Finding a Pot of Gold at the End of an Internet Rainbow: Further Examination of Fraudulent Email Solicitation

Johnny Nhan[1], **Patrick Kinkade**[2], **& Ronald Burns**[3]
Texas Christian University, USA

Abstract

The amount of Internet spam has grown exponentially over the last decade. While much of this unsolicited email is harmless advertising, a growing proportion of it is insidious in nature and fraudulent in intent. The current research assesses the nature of this type of criminal approach. Two email accounts captured a total of 476 unsolicited emails identified as suspect in intent over a three month period. The researchers analyzed the nature of the solicitation, the nature of the solicitor, and the information asked of the target. Initial findings suggest relationship-building social engineering methods are preferred over direct inquiry of sensitive information. A descriptive analysis is provided and policy implications are discussed.

Keywords: Internet Spam; Unsolicited emails; Harmless advertising

Introduction

New technologies such as the Internet have radically changed the means by which society communicates, conducts business, and engages in recreation. The speed and convenience of the Internet has attracted a critical mass of global users. For the same reasons, Internet transgressors adopted the medium as a new avenue for crime. Many scholars consider the Internet as a medium for crime which consists of the same legal elements and motivations as conventional or street crimes (Brenner, 2001; Grabosky, 2001; Yar, 2005). However, the proliferation of cybercrime indicates that the Internet medium has outstripped traditional forms of social control. First, formal social control institutions rooted in static organizational design and legal tradition lack the appropriate flexibility and resources to deter online fraudulent activities (Wall, 1999, 2000; Walker, Wall, & Akdeniz, 2000; Burns, Whitworth, & Thompson, 2004). Second, the relative anonymity of computer crime and the ability to commit crime from a safe distance are but a few of the attractive features of computer crime that have contributed to its proliferation

[1] Assistant Professor, Department of Criminal Justice, Texas Christian University, Box 298720, Fort Worth, Texas 76129, USA. Email: j.nhan@tcu.edu
[2] Associate Professor, Department of Criminal Justice, Texas Christian University, Box 298720, Fort Worth, Texas 76129, USA. Email: r.burns@tcu.edu
[3] Associate Professor, Department of Criminal Justice, Texas Christian University, Box 298720, Fort Worth, Texas 76129, USA. Email: p.kinkade@tcu.edu

(Wall, 2001; Grabosky, 2004). Third, users often resist forms of social control imposed on the Internet as an affront to its ethos of unrestricted openness and unfettered exchange of ideas and information (Hafner & Markoff, 1995; Levy, 2001; Lasica, 2005; Lessig, 2005). Nonetheless, the "dark side" of the Internet, representing undesirable activities ranging from the invasion of privacy to the unsolicited distribution of obscene pornographic materials, exists as a reflection of society (Kleinrock, 2004).

The current research focuses on the changing modus operandi through which crime is committed. Particularly, we elaborate on the relatively scant research that focuses on two of the oldest forms of crime, fraud and deception, as they currently exist in the *information age* (Lyon, 1988; Alberts, Papp, & Kemp III, 1997; Castells, 2000). The social sciences has largely discounted online fraudulent activity is being a nuisance of the digital technology. However, it represents a very harmful activity that has been facilitated purely by the Internet and has presented new risks that threaten the communications and commercial infrastructures (Wall, 2005).

The present study used data gathered from a sample of online fraud attempts from two computers in the form of unsolicited mass emails, commonly known as "spam," [4] over a two-month period. These results are generally considered with regard to earlier research that also addressed the nature of advance fee email solicitations (Dyrud, 2005; Holt and Graves, 2007). Thomas Holt and Danielle Graves (2007) earlier conducted a study similar to the present work by examining 412 fraudulent email messages and analyzing the mechanisms used by email scammers. Particularly, the researchers analyzed the structure and content, and the linguistic compositions within the email solicitations. Among the findings, Holt and Graves noted that roughly half of the email messages requested that recipients forward personal information to the sender. Their research closely resembles the present study, and finding from their work are discussed throughout the Discussion section of the present work. The studies differ in that the present work provides a deeper analysis and deconstruction of the email content and foregoes examination of the language patterns found in Holt and Graves' study.

The present study contributes to the literature primarily through providing advanced analyses of the content within the email solicitations, and offering a basis of comparison for the findings from the Holt and Graves study. The authors seek to give insight into the structural and economic motivations for the perpetuation and nature of spam and online fraud. The focus of the research is the issue of gaining trust in order to deceive potential victims. Dyrud's (2005: 9-10) similar method of linguistic analysis of Nigerian 419 letters concludes that "scammers are accomplished persuaders who garner substantial, albeit unethical, rewards for their efforts."

The present research also provides direction for law enforcement agencies to prevent and confront computer fraud. Law enforcement and general crime prevention efforts may be misguided without accurate assessment of the problem(s) surrounding computer fraud, and the limited scholarly research in the area provides little assistance. The findings from the present study-, and results from related works provide direction for preventing and responding to computer fraud, as social control agents can more accurately guide their efforts.

Further, the results offer assistance to potential victims. Individuals who are more aware of the nature of fraudulent computer schemes are better positioned to avoid becoming

[4] "Spam" is common slang for any type of unwanted or unsolicited online communication. *See* http://www.microsoft.com/protect/terms/spam.aspx.

actual victims. The ability to identify, avoid, and/or report computer scams facilitates the overall prevention of fraudulent behavior, and saves potential victims much time, aggravation, and financial resources.

The following review of the literature addresses several topics pertaining to online fraud. Particularly, the discussion entails an overview of this growing problem, including an examination of the various types of fraud and a discussion of both legislative and law enforcement efforts to confront the activity.

Review of Literature

The Growing Problem of Online Fraud

Fraud, loosely defined as intentional misrepresentation for the purpose of gain, has existed in various forms for centuries. David Friedrichs (2004) argues that fraud, recognized as "contrepreneurial crime" under the umbrella term "white-collar crime," has existed since the origin of recorded history. Legislation pertaining to fraud dates back to the fourth century B.C. in ancient Greece (Drapkin, 1989). Despite the fundamental nature of the crime remaining constant (larceny by trick, false pretence, or deception), fraud has evolved with legal and marketplace changes. As Chambliss and Courtless (1992) point out, "fraud presents a difficult set of legal and social problems," yet "few statutory definitions spell out [all the elements of the crime]" despite its accounting "for a greater economic burden on the average citizen than all other crimes combined" (p.241). The complexities of fraudulent behavior are rooted in the varieties of forms it can take and its continuing evolution as a type of criminal commerce, ranging from political fraud (e.g., intentionally excluding groups of individuals from voting or purchasing votes with government funds, e.g., Campbell, 2005) to electronic fraud, as discussed in the present research.

The nature of fraud became even more complex with the introduction of Internet communications and electronic commerce. Junk mail was recognized by researchers long before the Internet was made publicly available. Early in the development of Internet in 1975, an Advanced Research Projects Agency (ARPA) network engineer warned, "In the ARPA Network Host/IMP interface protocol there is no mechanism for the Host to selectively refuse messages…Such a Host could be sent many messages by a malfunctioning Host," leading to "a denial of service to the normal users of this Host" (Postel, 1975:1; Hinde, 2003). Decades later, volumes of unsolicited email flood users' inboxes by sophisticated spammers who have learned to automatically harvest millions of email addresses (Prince, et al., 2005), generate fake websites ("spoofing") to mislead users ("phishing") (Dhamija, Tygar, & Hearst, 2006;), virally infect computers to steal information (Geer, 2005; Holz, Engelberth, & Freiling, 2009), circumvent spam-blocking technologies (Wagner, 2003) and other advanced forms of fraud.

