Assistance, and the Federal Bureau of Investigation, 2009.

[10] Model Criminal Law Officers' Committee of the Standing Committee of Attorneys – General, "Final report on identity crime," Australian Capital Territory, 2008.

[11] United Kingdom Office of Fair Trading, "Research on the impact of mass marketed scams," OFT883, Crown Copyright, 2006.

[12] H., Chen, W., Chung, J.j., Xu, G., Wang, Y., Qin, and M., Chau, "Crime data mining: A general framework and some examples," IEEE Computer Society, pp 50-56, 2004.

[13] G., Farrell, K., Clark, D., Ellingworth and K., Pease, "Of targets and supertargets: A routine activity theory of high crime rates," The Internet Journal of Criminology, 2005. Available: www.internetjournalofcriminology.com [Accessed March 2, 2009].

[14] K., Choi, "Computer crime victimization and integrated theory: An empirical assessment," International Journal of Cyber Criminology, volume 2, No. 1, pp. 308 – 333, 2008.

[15] A., Stabek, "The effectiveness of using static features in identifying scam genres," M.M.S thesis, University of Ballarat, Ballarat, Australia, 2010.