International Journal of Cyber Criminology
Vol 1 Issue 1 January 2007

A Qualitative Analysis of Advance Fee Fraud E-mail Schemes

Thomas J. Holt[1]
Danielle C. Graves[2]
University of North Carolina, Charlotte, USA

Abstract

Criminals utilize the Internet to perpetrate all manner of fraud, with the largest dollar losses attributed to advance fee fraud e-mail messages. These messages come from individuals who claim to need assistance moving a large sum of money out of their country. Individuals who respond to the messages often become victims of fraud and identity theft. Few criminologists have examined this type of fraud, thus this study explores the mechanisms employed by scammers through a qualitative analysis of 412 fraudulent e-mail messages. The findings demonstrate that multiple writing techniques are used to generate responses and information from victims. Half of all the messages also request that the recipient forward their personal information to the sender, thereby enabling identity theft. The implications of this study for law enforcement and computer security are also discussed.

Keywords: E-mail; Fraud; Victims; Computer Security; Techniques;

Introduction

Criminals utilize the Internet to perpetrate all manner of fraud, with the largest dollar losses attributed to advance fee fraud e-mail messages. These messages come from individuals who claim to need assistance moving a large sum of money out of their country. Individuals who respond to the messages often become victims of fraud and identity theft. Few criminologists have examined this type of fraud, thus this study explores the mechanisms employed by scammers through a qualitative analysis of 412 fraudulent e-mail messages. The findings demonstrate that multiple writing techniques are used to generate responses and information from victims. Half of all the

[1] Assistant Professor, Department of Criminal Justice, 5069 Colvard, The University of North Carolina at Charlotte, 9201 University City Blvd.,Charlotte, NC 28223, USA., Email:tjholt@uncc.edu
[2] Department of Software and Information Systems, 341 Woodward Hall, The University of North Carolina at Charlotte, 9201 University City Blvd., Charlotte, NC 28223, USA. Email:dcgraves@uncc.edu

messages also request that the recipient forward their personal information to the sender, thereby enabling identity theft. The implications of this study for law enforcement and computer security are also discussed.

A significant amount of criminological research has explored the prevalence and incidence of fraud, where criminals gain property or money from victims through deception or cheating (e.g. Baker and Faulkner, 2003). Most fraud involves some type of interaction between the victim and the offender, either through face-to-face meetings (Kitchens, 1993; Knutson, 1996) or telephone based exchanges (Stevenson, 1998). As individuals around the world increasingly depend on the Internet and computer mediated communications, criminals have begun to use this medium to commit fraud (Wall, 2001; Grabowski, Smith, and Dempsey, 2001). Electronic communications afford tremendous opportunities for criminals to connect with a large population of potential victims cheaply and efficiently (Savona and Mignone, 2004).

There are several different types of fraud that are perpetrated on-line, including electronic auction or retail-based fraud schemes, stock scams, and work-at-home plans (Grabosky et al., 2001; Newman and Clarke, 2003). However the most costly form of Internet fraud are advance fee e-mail schemes (National White Collar Crime Center and the Federal Bureau of Investigation, 2006). These messages are often referred to as "Nigerian" or "419" scams because the e-mails often come from individuals who claim to reside in a foreign country such as Nigeria or other African nations (see Smith, Holmes, and Kaufmann, 1999, p. 2). The sender claims to need assistance transferring a large sum of money out of their country. In return, the sender will share a portion of the sum with the individual who aids them.

A massive amount of advance fee fraud messages are sent out every day around the world, though many recipients ignore or discount their content. At the same time, a small percentage of all recipients respond to these messages and become victims who lose money or have their identities stolen at the hands of fraudsters (see Edelson, 2003). In fact, victims of advanced fee fraud e-mail scams in the United States lost an average of $5000 in 2005 (National White Collar Crime Center and the Federal Bureau of Investigation, 2006). Furthermore, fraudulent e-mails have cost individuals and businesses around the world

approximately one billion dollars in the past decade (Taylor, Caeti, Loper, Fritsch, and Liederbach, 2006, p. 112).