Much evidence suggests technology-based fraud is increasing in frequency despite law enforcement efforts. According to a February 2009 Spam report by security software firm Symantec, the presence of spam, ranging in nature from advertising to outright fraud, has spiked since 2008. Results from the National White Collar Crime Center's 2005 National Public Survey on White Collar Crime noted a "sharp rise" in the number of technology-based white collar crimes, and suggested that technology-based crimes were becoming increasingly prevalent (National White Collar Crime Center, 2006). The Internet Crime Complaint Center and the Federal Trade Commission both identified a notable rise in the

number of deceptive practices committed via the Internet (National White Collar Crime Center, 2004 & 2005; Federal Trade Commission, 2005). The use of illegitimate emails to commit fraud has seen a "marked increase in recent years at a growth rate greater than that seen by more traditional forms of fraud" (National White Collar Crime Center, 2006). The increase in fraudulent emails is also supported by a 2008 Microsoft security report which found over 97% of all emails are unwanted and target the small percentage of users who fall prey to seemingly innocuous links and email attachments (Microsoft Security Intelligence Report, 2008).

The current economic downturn has fueled an increase in more aggressive fraudulent online activities, resulting in more frequent and malicious forms of this type of crime. According to one cyber security project manager, "The economy will likely remain a strong theme in upcoming months as cyber criminals tap into fear-mongering tactics to take advantage of the global economic downturn" (Threatscape Report, 2009). A 2008 McAfee report indicated that the global economic financial crisis has significantly exacerbated cybercrime as offenders are more likely to be motivated by financial gain (McAfee Virtual Crime Report, 2008). A Sophos report noted that offenders' strategies have evolved to more creative methods in deceiving users, for instance by targeting social networking venues such as Facebook and Twitter by masquerading as friends of victims (Goodchild, 2009; Internet Crime Complaint Center, 2009). The increase in creativity is indicative of the dynamic nature of online fraud.

Increases in the proliferation and sophistication of spammers have resulted in significant increases in harm. For example, scammers have masqueraded as FBI agents investigating fraud (FBI Internet Crime Complaint Center Intelligence Note, 2008). Other concerns include unwary Internet users responding to emails or misdirected links with personal information. These *phishing* scams acquire direct information, such as usernames and passwords, often through misrepresentation. While the present study focuses on advance-fee fraud, increased harm from the proliferation of spam must be considered. Statistics from the National Consumer's League's (NCL) National Fraud Information Center suggested that the total loss from Internet fraud in 2005 was over $13.8 million, a figure much higher than the $5.78 million lost in 2004. The average loss to Internet fraud victims was also much higher in 2005 than in 2004 (National Consumer's League, 2005, 2006).

Victims sometimes unknowingly install malicious software, or *malware*, on their personal computers. A 2008 McAfee report shows a dramatic increase in malware (McAfee Virtual Crime Report, 2008). Users may inadvertently install malware by opening email attachments or clicking on embedded links. This software can turn a computer into a "zombie," under the control of a third party operator. Cyber culprits can use networks of these infected computers, or *botnets,* for malicious activities ranging from attacking bank servers containing private information to automatically sending thousands of simultaneous emails for the purpose of defrauding users (Bacher, Holz, Kotter, & Wicherski, 2005; Provos & Holz, 2008; Liu, Xiao, Ghaboosi, Deng & Zhang, 2009). One infected computer can potentially generate 25,000 spam messages per hour or 600,000 per day (Keizer, 2009).

Scammers also appeal to sympathy. Two notable reasons for solicitation are illness and social/political victimization. Phishing scams often spike immediately after traumatic events, such as natural disasters. For example, in the aftermath of Hurricane Katrina, several charitable websites with legitimate sounding addresses (and some representing

themselves as the Red Cross) were shut down by authorities (Ragucci & Robila, 2006). Internet fraud, similar to all types of fraud, tends to prey on the sympathy of victims. Holt and Graves (2007) found that roughly 5.1 percent of solicitations were from individuals who claimed to have a terminal illness.

The present research suggests social engineering, or manipulation of people, is the most important part of online fraud. Two types of victimization are: (1) indirect victimization, or *pharming*, where links within emails redirect users to authentic-looking websites to capture information[5] for the purpose of selling the information to third parties or for use in identity theft and (2) direct victimization, in which a scammer, using a variety of guises and methods, manipulates victims into sending funds directly.

Computer fraud victimization can have an emotional impact and lingering effects on victims. For instance, victims of phishing scams can suffer from ailments ranging from embarrassment to depression, with some psychologists drawing similarities to Post Traumatic Stress Disorder (PTSD) (Carey, 2009). According to the Federal Trade Commission, 31% of identity theft victims who had new credit cards taken out in their name required over 40 hours to rectify credit issues and faced consequences such as harassment by creditors (48%), loan rejections (25%), and criminal investigations (12%) (Federal Trade Commission, 2006). The median loss per victim filed at the Internet Crime Complaint Center (IC3) were highest among check fraud ($3,000), confidence fraud ($2,000) and Nigerian advance fee fraud ($1,650), totaling $264.6 million in 2008 (IC3 Annual Report, 2008). In one extreme case, a British man committed suicide when victimized by an Internet money-laundering scam (Suicide of Internet Scam…, 2004).

Types of Fraud

Among the more common forms of Internet fraud are credit card fraud, identity theft fraud, Web and email spoofing (e.g., creating a Website that appears authentic when in fact it is not, and sending email directing potential victims to the site; this type of fraud is sometimes referred to as phishing), *IM spimming* (similar to spoofing, although it involves the use of instant messaging), high-tech disaster fraud, and online hoaxes (Harley & Lee, 2007; McQuade, 2006).[6] While each form of fraud is worthy of consideration, the present work primarily focuses on Web and email spoofing, and online hoaxes, which involve a variety of deceptive practices. To be sure, the categories that constitute cybercrime and Internet fraud sometimes overlap and the entire area of study is under constant development.

Phishing is an increasingly popular form of Internet fraud (e.g., Goth, 2005) with an increasing number of victims (McMillan, 2007). Sometimes called brand spoofing, phishing involves the use of emails that appear to originate from businesses with which targeted victims have been, or are associated. Some of the more common businesses and industries included in phishing include banks, online businesses (e.g., eBay and PayPal), and online service providers (e.g., Yahoo and AOL). Unsuspecting victims receive emails that appear to be from these entities, often suggesting suspicious activity regarding the account and requesting personal information (e.g., personal identification numbers, credit card numbers, and social security numbers). The sender (i.e., the offender) ultimately seeks

[5] This is commonly known as a "man-in-the-middle" attack pattern in which information is passively captured, akin to digital eavesdropping, before being forwarded to the legitimate destination.

[6] The Internet Crime Complaint Center (IC3) (http://www.ic3.gov/crimeschemes.aspx) and the FBI (http://www.fbi.gov/majcases/fraud/internetschemes.htm) have a listing of the varieties of Internet crime.

to use the victim's personal information for individual gain (see Larcom and Elbirt, 2006, for a thorough discussion of phishing, including prevention and retaliation efforts). The emails convince up to 20 percent of recipients to respond to them, sometimes leading to financial losses, identity theft, and other forms of fraud (Kay, 2004). "Brand" association is an effective technique that allows scammers to directly steal information or be able to use social engineering to persuade users to disclose financial information (James, 2005; Harley & Lee, 2009). Fraudsters also set up bogus websites portrayed as legitimate sites from which unwary customers purchase goods they never receive.

Online hoaxes may consist of emails containing lottery scams and "get rich quick" schemes of various sorts. Lottery scams often involve unsuspecting victims receiving an email stating that they have won a sum of money and/or prizes. The gist of this scam involves the recipient/"winner" being required to call someone (i.e., an individual involved with the scam) who then instructs the "winner" to send fees in order to process the winnings. More skillful con artists rarely solicit direct victim information but instead rely on social engineering to create a web of deceit using fictitious legal and administrative costs associated with foreign lotteries to obtain personal information and payments (Barrett, 2004). "Get rich quick" schemes often appeal to targeted victims' motivation to make a large sum of money with little effort. Such schemes may involve an email detailing a tragic incident and the need for the email recipient (i.e., the potential victim) to forward personal information and/or money. Once the confidence of the victim is earned by building a rapport using false pretenses of a non-existent good, service, or payment, the offenders are able to make a substantial profit. The authors of fraudulent emails often operate out of countries that do very little to prevent and enforce Internet fraud (McQuade, 2006).

Earnings from Internet fraud can contribute significantly to depressed economies. Nigeria, in particular, has drawn international attention by its proliferation of advance fee schemes (e.g., Smith, Holmes, & Kaufmann, 1999; Edelson, 2003; James, 2005; Holt & Graves, 2007; Harley & Lee, 2007, 2009). Online advance fee fraud has been synonymously known as "Nigerian 419" scams, named after Nigerian Criminal Code chapter 38 §419 dealing with fraud. This is not to say that advance fee fraud originates from Nigeria, but that the region has become associated with this type of fraud and corruption over the course of several decades (Smith, 2007; Glickman, 2005). Former U.S. Secretary of State Colin Powell even referred to Nigeria as "a nation of scammers" (Glickman, 2005).

According to Microsoft, Nigerian 419 scams are a very common type of advance fee fraud where scammers generally claim to be from Nigeria and execute a variety of deceptive schemes that require victims to front money.[7] These scams are frequently executed from access points in the form of local cyber cafés, which have been the target of more recent raids from Nigeria's Economic and Financial Crimes Commission (EFCC) (Lilly, 2009). However, Internet scammers often remain largely undeterred by law enforcement activities (Goodman & Brenner, 2002). The situation in Nigeria clearly exemplifies the criminogenic conditions created by lax laws and enforcement regarding the Internet.

One may best explain Internet fraud by examining environmental conditions that contribute to its proliferation. Researchers have identified several factors as contributing to

[7] *See* http://www.microsoft.com/protect/fraud/phishing/feefraud.aspx.

fraud in Nigeria: (1) ease of access, (2) anonymity, (3) availability of email extraction software, (4) ignorance of the gravity of online crimes, (5) economic conditions, and (6) inadequate law enforcement (Adomi & Igun, 2008). For example, cyber cafés have been identified as facilitating fraudulent activities in Nigeria more than any other Internet access points (Longe & Chiemeke, 2008). Local social conditions further exacerbate environments that are conducive to crime due to the limited legal response to computer crime.

Community members tacitly accept Nigerian 419 scams. Scammers are perceived as legitimate businesspersons and are allowed to operate in localized regions (see, e.g., Adeniran, 2008, for discussion of the impact of the Internet on the creation and perpetuation of a criminal subculture in Nigeria). Robert Merton's (1938) *strain theory*, as well as the subsequent variations of Merton's work (e.g., Agnew, 1992; Cloward & Ohlin, 1960; Messner & Rosenfeld; 1994) can explain these criminogenic regions as the result legitimate means of goal attainment being blocked or unavailable. According to one representative from the EFCC, "419 scams are still the main problem but we are also witnessing other problems such as credit card fraud and lottery scams as well as the hacking and cloning of websites" (McCue, 2005). Offenders are undeterred from misconduct without community stigma (Lemert, 1974; Braithwaite, 1989). Moreover, victims are often blamed for being greedy. For instance, Nigerian high commissioner Sunday Olu Agbi stated that "people who send their money are as guilty as those who are asking them to send the money" (Cheng, 2008).

The Internet has reduced the costs of committing fraud while exponentially expanding the base of potential victims. Among other effects, this has resulted in advance fee emails being sent to an "extremely conservative" estimate of over 10 million recipients worldwide daily (King & Thomas, 2008). The large numbers of emails are necessary to capture the relatively small number of respondents. According to a University of California study, only one in 12.5 million fraudulent email attempts receive a response (Kanich et al., 2008). During the study period of 26 days, only 28 sales resulted from over 350 million emails sent, a response rate of only 0.00001%. However, that small percentage can translate into a significant amount of earnings. Despite the extremely small percentage of respondents, one can estimate that the spam in an entire botnet would generate roughly $3.5 million in revenue each year.

Legislating and Policing Internet Fraud

The Internet poses new challenges for victims, law enforcement, and lawmakers. The technical and distributed nature of cybercrime often confuses victims in need of help and lawmakers trying to draft laws that will hold up across multiple jurisdictions. Law enforcement must also deal with the difficulties associated with jurisdiction (Brenner & Koops, 2004; Burns, Whitworth & Thompson, 2004), digital evidence (Scarborough, Rogers, Frakes & Martin, 2006), and issues related with the culture and structure of law enforcement (Nhan & Huey, 2008).

Numerous laws exist to confront computer crime, and, more specifically, Internet fraud. Legislation in this area is continuously emerging and evolving as technological advances create the need for additional legislation and the revision of existing laws.[8]

[8] Ralph Clifford's (2006) book *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime* (2nd edition) is among the works that provide a thorough account of the legal responses associated with computer crime.

Clearly delineating the legislation surrounding cybercrime or Internet fraud is beyond the scope of this work. However, the nature of the present work, which involves examination of a new form of an existing crime (fraud), warrants a brief overview of legislation in this area.

U.S. laws often do not distinguish Internet fraud from traditional fraud. Brenner (2006) highlights the legislation surrounding identity theft, including Section 1028 of Title 18 of the U.S. Code which prohibits behaviors considered fraud in conjunction with identification documents and contains penalties of five to fifteen years of imprisonment, as well as fines and forfeiture. For instance, under federal law it is illegal to knowingly and without permission produce an authentication feature, an identification document, or a false identification document. Further, transferring these types of documents knowing that they were stolen or produced without authority is illegal.

Offenders will sometimes unlawfully use the trademark of an established, reputable agency in attempts to persuade unwitting victims to submit funds or personal information. Email spoofing, a form of phishing, is often committed in violation of the Lanham Act (15 U.S.C. §§ 1051-1141n (2000)) and the Trademark Counterfeiting Act (18 U.S.C. §2320(a) (2000)), which address violations of trademark infringement. The Lanham Act addresses civil damages for trademark infringement; the Trademark Counterfeiting Act facilitates criminal penalties. To successfully impose criminal charges, prosecutors must demonstrate that the defendant intentionally and knowingly used the counterfeit trademark to traffic, or attempt to traffic, in goods and services. These and related actions, as detailed by Brenner and other legal scholars who elaborate on the nature of identity theft legislation, have become more feasible due to extensive technological advancements.

The Internet has not fundamentally changed the legal orientation and motivations for fraud. Phishing, for instance, is simply fraud committed using electronic means. Brenner (2001: 1) categorized cybercrime into four core legal components:

(1) *Actus reus* (the perpetrator communicates false information)

(2) *Mens rea* (communicating false statements for the purpose of defrauding the victim),

(3) *Attendant circumstances* (perpetrator's statements are false) and

(4) Harm (the victim was defrauded out of property or something of value). Under this legal analysis, existing laws are adequate to indict Internet fraudsters. Prosecutors can use traditional mail- and wire-fraud statutes, although not cybercrime-specific, to convict fraud committed via the Internet (Brenner, 2006).