Despite the significant impact that this type of fraud can have on victims, few criminologists have explored the structure or content of advance fee fraud messages. There may be patterns in the message syntax or phraseology that increase the likelihood that victims will respond to the sender. Also, the schemes used by scammers may change rapidly due to the speed afforded by computer-mediated communications. This study explores the mechanisms employed by scammers through a qualitative analysis of 412 fraudulent e-mail messages received at two universities over a two and a half year period. The findings are used to improve our knowledge of Internet-based fraud and identity theft, and help inform law enforcement and computer security policy.

Advance Fee Fraud Schemes

Advance fee fraud or Nigerian e-mail scams initially appeared as handwritten letters in postal mail or faxes in the 1980s (United States Department of State, 1997). These scams became propagated via e-mail in the early 1990s as individuals around the globe adopted e-mail technology. In the past decade, advanced fee schemes were labeled as spam, or unsolicited bulk e-mails with multiple messages that offer illicit or counterfeit services and information (Wall, 2004). Since over half of all the e-mail traffic directed toward commercial entities today constitutes spam, these messages are a nuisance for computer users (see Gartner Group, 2003). Software and hardware filters have been developed to limit the amount of spam that actually reaches end users (Moustakas, Ranganathan, and Duquenoy, 2006; Edelson, 2003). These filters use parameters to identify and sort out advanced fee fraud messages on the basis of dollar values placed within messages, and subject lines (see Edelson, 2003). Though filtering programs have some success, they do not completely eliminate all spam from e-mail inboxes. In fact, a substantial number of individuals still receive and fall victim to advance fee fraud e-mail scams around the world. Thus, there is some need to consider how these messages are structured to better understand the methods of e-mail fraudsters.

Recent research by Edelson (2003) identified a few common themes used by fraudsters (p. 393). One of the more popular variations involves the sender posing as a public official who has been able to

skim funds from a business or government contract (Edelson, 2003, p.393). The official is making contact to help get the money they illegally obtained out of an account. A similar scheme takes the form of a banker trying to close a dead customer's account using the potential victim as the deceased's next of kin (Edelson, 2003, p.394). A third variation of this scam involves the sender acting as the relative of a deceased military or political figure who is trying to claim an inheritance (Edelson, 2003, p. 394). Other adaptations have been identified, though the majority of scams implicate the sender in some form of illegal behavior. In turn, the sender attempts to ensnare the recipient in this illicit, yet ultimately false, transaction.

Should an individual receive and respond to one of these messages, anecdotal evidence suggests the sender can defraud their victim in one of three ways (see Edelson, 2003). One method involves inviting the victim to visit the scammer in their "home" country to explain their situation in person and ask for money and assistance. This ploy is relatively uncommon, though it can lead the victim to be held hostage or killed (Edelson, 2003). Another technique employed by scammers is to slowly drain funds from their victims over time (Smith et al., 1999, p. 4). This process begins with the scammer asking their potential victim for a small donation to get an account or fund out of a holding process. The scammer then continues to receive payments from the victim because of "complications" in obtaining their account. (Smith et al., 1999, p. 4). This process continues until the victim is no longer willing to pay, and generates a significant dollar loss for the victim. A final method requires the victim to provide the scammer with personal information, such as their name, address, employer, and bank account information. The initial request may be made under the guise of assuring the sender that the recipient is a sound and trustworthy associate (Edelson, 2003). However the information is surreptitiously used by the sender to drain the victim's accounts and engage in identity theft.

Regardless of the method used, victims may not report their experience to law enforcement agencies. Some victims may be reticent to report the incident out of fear they will be prosecuted for their involvement in the illegal act described in the initial message they received (Buchanan and Grant, 2001). Victims may also feel too embarrassed to report that they lost money by simply responding to an e-mail message (Buchanan and Grant, 2001). As a result, it is unknown

how many individuals actually receive, respond to, and are defrauded through advance fee e-mail scams.

There is also limited knowledge on the reasons individuals respond to fraudulent e-mail messages. Since it is difficult to gain access to the victims of this type of fraud, examining the structure and persuasive language employed in these scams may provide insight into why individuals respond to these messages. There may be certain themes or phrases that commonly appear that may be used to elicit a response from potential victims. The senders may utilize unique phrases that lend credibility to their story or message. The dynamic nature of the electronic communications may also allow the senders to link their story to current events, thereby increasing the credibility of their story. Thus, there is a strong need to examine advanced fee fraud messages to improve our understanding of the methods used to defraud individuals. In turn, this can improve our knowledge of the ways that criminals use the Internet to engage in fraud.

Data and Methods

This study examines a sample of 412 e-mail messages received in two e-mail accounts at two medium-sized state universities. These messages constitute spam, as they were not requested or sent from any individual known to the researcher. The e-mails were received at all hours of the day, every day of the week, and each month. In fact, there were no specific correlations between the days, dates, or times the messages were received.[3]

The messages appeared to have been generated from 121 different public and private e-mail providers around the world. The domains of these accounts also seem to come from a number of countries around the world, including Italy, the UK, China, Zaire, and Russia. Yet, the originating e-mail addresses in the messages may not be accurate, as this information can be "spoofed" or falsified (Moore, 2005, p. 40).[4] As a result, it is not possible to accurately identify where this sample of messages originated. However, this does not limit the

[3] The day, date, and time stamp of each message were entered into SPSS to determine if there were any relationships between these variables. However, no statistically significant correlations or relationships identified through crosstabs or bivariate correlation tests.

[4] The header and footer of each e-mail must be examined in order to determine the country of origin and e-mail account associated with each message. Specialized software is required to generate this information from Microsoft Outlook software which could not be obtained due to budget restrains. As a result, the originating information for each message was not available at this time.

analyses since the focus is on the structure and content of fraudulent messages rather than their point of origin.

It is also important to note that both universities utilize filtering technology to reduce the volume of spam e-mail that users receive on a daily basis.[5] As such, the messages received in the two accounts represent a small percentage of all the spam e-mail sent to these institutions. This is an important limitation, since this sample may not be representative of all fraudulent e-mails currently circulating on-line. However, e-mails that can pass through filtering technology are more likely to reach multiple users, increasing their likelihood of victimization. Thus, this data constitutes a convenient, yet purposive sample of advance fee fraud e-mails currently circulating on-line.

As each message was received, it was downloaded from the inbox and saved as a word file. Then the messages were printed, analyzed, and coded by hand using grounded theory techniques (Corbin and Strauss, 1990). This method requires data collection and analyses to proceed at the same time, enabling the research to perform a rigorous qualitative analysis. Specifically, grounded theory methodology uses a three stage coding process to develop categories and patterns in the data that must be identified multiple times through comparisons to determine if they similar. In this way, concepts become relevant via repeated appearances or absences in the data, ensuring they are derived and grounded in the "reality of data" (Corbin and Strauss, 1990, p. 7).

For example, message categories were created on the basis of the stated credentials of the sender and their reason for making contact with the recipient. Since most of these messages involved some form of fixed fee transfer, the position or title of the sender, such as banker, attorney, doctor, or government agent, were used as a primary means of categorization. However, if the sender provided no detail on their credentials, their reason for contacting the recipient was used to categorize the message. For example, e-mails from individuals seeking assistance to make consignment transfers, invest in foreign companies, or establish businesses in the US were placed into their own discrete category. This strategy provided a great deal of flexibility and

[5] Both universities in this sample use software filters that block inbound e-mail traffic based on certain criteria, including infected e-mail attachments, image analyses, and known spam headers. One university also uses Geo-IP blocking, where e-mails from specific IP addresses are immediately blocked due to their consistent spam traffic. Thus, these institutions attempt to limit the amount of spam end-users receive on a regular basis.

specificity to classify messages into categories based on their content rather than any existing typology of advance fee fraud schemes. Thus, grounded theory techniques are used to structure the following analysis of the content and structure of advanced fee fraud e-mail, using quotes from the data set when appropriate.

The Scam Types

Multiple fraud schemes were received across both accounts over the data collection period (see Table 1). As stated previously, most of these messages were from individuals requesting assistance to transfer a fixed amount of money into the recipient's bank account. For example, 124 of the emails (30 percent) involved fixed fee transfers from individuals claiming to be bankers. A smaller percentage (5.8 percent) purported to be barristers seeking assistance to obtain funds from a deceased client (see also Edelson, 2003). A number of messages were also received from individuals claiming to be government agents that have over-drafted a business contract (see also Edelson, 2003). The senders need someone to act as the recipient of the over-drafted amount and assist in getting the funds out of their country. Thirty six (8.7 percent) messages were sent from individuals who say they were the children of deceased wealthy diplomats or merchants. These messages involve an individual whose parents left them a significant amount of money, but who are unable to access the funds and may lose it to their living relatives. As a result, they are requesting help to transfer funds out of the country.