State, federal, and international laws exist to confront jurisdictional issues of Internet fraud. The inter-jurisdictional nature of most computer crime provides particular challenges not found in many traditional forms of criminal behavior. States and countries vary in their responses to computer crime, with some having more well-defined laws than others. In 2006, the United States became an official participant of the Convention on Cybercrime Treaty established by the Council of Europe in an effort to set minimum standards on international cyber laws.[9]

Uncertainties in jurisdiction can attribute to differences in laws. Brenner and Koops (2004) note two situations associated with international jurisdiction issues: (1) no

[9] *See* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=9/2/2006&CL=ENG. Critics of the treaty have underscored the expansion of law enforcement authority and lack of legal safeguards to protect against privacy rights.

one claims jurisdiction and (2) more than one country claims jurisdiction. They explain that at a more fundamental level, "it is unclear just what constitutes jurisdiction: is it the place of the act, the country of residence of the perpetrator, the location of the effect, or the nationality of the owner of the computer that is under attack? Or all of these at once?" (p. 3). In addition, substantive differences in laws, such as the age at which a society considers one a minor, and the age which distinguishes pornography from child pornography, can be problematic.

Legal and jurisdictional issues compound the technical and structural complications associated with policing Internet fraud. The patchwork of overlapping hierarchy of law enforcement agencies makes required collaborations cumbersome. Moreover, historically, police tend to tie their practices to traditional notions of territory and have had difficulty adapting to the "abstract" nature of cyberspace (Huey, 2002). Many scholars have called for radical changes in the paradigm of law enforcement that incorporates partnerships with non-state entities to adapt to the information age (Wall, 2007; Nhan and Huey, 2008).

The police prioritize traditional crime control activities associated with street crime and must service the needs of localized citizens and groups (Bayley, 2005). Consequently, the lack of adequate enforcement stemming from law enforcement's static nature in a dynamic environment creates "digital disorder" online, resulting in "broken windows" conditions that are conducive to deviance (Correia & Bowling, 1999).

Methodology

The present study addresses the dearth of criminological research attention regarding online fraud (e.g., Holt and Graves, 2007). Particularly, in May and June of 2007, the researchers used two email accounts for the reception of unsolicited emails. Exceptions were made by the authors for those items identified as containing potentially harmful computer code, which were counted as an item of spam but not opened due to software restrictions at the risk of damage to computer systems. The number of unsolicited mail contacts received at the two reception sites totaled 603. These emails were initially sorted to remove duplicates sent to the same computer continuously or to both computers simultaneously. The initial screening left a total of 476 emails that were appropriate for analysis.

The email accounts were owned and administrated by a higher education institution. Two authors used these ".edu" accounts on a daily basis primarily for business. The researchers have been actively using these accounts for approximately one decade at the time of the data collection. Email administrators filtered the emails at the enterprise level using Microsoft Exchange Server. All filtered emails were quarantined in the User Quarantine Release folder that is deleted upon the discretion of the end user. Any emails that circumvented spam filtering were collected in the inbox by the authors for analysis. The authors intended for these accounts to represent typical email accounts used for business over free personal accounts that are often sold or distributed to third parties for advertising.

The general intent of this work is to provide a descriptive content analysis of sample emails received. Accordingly, each component of the solicitation and the solicitor identified within the documents were analyzed. The researchers evaluated emails in three stages. First, the emails were assessed to determine whether they were used as a source of information in relation to the identified components of the transaction. Next, the content of each email was scrutinized and deconstructed by two of the authors to glean individual

characteristics. Manifest content analysis was used in all three stages with the intent to reduce any level of subjectivity in analyses of the emails. Manifest content, which involves documenting the "visible, surface content" of a communication and eliminates the need for much interpretation of the underlying meanings of the material (Maxfield & Babbie, 2005, p. 342), was selected given the nature of the data collected. Accordingly, there was inter-rater reliability in all instances.

Fraudulent emails have patterns and indicators that help identify deception. For instance, researchers have found that multiple writing techniques were used by advance fee fraudsters to generate information and responses from potential victims (Cukier, Nesselroth, & Cody, 2007; Holt & Graves, 2007). Illegitimate emails often contain grammatical and spelling errors that are consistent with the typical protocol for advance fee frauds where scammers initiate contact with innocuous emails to gain trust and move on to more aggressive requests for money (e.g., Holt and Graves, 2007; Dyrud, 2005; Symantec 2009). This aspect of trust is perhaps the most important element of fraud.

A potential limitation of the present work concerns the possibility that the emails used in the present study were, in fact, legitimate. In other words, it is possible (although unlikely) that some of the proposals, opportunities, and offers provided in the emails analyzed in the present study were what they claimed - offers of opportunity and requests for needed help. However, the large percentage (42%) of the emails containing grammatical errors and requests to immediately transfer funds (36%) suggest the non-credible nature of these unsolicited contacts. Still, the possibility that a small number of credible emails may have had some minor impact on the overall results warrants mentioning.

It should also be noted that the convenience sample used in the present study is by no means representative of all online fraud. Nevertheless, the data certainly provide insight into the nature of online fraud. The small sample size and limited scope of this research does not imply generalizability, but instead offers exploratory descriptions to draw further research considerations.

Results

The following section presents the results from the analyses of the emails/data. Specifically, the findings address: (1) the claimed countries of origin from which the fraudulent emails originated; (2) the nature and prevalence of corporate or organizational identities used in fraudulent emails; (3) the specific types of corporate entities used in email fraud; (4) the alleged positions of those soliciting information/money via fraudulent emails; (5) the types of personal information included by solicitors engaged in email fraud; (6) the specific nature of the fraud (e.g., lottery winnings, job offer); (7) the specified amount of money involved in the fraudulent email; (8) the specified percentage return on investment for those who respond to the fraudulent email, and; (9) the type and extent of personal information solicited from potential victims.

Table 1 notes the country of origin for those distributing fraudulent emails. The large majority of emails (70.8%) originated from the United Kingdom (37.3%) and Nigeria (33.5%). Emails also came from other countries, including Taiwan (11.2%), Russia (6.8%), China (5.6%), the Ivory Coast (3.7%), and France (1.9%). The authors did not examine email headers with Internet service providers (ISPs) to verify the claimed source location of the email matches with actual email origin (email spoofing). Instead, attention was

given to the claimed source of origin, which was important in assessing if scammers perceived positive associations with certain regions.

Table 1

Claimed source of fraudulent email

Country of Origin	N	%
United Kingdom	60	37.3
Nigeria	54	33.5
Taiwan	18	11.2
Russia	11	6.8
China	9	5.6
Ivory Coast	6	3.7
France	3	1.9
Total	161	

The present findings suggest a two-pronged approach by fraudsters to establish credibility and trust: (1) claiming an association with known corporations or organizational entities and (2) claiming an association with reputable types of corporations. First, scammers often attempt to establish trust by associating themselves with legitimate and highly respected businesses and organizations. For example, one email from the "MICROSOFT/AOL AWARD TEAM" notified its winners of a sweepstake by stating, "The prestigious Microsoft and AOL has set out and successfully organized a Sweepstakes marking the end of year anniversary we rolled out over 100,000.000.00 for our new year Anniversary Draws." The email then proceeded to ask for the potential victim's personal information. The top three organizations represented were from the U.S.: Microsoft (27.1%), America Online (18.6%), and PayPal (15.7%), as noted in Table 2.

Table 2

Used Known Corporate/Organizational Entity

Organization	N	%
Microsoft	19	27.1
America Online	13	18.6
PayPal	11	15.7
OPEC	10	14.3
Bank of America	9	12.9
United Nations	8	11.4
Total	70	

Fraudsters also attempted to establish trust through associating with credit-issuing financial corporations and authoritative organizations and groups. As noted in Table 3, the most popular forms of industries identified were banks (30.7%). Offenders were also likely to note an association with various corporations (24%) and political organizations, such as official government offices (17.9%).