There were also a number of messages from international lottery agencies stating that the recipient had won. Fifty seven business solicitations (13.8 percent) were sent from international companies seeking assistants to receive and cash payments from business clients. A very small number of messages (5.1 percent) were also sent from people claiming to have a terminal illness. The senders wanted to transfer funds from their bank accounts to the recipient for donation to religious charities around the world. A number of other types of fraudulent messages were received, though most all of these messages revolve around fixed fee transfers.

Table:1
Types of scams received :

Scam Type	University 1	University 2	Total	%
Business Solicitation	13	44	57	13.80%

Fixed Fee Transfer from Bank	41	83	124	30.00%
Fixed Fee Transfer from Barrister	2	22	24	5.80%
Over-drafted Contract	7	20	27	6.50%
Charity Message	5	16	21	5.10%
Lottery Message	6	31	37	8.90%
Fixed Fee from Government	6	11	17	4.10%
Fixed Fee from Citizen	11	25	36	8.70%
Investment	2	8	10	2.40%
Banking Transaction	2	1	3	0.70%
Fixed Fee Transfer to Account	5	5	10	2.40%
Fixed Fee Transfer for Investments	3	17	20	4.90%
Consignment Transaction	6	17	23	6.00%
Fixed Fee from Diplomat	0	3	3	0.70%
Total Messages Received	108	304	412	100.00%

Message Structure and Content

Examining the content of the messages received across both accounts demonstrates several common elements were present. For example, scammers used language in the subject line of the message that may entice recipients to open the e-mail. Some used language with a critical and serious tone, such as "Urgent Attention" or "Read and Reply As Soon As Possible." Other messages used cordial phrases, such as "Attention Friend," or announced the sender with statements like "From Dr. Mrs. Mariam Abacha." Lottery notifications typically employed expressions such as "Congratulations" or "Attention Winner," while business messages used expressions like "Payment Agent Needed." A few messages had no subject, providing little indication regarding what the message may contain.

The body of these messages illustrates the phrasing and syntax used by scammers. Specifically, the messages did not typically contain a gender specific greeting, such as "dear sir." Instead, the majority (92.5 percent) used gender neutral or non-specific language, such as "dear sir/madam" or "dear friend." A small number also used a religious greeting, such as "blessed one in Christ." Some messages eschewed a formal greeting altogether and moved directly into the contents of the message. Using a vague greeting or none at all benefits the sender, since the messages are sent out in batches to unknown recipients. A cordial greeting that makes the recipient feel special or emotionally linked to the sender may also increase the likelihood of a response.

The main content of the e-mails provided information on the sender and their reason for contacting the recipient. The majority (75

percent) of messages were sent by individuals claiming to be male, and employed as a bank manager, attorney, or doctor. For example, e-mails from bankers began with sentences such as, "I am Mr. Ben Ani, a consulting auditor, Financial Trust bank, Lagos Nigeria." Business solicitations began with statements including "I am Mr. Yeo Mao Cheng, Managing Director of Matroc Technical Ceramics Co. Ltd." However, some individuals gave no indication of their credentials. Approximately 25 percent of the e-mails provided a physical business address for the sender, despite the significant number of messages from bankers, government agents, or barristers. The senders may intentionally keep this information out of the messages because they are concerned about their involvement in potentially illegal activities.

Most of these messages (75 percent) also gave no indication of how the sender identified the recipient. Instead, some simply stated that the message was sent because the recipient is a foreigner. For example scammers used language such as "our assistance as a foreigner is necessary because the management of the bank will welcome any foreigner who has correct information to the account which I will give to you immediately." Lottery messages provided a different explanation, stating that the recipient's information was "selected Through [sic] a computer ballot system drawn From over 20,000.00 companies and 3,000,000 individual Email addresses and names from all over the world." A small percentage of messages (18 percent) indicated that the sender found information about the recipient on-line with language such as "I the came across your address on the Internet as I was searching for a reliable and honest person." However, the majority of messages explained the senders' predicament with little exposition on how or why they identified the recipient.