Table 3

Specified Industries

Organization	N	%
Bank	55	30.7
Miscellaneous Corporations	43	24.0
Political Organization	32	17.9
Insurance Agency	26	14.5
Stockbroker	23	12.9
Total	179	

Those engaging in email fraud often pose as respected individuals. As noted in Table 4, those posing as others were most likely to claim a position as a bank officer (28.6%) or a lawyer (27.1%). Others claimed to be a politician (16.5%), a member of the clergy (12.8%), a military officer (8.3%), or a doctor (6.8%). These categories were often combined with reputable organizations for greater effectiveness. For example, one scammer claimed to be a "portfolio Manager with Fidelity Investment International (UK)." Table 4 depicts these findings.

Table 4

Profession of Solicitor Provided

Apparent position	N	%
Bank Officer	38	28.6
Lawyer	36	27.1
Political	22	16.5
Clergy	17	12.8
Military Officer	11	8.3
Doctor	9	6.8
Total	133	

To gain the trust of targeted victims, solicitors typically generate and include in the email a scenario appealing to the victims' concern for others. Accordingly, solicitors include alleged personal information in their emails. Most commonly, solicitors mentioned

that they were married (32.4%) or they were ill (22.7%). Others reported being a victim of some social or political event (14.8%), having children (11.5%), being somehow related to a victim of a tragic incident (9.7%), or being an heir (6.5%) who will soon collect a large sum of money that they will allegedly share. For example, one solicitor claiming to be an HSBC bank representative stated, "I received a call that one of my customer [sic] died in the Tsunami Disaster with his wife and only child while on vacation at Phuket Island in Thailand." Table 5 depicts these findings.

Table 5

Personal Information Provided by Solicitor

Apparent position	**N**	**%**
Married	90	32.4
Ill	63	22.7
Social/Political Victim	41	14.8
Children	32	11.5
Related to Victim	27	9.7
Heir	18	6.5
Royalty	7	2.5
Total	278	

Fraudulent emails often appeal to human greed through lucrative opportunities. The present study found two broad categories in which fraudulent spammers operate using a two-pronged approach: (1) the desire to share in a lucrative opportunity and (2) extremely high returns on large amounts of money. The largest category of fraudulent emails involved offerings of a share of discovered fortune (43.5%), followed by a share of winnings (26.2%), requesting assistance (19.0%), and a job offer (11.4%). Table 6 depicts these findings.

Table 6

Nature of Fraudulent Email

Specified Issue	**N**	**%**
Share Discovered Fortune	103	43.5
Winnings	62	26.2
Asking Help	45	19.0
Job Offer	27	11.4
Total	237	

Fraudsters typically appeal to personal greed through promises of financial rewards. It would seem that larger sums of financial returns would generate greater responses from targeted victims. However, the largest percentage of solicitors offered between $1 million and $10 million for assistance (39.9%), followed by offerings between $10 million and $100 million (26.2%). The smallest percentage of emails offered over $100 million (3.5%). Table 7 depicts these findings.

Table 7

Specified Amount of Money Involved

Amount	N	%
$0 - $100,000	27	10.9
$100,000 - $500,000	19	7.7
$500,000 - $1,000,000	29	11.7
$1,000,000 - $10,000,000	99	39.9
$10,000,000 - $100,000,000	65	26.2
$100,000,000 +	9	3.6
Total	248	

Fraudsters sometimes promise a percentage of large sums of money for victim cooperation. As noted in Table 8, solicitors were most likely to offer higher percentages of returns to potential victims. Specifically, the largest percentage of solicitors offered fifteen percent or more of their anticipated earnings (42.9%), followed by promises of 10-15 percent (29.5%), 5-10 percent (17.1%), and 0-5 percent (10.5%).

Table 8

Specified Percentage Return on Investment

Percentage	N	%
0% - 5%	11	10.5
6% - 10%	18	17.1
11% - 15%	31	29.5
16% +	45	42.9
Total	105	

To benefit from their fraudulent behavior, solicitors generally request personal information they can subsequently use for criminal behavior. Among the more frequently requested pieces of information solicited from potential victims were email addresses (26.7%), telephone numbers (15.1%), names (14%), and addresses (10.6%). In one typical example, one email notification of a sweepstakes winner asked respondents for:

1. Full Names
2. Residential Address
3. Sex
4. Marital Status
5. Mobile
6. Age
7. Occupation
8. Amount Won
9. Nationality
10. Ticket Number and Serial Numbers

Interestingly, scammers solicited bank account numbers (3.2%) and social security numbers (2.5%) relatively infrequently. This is consistent with studies of social engineering as a means to circumvent security measures. Winkler and Dealy (1995) conducted a case study of social engineering and found expensive information security technologies can be easily bypassed completely by simple methods such as calling a company and simply asking people for their passwords. Moreover, the most infamous hackers of the computer generation, such as Kevin Mitnick, have often preferred non-technical methods ("human hacking"), such as rummaging through trash ("dumpster diving"), to obtain information (Slatalla & Quittner, 1995; Mitnick & Simon, 2002; Long & Mitnick; 2008)

Table 9

Target Information Requested

Nature of Information	**N**	**%**
Email	207	26.7
Telephone	117	15.1
Name	108	14.0
Address	82	10.6
Age	47	6.1
Gender	45	5.8
Occupation	34	4.4
Bank Account Number	25	3.2
Social Security Number	19	2.5
Marital Status	19	2.5
Company Name	11	1.4
Next of Kin	9	1.2
Nationality	7	.9
Total	774	

Discussion

Several factors emerged from analyses of the data used in the present study. Prominent among the findings are: (1) the top two claimed countries of origin were the United Kingdom and Nigeria, respectively; (2) discovered fortunes were the most prevalent selling point, suggesting greed as an apparent motivating factor amongst victims; (3) solicitors tended to pose as financial institutions such as banks and reputable companies such as Microsoft; (4) solicitors generally requested email addresses and names instead of social security and bank account numbers, suggesting social engineering is the main avenue towards the fraud; and (5) solicitors often represented themselves as white-collar professionals, such as bank officers and lawyers. These factors suggest the nature of scams identified in the present study did not involve charity; instead they focused on victims' desires to make money.

The findings suggest that fraudsters often represent themselves as originating primarily from the United Kingdom or Nigeria. These findings are consistent with the scam known as advance-fee fraud (Smith, Holmes, & Kaufmann, 1999; Glickman, 2005; Holt & Graves, 2007). This scam, which originated before the widespread use of the Internet, uses false pretenses to lure victims into disclosing information and ultimately sending money. It often involves a request for victims to assist with the release of alleged funds. Advance-fee scams often involve a request for victim financial assistance to release funds, inheritance monies, or lottery winnings (Microsoft, 2009). Variants of the scam contain elements ranging from fake checks to directing victims to sophisticated bogus websites designed to capture personal information. These scams appeal to many human emotions and behaviors, including greed, fear, and sympathy.

Nigeria is presently a hot spot for fraudulent Internet scams. While advance-fee fraud did not originate in Nigeria, the country has certainly contributed to its proliferation. Adomi and Igun (2008) explain that the country's lack of enforcement and culture of corruption are especially conducive to online fraudulent activities. The authors comment on the conditions, stating that "Cyber crime cannot be divorced from the widespread corruption in the Nigerian society. There is a harsh economic climate, high unemployment, utter disregard for the rule of law and lack of transparency and accountability in governance" (Adomi & Igun, 2008: 1).

Due to the anomic conditions and the lack of meaningful enforcement, a relatively small, but prolific group of scammers has emerged in Nigeria. This lends itself to two criminological theories based on rational thought: *strain theory* and *rational choice/deterrence theory*. For instance, strain theory proposes that deviant behavior can be attributed to a combination of structural blockages or unavailability of lawful societal means to achieve legitimate social goals and individuals pursuing *innovative* (unlawful) means to achieve these goals (Merton, 1938, 1964).

The prolific number of scams notoriously associated with Nigeria can be explained by the lack of official sanctions and enforcement of perpetrators. Rational choice theory explains human behavior as dictated by a hedonistic pursuit of pleasure and avoidance of pain. Deterrence, therefore, is only possible with proper sanctions based on *certainty, severity,* and *celerity* of punishment (Beccaria, 1764/1986). *Routines activity theory* further explains individual criminal behavior as a result of three prerequisite conditions: (1) motivated offenders, (2) suitable crime targets, and (3) inadequate or unwilling guardians (Cohen & Felson, 1979).

Much to the chagrin of its government,[10] Nigeria has garnered a reputation for frequently engaging in Internet fraud. A study of this region highlights structural strains (Smith, 2007) that contribute to the region's proliferation of fraudulent emails. Adomi (2008: 718-719) identified several structural variables that contribute to the criminogenic environment that create conditions for opportunity: (1) ease of access to the Internet, (2) anonymity of the Internet, (3) availability of email extractor software, (4) ignorance of online laws, (5) economic conditions of the people, and (6) inadequate law enforcement. Furthermore, Adomi explored different tactics to remedy the lax enforcement in Nigeria and proposed: the creation of a central federal agency that would target cybercrime, the enactment of cyber laws, the regulation of cyber cafés, and the formation of government alliances with American companies such as Microsoft. Ironically, the Nigerian government's association with Microsoft is misleadingly mirrored by scammers, albeit for more sinister reasons.

Findings from the present study suggest that fraudsters often attempted to gain trust by representing themselves as reputable individuals within respected companies and organizations, particularly banks and bank officers. This finding jives with results from Holt and Graves' (2007) work, which found that roughly 30 percent of the fraudulent emails they received claimed to be from bankers. Interestingly, medical doctors, whose reputation ranks high in American culture, were the least frequently represented persons in the present study. Perhaps the association with financial institutions or officers working in financial institutions appeals to the victims' assumed interest in obtaining financial reward.

Scammers often couple business ventures with unrealistically high returns on investments that appeal to even highly educated individuals. The present research noted that the most popular amount of money specified was between one and ten million dollars. Holt and Graves (2007) noted that they received solicitations with promised returns ranging from $90,000 to $423,000,000, and added that most often the amount promised was in the millions. Victims targeted in the present work were promised unrealistically high rates of returns. The most prevalent amount given was 15% or greater, another finding that supports the work of Holt and Graves (2007) who found that recipients who assisted the sender (i.e., the fraudster) were most often promised between 10 and 40 percent of the total amount. These returns on investments of extremely large amounts of money may seem like an obvious scam, but some individuals nevertheless fall prey. For example, renowned University of California at Irvine psychiatrist Dr. Louis Gottschalk was bilked out of $3 million over a 10-year period by Nigerian scammers. Gottschalk's attorney explained, "While it seems unlikely, even ludicrous, that a highly educated doctor like [Gottschalk] would fall prey to such an obvious con, that is exactly what happened" (Lobdell, 2006).

Findings from the present research also suggest that scammers preferred social entrées to victims over direct financial information. In essence, phishing is a form of social engineering that requires an element of trust as the primary mechanism for fraud. Scammers often establish trust with potential victims through repeated personal contact. The most requested form of information solicited from targets were email addresses and telephone numbers; findings which concur with results of Holt and Graves' (2007) earlier

[10] Nigeria has recently demanded an apology of Sony Entertainment for its advertisement depicting Nigeria as a "home of fraud where its citizens hardly do genuine business." *See* http://www.vanguardngr.com/2009/09/08/sony-corporation-portrayed-nigeria-as-home-of-fraud-fg/

work, and suggest that solicitors seek long-term strategies to establish rapport with victims. In comparison, directly exploitable information such as bank account numbers and social security numbers were requested less often.

Social engineering has historically been used in electronic fraud. Perhaps the most famous hacker, Kevin Mitnick, emphasized the use of social engineering to manipulate victims into disclosing information that allowed him access to telephone lines and computer systems. In his book The Art of Deception: Controlling the Human Element of Security, Mitnick described fictional tales of circumventing hi-tech security measures such as passwords and physically entering unauthorized areas by simply "pretending to be someone else and *just asking for it*." Such actions are representative of his personal exploits in the cyberpunk movement from the late 1970s to early 1990s (Mitnick & Simon, 2002: 3).

Online frauds that target individual victims often focus on social engineering. The present study regarding the content of spam supports existing research showing that Internet scammers focus on obtaining information from individuals by building trust rather than using direct ways of gathering information. Therefore, electronic measures alone cannot curtail victimization by increasingly savvy malefactors. Several software security companies have underscored the importance of individual prudence to supplement their products and services that filter and warn of scams. Ultimately, the individual must be vigilant in preventing victimization. The SEC recommends that individuals verify financial transactions with all institutions with whom they do business, be wary of embedded links within emails, install and update security software, read monthly statements, and learn to spot potential malefactors by researching non-profit websites on Internet scams.[11]

Conclusion

Internet fraud is problematic and takes many shapes and forms. Further, Internet fraud is not restricted to the United States. For instance, research conducted by computer security company McAfee found that the largest target of Nigerian 419 scams is the UK, which received 23% of all global Nigerian email scams. One user experienced 5,414 pieces of junk email in a single month (McAfee S.P.A.M. Experiment, 2008).[12] The United States is the second largest target, with 20% of all global junk email. Researchers often reason that Nigerian scammers believe the UK and US are the most lucrative countries with large numbers of potential victims. Most spam content is written in English, further indicating this preference by Nigerian fraudsters. However, an assessment of the content of emails indicates that no one particular group or country is free from attempted fraudulent activities.

The types of computer crime committed vary as computers evolve and continuously play a significant role in society. The increased frequency with which electronic fraud is attempted and committed underscores the need for additional Internet fraud research. This small but growing area of research is ripe with opportunity to explore the changing nature of crime. Despite the increasing frequency with which Internet fraud occurs (e.g., Baker, 1999; Sherman, 2001) and the notable harms it generates (e.g., Farnsworth & Kelleher, 2002; Farnsworth & Knap, 2002; Sherman, 2001), studies of Internet fraud remain scarce

[11] *See* http://www.sec.gov/investor/pubs/phishing.htm.

[12] Please note that participants in the McAfee experiment actively clicked on online advertisements, causing an exponential growth of spam mail received. Our study compliments this study by assessing the contents of fraudulent messages.

in the research literature (e.g., Holt and Graves, 2007). Accordingly, the present work focused on one of the more commonly encountered computer crimes, Internet fraud. In particular, the present work addressed the nature of email solicitations used in attempts to defraud victims of information and other resources, and in doing so expanded upon and contributed to the scarce body of research in this area. Further, findings from the present study also provide direction for law enforcement efforts and offer guidance for individuals solicited by electronic fraudsters. The significance of and increasing frequency with which electronic crimes are committed dictates additional research efforts in this area are needed.

References

Adeniran, A. (2008). The internet and emergence of Yahooboys sub-culture in Nigeria. *International Journal of Cyber Criminology*, *2*(2), 368-381.

Adomi, E. E., & Igun, S. E. (2008). Combating cyber crime in Nigeria. *The Electronic Library*, (26)5.