Since many of the messages described a desire to transfer funds through the recipient, the senders detailed the dollar amounts involved. For example, a message from a government agent in Nigeria stated:

> 'I am in search of an agent to assist us in the transfer of Twenty Million United State [sic] Dollars (USD20M) and subsequent investment in properties in your country. . . If you decide to render your service to us in this regard, 40% of the total sum of Twenty million United State Dollars (USD20M) will be for you.10% for any expense that may incur (both parties) during processing for the transfer to your nominated bank, while 50% for me and other officials.

Similar language was present across eleven of the types of scams received with dollar figures ranging from $90,000 to $423,000,000, though the amount was most often in the millions. Recipients who assist the sender were entitled to receive a portion of the total amount, most often between 10 and 40 percent of the total sum. The money involved may be a significant and attractive benefit for the message recipient, as a person could become extremely wealthy by assisting the sender (see also Buchanan and Grant, 1999). Most of the e-mails described leaving five to ten percent of the total amount set aside for expenses during the transfer process and, in some cases, charity.

Two scam types differed from this common pattern. Messages offering the recipient a job do not describe the funds involved, but state that "subject to your satisfaction you will be given the opportunity to negotiate your mode of payment for your services." This statement appears almost verbatim across all business solicitation messages. Similarly, lottery scheme messages indicate that the recipient has won and will receive the entire amount that is described, as in this excerpt from a UK based lottery scam:

> 'You have therefore been approved for a lump sum pay of US$2,800.809.00. (TWO MILLION EIGHT HUNDRED THOUSAND, EIGHT HUNDRED AND NINE UNITED STATES DOLLARS ONLY).This is from a total cash prize of US$70,020.225.00, shared among the (25) twenty-five international winners in this category.

In order to collect or receive the funds described, the recipient must contact the sender in some fashion. Almost all of the messages ask that the recipient contact them by phone or e-mail. However, the e-mail address they provide is often different from the originating e-mail account, stating "reply through my private box" or "send mail to my private e-mail account." Many senders (47 percent) stated this is due in large part to the need for confidentiality since most all of the schemes involved money that was supposedly obtained through illicit means. Senders described concern that they may lose their job or be caught by law enforcement, thus they included statements like "treat as strictly confidential" or "observe utmost discretion in all matters concerning this issue." A limited number of messages provided a much more professional statement on confidentiality:

'The total content of this e-mail is intended only for the person or entity to which it is addressed and may contain confidential and/or

privileged [sic] material. If you are not the intended recipient of this message you are hereby notified that any use, review, retransmission, dissemination, distribution, reproduction whether orally or through any other media and/or any action taken upon this message is prohibited.'

In addition to confidentiality, the senders requested that they be contacted as quickly as possible in 83 percent of all the messages. By rapidly replying to the message, the sender could begin to process paperwork or start to transfer funds. However, many messages demand that the recipient provide more than just a "yes" or "no" response to the request. Half of the e-mails received ask the recipient to provide them with personal information (see also Edelson, 2003). The most commonly sought information included the recipient's name, phone number, and address, though some also asked for employment and bank account information. Senders attempted to justify these requests, often to establish alternative means of communication, suggesting "Please include your private telephone and fax numbers in your reply for easy communication." Bank or barrister-based messages often suggested they needed this information to develop and process paperwork, like in this excerpt:

> "All the information needed to claim the funds would be sent to you as soon as you indicate your interest in assisting them as well as providing the following information to facilitate the smooth conclusion of the transaction."
>
> 1) Your Full Name:
>
> 2) Your Address:
>
> 3) Your Telephone Number:
>
> 4) Your Fax Number:
>
> 5) Your Mobile Number:
>
> 6) The Name of the Closest Airport to your City of Residence:
> 7) Your Age:

However, not all messages requested information from the recipient. Instead they simply ask that the individual contact them as soon as possible to state whether or not they would like to help them.