Alberts, D. S., Papp, D. S., & Kemp III, W. T. (1997). The technologies of the information revolution. In D. S. Alberts, & D. S. Papp (Eds.), *The information age: An anthology on its impact and consequences*. CCRP Publications. Retrieved on November 25, 2009 from http://www.dodccrp.org/files/Alberts_Anthology_I.pdf.

Bacher, P., Holz, T., Kotter, M., & Wicherski, G. (2005). Know your enemy: Tracking botnets. Retrieved on November 25, 2009 from http://www.scribd.com/doc/2674759/Know-your-Enemy-Tracking-Botnets.

Baker, C. R. (1999). An analysis of fraud on the Internet. *Internet Research: Electronic Networking Applications and Policy*, (9), 348-359.

Barrett, R. (2004). Show me the money: Foreign lottery scams hit the jackpot in the U.S. *Consumer Reports web watch*. Retrieved on November 23, 2009 from http://www.consumerwebwatch.org/dynamic/fraud-investigation-show-me-the-money.cfm.

Beccaria, C. (1764/1986). *On crimes and punishments*. Indianapolis: Hackett Publishing.

Bayley, D. H. (2005). *Changing of the guard: Developing democratic police abroad*. New York: Oxford University Press.

Braithwaite, J. (1989). *Crime, shame and reintegration*. New York: Cambridge University Press.

Brenner, S. W. (2001). Is there such a thing as "virtual crime"? *California Criminal Law Review*, (4)1.

Brenner, S. W. (2006). Defining cybercrime: A review of state and federal law. In R. D. Clifford (Ed.), *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime* (pp. 13-95) (2nd ed.). Dunham, NC: Carolina Academic Press.

Brenner, S. W., & Koops, B. J. (2004). Approaches to cybercrime jurisdiction. *Journal of High Technology Law*, *4*(1), 1-45.

Burns, R. G., Whitworth, K. H., & Thompson, C. Y. (2004). Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice*, *32(*5), 477-493.

Campbell, T. (2005). Deliver the vote: A history of election fraud, and American political tradition – 1742-2004. NY: Carroll & Graf.

Carey, L. (2009, July 29). Can PTSD affect victims of identity theft: Psychologists say yes. *Associated Content*. Retrieved on November 21, 2009 from http://www.associatedcontent.com/article/2002924/can_ptsd_affect_victims_of_identity.html.

Castells, M. (2000). *The rise of the network society 2nd edition*. Malden, MA: Blackwell Publishers.

Chambliss, W. J., & Courtless, T. F. (1992). *Criminal law, criminology, and criminal Justice: A casebook*. Brooks/Cole: Belmont, CA.

Cheng, J. (2008, August 22). Nigerian official: Greedy marks as guilty as 419 scammers. *Ars Technica*. Accessed on March 1, 2009 from http://arstechnica.com/security/news/2008/08/nigerian-official-greedy-marks-as-guilty-as-419-scammers.ars.

Clifford, R. D. (Ed.). (2006). *Cybercrime: The investigation, prosecution and defense of a computer-related crime* (2nd ed.). Dunham, NC: Carolina Academic Press.

Cloward, R., & Ohlin, L. (1960). *Delinquency and opportunity*. New York: Free Press.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review*, *44*, 588-608.

Correia, M. E., & Bowling, C. (1999). Veering toward digital disorder: Computer-related crime and law enforcement preparedness. *Police Quarterly*, *2*(2), 225-244.

Cukier, W. L., Nesselroth, E. J., & Cody, S. (2007). Genre, narrative and the "Nigerian letter" in electronic mail. Paper presented at the 40th Annual Hawaii International Conference on System Sciences, HICSS, January, 2007.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing works. Proceedings of the SIGCHI conference on Human Factors in computing systems. April 22-27, 2006, Montreal, Quebec, Canada. Retrieved on November 25, 2009 from http://portal.acm.org/ft_gateway.cfm?id=1124861&type=pdf&coll=GUIDE&dl=GUIDE&CFID=63613805&CFTOKEN=27178258

Drapkin, I. (1989). *Crime and punishment in the ancient world*. Lexington, MA: Lexington.

Dyrud, M. A. (2005). "I bought you a good news": An analysis of Nigerian 419 letters. Proceedings of the 2005 Association for Business Communication Annual Convention. Retrieved on November 25, 2009 from http://www.businesscommunication.org/conventions/Proceedings/2005/PDFs/07ABC05.pdf.

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.

Farnsworth, C., & Kelleher, J. (2002, January 15). The web of deception. *The Orange County Register*, 1.

Farnsworth, C., & Knap, C. (2002, May 26). Net fraud is tangled Web for victims and police. *The Orange County Register*, 1.

FBI Internet Crime Complaint Center (IC3) Intelligence Note (2008, January 4). Retrieved on October 13, 2009 from http://www.ic3.gov/media/2008/080104.aspx.

Federal Trade Commission and Synovate. (2006). Identity theft survey report. Accessed March 10, 2009 from http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

Federal Trade Commission. (2005). National and state trends in fraud and identity theft. Accessed November 1, 2007, from http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf.

Friedrichs, D. (2004). *Trusted criminals: White collar crime in contemporary society*, 2nd edition. Belmont, CA: Wadsworth.

Geer, D. (2005). Malicious bots threaten network security. *IEEE Computer Society*. Retrieved on November 25, 2009 from http://www.cis.uab.edu/zhang/Spam-

mining-papers/Malicious.Bots.Threaten.Network.Security.pdf.

Glickman, H. (2005). The Nigerian "419" advance fee scams: Prank or peril? *Canadian Journal of African Studies*, (39), 3, 460-489.

Goodchild, J. (2009, January 23). Report: Spam is more malicious than ever. *CSO Online*. Accessed February 10, 2009 from http://www.csoonline.com/article/477612/Report_Spam_is_More_Malicious_than_Ever?page=1.

Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *UCLA Journal of Law and Technology*. (3).

Goth, G. (2005). Phishing attacks rising, but dollar losses down. *IEEE Security & Privacy*, *3*(1), 8.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social legal studies*. *10*, 243-249.

Grabosky, P. N. (2004). The global dimensions of cybercrime. *Global Crime*. *6*(1), 146-157.

Hafner, K., & Markoff, J. (1995). *Cyberpunk: Outlaws and hackers on the computer frontier*. New York: Touchstone.

Harley, D., & Lee, A. (2007). The spam-ish inquisition. ESET antivirus and security white papers. Retrieved on November 27, 2009 from http://www.eset.com/download/whitepapers/CommonHoaxes+ChainLetters%28May2008%29.pdf.

Harley, D., & Lee, A. (2009). A pretty kettle of phish. ESET antivirus and security white papers. Retrieved on November 27, 2009 from http://www.eset.com/download/whitepapers/PhishingOnline.pdf

Hinde, S. (2003). Spam: The evolution of nuisance. *Computers & Security*. *22*(6), 474-478.

Holt, T. J. & Graves, D. C. (2007). A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology*, *1*(1), 137-154.

Holz, E., & Freiling. (2009). Learning more about the underground economy: A case-study of keyloggers and dropzones. Computer security – ESORICS, pp 1-18. Berlin: Springer Berlin/Heidelberg.

Huey, L. J. (2002). Policing the abstract: Some observations on policing cyberspace. *Canadian Journal of Criminology*, *44*(3), 243-254.

Internet Crime Complaint Center (2008). 2008 IC3 Annual Report. FBI/NW3C. Retrieved on November 26, 2009 from http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf.

Internet Crime Complaint Center (2009, October 1). Techniques used by fraudsters on social networking sites. *Internet Crime Complaint Center(IC3) Intelligence Note*. Retrieved on November 24, 2009 from http://www.ic3.gov/media/2009/091001.aspx.

James, L. (2005). *Phishing exposed*. Rockland, MD: Syngress Publishing.