Writing Techniques

Since many of these schemes involve some form of illegal behaviour, the senders attempt to mitigate the risks involved for the e-mail recipient. Many messages indicate that the transfer scheme is safe and will be legally binding, using language like "this transaction is totally free of risk and troubles," or "this will be a proper and legal money transfer and there is no risk!" In a similar fashion, the senders in bank or barrister-related scams often make the following statement:

> 'All legal documents to back up your claim as the deceased Next of Kin will be provided. All I require is your honest cooperation to enable us seeing this deal through. I guarantee that this will be executed under a legitimate arrangement that will protect you from any breach of the law and you should endeavor to keep it confidential.'

Some scams make it a point to state that they are seeking out trustworthy, honest, or reliable persons to aid in their efforts. Thus, they have contacted you for assistance because the sender knows "you will not let me down."

Scammers also linked their stories to current events in an attempt to increase the plausibility of the scam. The claims made depended on the scam, though individuals commonly referenced recently deposed military or government officials as well as the Iraq war. For example, a woman seeking aid to move funds out of Nigeria claimed "my late father was deputy minister of public works in the administration of our former president Charles Taylor who is now in exile after killing many innocent souls." In bank and barrister related messages, senders claimed to have clients who died in plane crashes or natural disasters. To further validate their claims, a limited number of messages (15.2 percent) provided web links to news stories or web sites. For example, a bank officer used the following language and working web link to justify his story:

> 'From my section in the bank, I discovered an abandoned sum of EIGHTEEN MILLION FIVE HUNDRED THOUSAND UNITED STATED DOLLARS ($18.5m) that belongs to one of our customer who died along with his entire families, on 25TH JULY,2000 CONCORDE PLANE CRASH[Flight AF4590] with the whole passengers aboard. . .
>
> N.B. in other for you to believe me honestly, go through this (website)before you start with me.
>
> Below is the website.

http://news.bbc.co.uk/1/hi/world/europe/859479.stm.'

Religious language is also employed in some of the messages which may evoke an emotional or spiritual response from the victim. For example, some messages began with a greeting such as "greetings in the name of our Lord Jesus Christ." Charity messages typically detail how the sender lost their spouse, became a born again Christian, and are now dying. These scams commonly referenced the Biblical passage Exodus 14; 14, using the language "the lord will fight my case and I shall hold my peace." A small percentage of banking or governmental schemes also mention how fasting and prayer brought you to their attention or that they have faith in God that you will not let them down. Some bring in religious sentiments in the closing statement of their message, such as "May the Grace of our Lord, the love of God is with you" or "Yours in Christ."

Errors were also commonly found in these messages (81.3 percent), ranging from simple misspellings to serious grammatical errors. Common errors included inappropriate capitalization, such as "this over Invoiced sum," or frequent, unnecessary use of commas. Run on sentences, odd phrases, and misspelled words were also present in many messages, as in the following excerpt from a lottery notification message:

> 'We are please to announce you as one of the 10 lucky winners in the Free Lotto draw held on the 20th of September. . .Consequently, you have therefore been approved for a total payout of USD$ 2,000,000,00 (TWO MILLION DOLLARS) only. Your email address emerged along side 9 others as a category to the winners in this year's Annual Lottery Program which will be held [sic] once every year till the 2010 finals in South Africa.'

Though grammatical errors may detract from the professional appearance of a message, they may be intentional on the sender's part. Since the many of the senders claimed to reside in Nigeria, South Africa, or other African states (42.3 percent), spelling and punctuation errors may reinforce the notion that the sender is a foreigner who is unfamiliar with English.

Discussion and Conclusions

This analysis sought to explore the content and methods employed in advanced fee fraud e-mails. The findings suggest that fraudsters employ deceptively simple messages in an attempt to

identify and victimize individuals. They utilize unique phrases throughout each e-mail to increase the plausibility of their messages and likelihood of responses. For example, most messages have an enticing subject line that may compel an individual to open the e-mail. The body of the e-mail allows the scammer to create a false impression of professionalism by providing business credentials and statements about the need for trust and confidentiality. The sender may also increase the plausibility of their claims by tying the story to current events, or through the use of religious phrases or emotional language in the message. In addition, the senders commonly describe having a large sum of money that must be transferred to a new bank account. The recipient will receive a significant amount of this fund if they ensure the transfer is successfully completed. The promise of fast, easy money may compel many recipients to respond to these messages. In this way, advance fee fraud schemes share similar features with real world confidence games. Each requires the swindler to convince their victim to engage in a transaction that appears believable and beneficial (Leff, 1976; Prus and Sharper, 1977).

However, individuals who respond to advance fee fraud messages are at great risk for identity theft and financial loss. Half of the messages in this sample require the recipient to provide the sender with their personal information, including name address, and phone numbers (see also Edelson, 2003). Obtaining personal information appears to be the key purpose of fraudsters' e-mail contact, as they can then engage in identity theft or drain victim bank accounts. Thus, advance fee fraud messages are an excellent mechanism for criminals to anonymously reach a number of potential victims quickly and efficiently.

In fact, the consistent patterns identified in the syntax and phraseology of the messages received at both institutions supports the notion that fraudsters employ scripts or templates to rapidly generate fraudulent e-mails (see Edelson, 2003). Once a scheme is created, it is used as a template and the names, locations, and amounts involved are changed for each new message. This allows for multiple messages to be distributed with little effort or output on the senders' part. These scripts may also be loaded into the payload of malicious software, such as bots, to automate the creation and distribute spam (see Wall, 2004; Wood, 2004). However, there are few criminological explorations of the connections between malware, spam, and fraud. Research is needed

examining the ways fraudulent e-mail messages are distributed and acted upon by criminals. This information can benefit law enforcement and computer security professionals in developing better strategies to combat spam and cybercrime.

Research is also needed to identify ways to reduce the number of fraudulent e-mails that people receive. The risk of fraud victimization is very high due to the large amount of spam e-mail traffic on-line today. In fact, many fraudulent messages were received in each of the e-mail accounts used for this research despite the presence of e-mail filtering technology. If better filtering mechanisms could be developed, it may minimize the potential for fraud victimization. Considering the patterns and commonalities identified in this research, it may be useful to create filtering parameters based on common phrases in advance fee fraud scheme e-mails (see Edelson, 2003). For example, phrase-based blocking on specific terms such as "this transaction is completely risk free" and "all legal documents to back up your claim as Next Of Kin will be provided" may eliminate a greater proportion of these messages from inboxes. Such a strategy may prove useful to keep a higher percentage of fraudulent messages from reaching potential victims.

At the same time, there is no real likelihood that advance fee e-mails will ever be completely eliminated. The creation of anti-spam laws such as the CAN-SPAM Act of 2003 in the United States and international directives by the European Union have had little impact on the volume of e-mails sent out daily (Wall, 2004, p. 321). There is also no easy way to identify the fraudsters responsible for these messages due to the use of spoofing and anonymizing software that conceals an individual's location. Thus, it is difficult for law enforcement agencies to effectively deal with spam. Yet, it may be possible to minimize fraud victimization through public awareness campaigns on the threat of advance fee fraud schemes. Internet Service Providers (ISPs) and institutional e-mail service providers could provide effective and simple messages on the dangers of responding to claims made in unsolicited e-mails. Empirical research on the correlates of advance fee fraud victimization may also assist in reducing the incidence of fraud overall. Identifying any connections between victims characteristics such as age, computer familiarity, or reading comprehension can provide some insight into why individuals respond to these messages (see also Edelson, 2003). The findings could be used

to deliver targeted fraud awareness programs to reduce the likelihood of fraud victimization.

Taken as a whole, this study has demonstrated the considerable role that computer mediated communications can play in facilitating fraud. The Internet and e-mail enable fast, efficient contact with a huge number of potential victims while concealing the criminals' identity. As a result, individuals are at risk from all sorts of deception and fraud over the Internet. However, advance fee e-mail scams are just one part of the much larger spectrum of fraud that occur on-line (Taylor et al., 2006). Scammers can sell fraudulent products through on-line retail and auction websites, as well as utilize e-mail to artificially inflate stock prices or obtain banking information from individuals via "phishing" (Taylor et al., 2006, p. 138). Thus, it is imperative that researchers consider the ways that fraud changes in tandem with the dynamic nature of the Internet. This will improve our understanding of the ways the Internet acts as a conduit for crime in the 21st century.

Acknowledgement

The authors would like to thank Joe Kuhns, Bill Chu, and the anonymous reviewers for their helpful comments on previous drafts of this manuscript.

REFERENCES

Baker, W. E., and Faulkner, R. R. (2003). Diffusion of fraud: Intermediate economic crime and investor dynamics. *Criminology,* 41(4), 1173-1206.

Buchanan, J., and Grant, A. J. (2001). Investigating and Prosecuting Nigerian Fraud. *United States Attorneys' Bulletin,* November, 29-47.

Corbin, J., and Strauss, A. (1990). Grounded Theory Research: Procedures, Canons, and Evaluative Criteria. *Qualitative Sociology,* 13, 3-21.

Edelson, E. (2003). The 419 scam: Information warfare on the spam front and a proposal for local filtering. *Computers and Security,* 22(5), 392-401.

Furnell, S. (2002). Cybercrime*: Vandalizing the Information Society.* Boston, MA: Addison-Wesley.

Gartner Group. (2003). *Gartner says marketers must differentiate e-mail marketing from spam.* Retrieved July 14, 2006 from, www4.gartner.com/5_about/press_releases/pr29sept2003a.jsp

Grabowski, P., Smith, R. G., and Dempsey, G. (2001). *Electronic Theft: Unlawful acquisition in cyberspace* Cambridge, England: Cambridge University Press.

Jewkes, Y., and Sharp, K. (2003). Crime, deviance and the disembodied self: transcending the dangers of corporeality. In Y. Jewkes (Ed.), *Dot.cons: Crime, deviance and identity on the Internet* (pp. 1-14). Portland, OR: Willan Publishing.

Kitchens, T. L. (1993). The cash flow analysis method: Following the paper trail in Ponzi schemes. *FBI Law Enforcement Bulletin*, August,10-13.

Knutson, M. C. (1996). The Remarkable Criminal Financial Career of Charles K. Ponzi. Retrieved August 21, 2006 from http://www.usinternet.com/users/mcknutson

Leff, A. (1976). *Swindling and Selling.* New York: Free Press. Moore, R. (2005). *Cybercrime: Investigating high-technology computer crime.* Lexis Nexis Anderson Publishing.

Moustakas, E., Ranganathan, C., and Duquenoy, P. (2006). E-mail marketing at the crossroads: A stakeholder analysis of unsolicited commercial e-mail (spam). *Internet Research*, 16(1), 38-52.

National White Collar Crime Center and the Federal Bureau of Investigation. (2006). *IC3 2005 Internet Crime Report.* Retrieved on 24.05.2007,from:http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf

Newman, G. R., and Clarke, R. V. (2003). Superhighway *Robbery: preventing e-commerce crime.* Portland: William Publishing.

Prus,R., and C.R.D.Sharper.(1977). *Road hustler: The career contingencies of professional card and dice hustlers.* Lexington, MA: Lexington Books.

Savona, E. U., and Mignone, M. (2004). The Fox and the hunters: How IC technologies change the crime race. *European Journal on Criminal Policy and Research,* 10(1), 3-26.

Smith, R. G., Holmes, M. N., and Kauffman, P. (1999). *Trends and issues in crime and criminal justice No. 121: Nigerian Advance Fee Fraud.* Australian Institute of Criminology; Retrieved on 15.01.2005:http://www.aic.gov.au/publications/tandi/ti121.pdf

Stevenson, R.J. (1998). *The Boiler Room and Other Telephone Scams.* Champagne: University of Illinois Press.

Taylor, R.W., Caeti, T.J., Loper, D.K., Fritsch, E.J., and Liederbach, J. (2006). *Digital Crime and Digital Terrorism.* Upper Saddle River, NJ: Pearson Prentice Hall.

United States Department of State. (1997). Nigerian *Advance Fee Fraud.* Bureau of International Narcotics and Law Enforcement Affairs.

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (Ed.), in *Crime and the Internet* (pp. 1-17). New York: Routledge.

_____ (2004). Digital realism and the governance of spam as cybercrime. *European Journal on Criminal Policy and Research*, 10, 309-335.

Wood, P. A. (2004). *Spammer in the works: Everything you need to know about protecting yourself and your business from the rising tide of unsolicited "spam" e-mail.* A Message Labs White Paper, April. Retrieved February 10, 2006 from: http://www.security.iia.net.au/downloads/spammer%20in%20works%20-%20an%20update%2014.5.pdf