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G. M., Paxson, V., & Savage, S. (2008). Spamalytics: An Empirical Analysis of Spam Marketing Conversion. Paper presented at CCS'08, October 27-31, Alexandria, VA. Accessed on March 10, 2009 from www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf.

Kay, R. (2004). "Phishing." *Computerworld*, *38*(3), 44.

Keizer, G. (2009, April 22). One Bot-infected PC= 600,000 spam messages a day. *Computer World*. Accessed on April 23, 2009 from

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=networking_and_internet&articleId=9131984&taxonomyId=16&intsrc=kc_top.

King, A., & Thomas, J. (2008). You can't cheat and honest man: Making ($$$s and) sense of the Nigerian E-mail scams. In F. Schmalleger and M. Pittaro (Eds.), *Crimes of the Internet* (pp. 206-224). Upper Saddle River, NJ: Pearson/Prentice Hall.

Kleinrock, L. (2004). The Internet rules of engagement: Then and now. *Technology in Society*, (26)2, 192-207.

Larcom, G., & A. J. Elbirt. (2006, Fall). Gone phishing. *IEEE Technology and Society Magazine*, 52-55.

Lasica, J. D. (2005). *Darknet: Hollywood's war against the digital generation*. Hoboken, NJ: Wiley & Sons.

Lemert, E. M. (1974). Beyond Mead: The societal reaction to deviance. *Social Problems*, (21)4, 457-468.

Lessig, L. (2005). *Free culture: The nature and future of creativity*. New York: The Penguin Group.

Levy, S. (2001). *Hackers: Heroes of the computer revolution*. New York: Penguin Books.

Lilly, P. (2009, October 23). Nigerian police crack down on scammers, shut down hundreds of websites. Maximum PC. Retrieved on November 26, 2009 from http://www.maximumpc.com/article/news/nigerian_police_crack_down_scammers_shuts_down_hundreds_websites.

Liu, J., Xiao, Y., Ghaboosi, K., Deng H., & Zhang, J. (2009). Botnet: Classification, attacks, detection, tracing, and preventive measures. *EURASIP journal on wireless communications and networking*. (2009), 1-11.

Lobdell, W. (2006, March 2). UCI psychiatrist bilked by Nigerian E-mail scams, suit says. *Los Angeles Times*. Accessed on March 2, 2009 from http://articles.latimes.com/2006/mar/02/local/me-nigerian2.

Long, J. & Mitnick, K. D. (2008). *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*. Burlington, MA: Syngress Publishing.

Longe, O. B. & Chiemeke, S. C. (2008). Cyber crime and criminality in Nigeria: What roles are Internet access points in playing? *European Journal of Social Sciences*, (6)4, 132-139.

Lyon, D. (1988). *The information society: Issues and Illusions*. New York: Blackwell.

Maxfield, M.G. & Babbie, E. (2005). Research methods for criminal justice and criminology (4th ed.). Belmont, CA: Wadsworth.

McCue, A. (2005, October 14). Nigeria enlists Microsoft to fight 419 scammers. Silicon.com. Retrieved on November 29, 2009 from http://software.silicon.com/security/0,39024655,39153344,00.htm.

McMillan, R. (2007, April). "Phishing sites explode on the Web." *PC World*, 25(4): 22.

McQuade, Samuel C. III. (2006). *Understanding and managing cybercrime*. Boston, MA: Allyn and Bacon.

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review*, (3), 672-682.

Merton, R. K. (1968). *Social Theory and Social Structure*. New York: Free Press.

Messner, S. & Rosenfeld, R. (1994). *Crime and the American Dream*. Belmont, CA: Wadsworth.

Microsoft (2009). Scams that promise money, gifts, or prizes. Retrieved on November 27,

2009 from http://www.microsoft.com/protect/yourself/phishing/hoaxes.mspx.
Microsoft Security Intelligence Report (2008). (6), July-December. Accessed on April 2, 2009 from http://www.microsoft.com/downloads/details.aspx?FamilyID=aa6e0660-dc24-4930-affd-e33572ccb91f&displaylang=en.
Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, IN: Wiley Publishing.
National Consumer's League. (2005). Internet scams: Fraud trends 2004. Retrieved October 1, 2007 at www.fraud.org/2004-internet%20scams.pdf.
National Consumer's League. (2006). Internet scams: Fraud trends, January-December 2005. Retrieved October 1, 2007 at www.fraud.org/2005_Internet_Fraud_Report.pdf.
National White Collar Crime Center. (2004). *IC3 2003 Internet fraud report*. Fairmont, WV: National White Collar Crime Center.
National White Collar Crime Center. (2005). *IC3 2004 Internet fraud report*. Fairmont, WV: National White Collar Crime Center.
National White Collar Crime Center. (2006). *The 2005 national public survey on white collar crime*. Fairmont, WV: National White Collar Crime Center.
Nhan, J., & Huey, L. J. (2008). Policing through nodes, clusters and bandwidth. In S. Leman-Lanlois (Ed.), *Technocrime: Technology, crime and social control* (pp. 66-87). Portland, OR: Willan Publishing.
Postel, J. (1975). On the junk mail problem. Network working group NIC #33861. Retrieved on November 25, 2009 from http://tools.ietf.org/pdf/rfc706.pdf.
Prince, M., Holloway, L., Langheinrich, E., Dahl, B. M., & Keller, A. M. (2005). Understanding how spammers steal your e-mail address: An analysis of the first six months of data from Project Honey Pot. Second Conference on Email and Anti-Spam, July 21-22, 2005, Stanford University, California. Retrieved on November 25, 2009 from http://www.cse.scu.edu/~tschwarz/coen252_07/Resources/spammer.pdf.
Provos, N., & Holz, T. (2008). *Virtual honeypots: From botnet tracking to intrusion detection*, 2nd Edition. Upper Saddle River, NJ: Addison-Wesley Professional.
Ragucci, J. W., & Robila, S. A. (2006). Societal aspects of phishing. Paper presented at the IEEE Symposium on Technology and Society, New York, NY, June 8-10.
Scarborough, K. E., Rogers, M., Frakes, K. & Martin, C. S. (2008). Digital evidence. In F. Schmalleger and M. Pittaro (Eds.), *Crimes of the Internet*. Upper Saddle River, NJ: Pearson/Prentice Hall.
Sherman, W. (2001, August 1). Internet's cons are pros: Unwary lose $3B a year. *New York Daily News*, 4.
Smith, D. J. (2007). *A culture of corruption: Everyday deception and popular discontent in Nigeria*. Princeton, NJ: Princeton University Press.
Smith, R. G., Holmes, M. N., & Kaufmann, P. (1999). Nigerian advance fee fraud. *Trends & Issues in Crime and Criminal Justice*, *121*, 1-6.
Slatalla, M. and J. Quittner (1995), *Masters of deception: The gang that ruled cyberspace*. New York: Harper Collins.
Suicide of Internet Scam Victim, (2004, January 30). *BBC News*. Access on March 1, 2009 from http://news.bbc.co.uk/2/hi/uk_news/england/cambridgeshire/3444307.stm.
Symantec (2009, February). The state of spam: A monthly report. Symantec Messaging and Web Security. Retrieved on November 20, 2009 from http://eval.symantec.com/mktginfo/enterprise/other_resources/b-

state_of_spam_report_02-2009.en-us.pdf.

Wagner, M. (2003, February 13). Spammers' technology secrets! Exposed! *Information Week*. Retrieved on November 25, 2009 from http://www.informationweek.com/news/showArticle.jhtml?articleID=6900020.

Walker, C. P., Wall, D. S., & Akdeniz, Y. (2000). The Internet, law and society. In Y. Akdeniz, C. P. Walker, & D. S. Wall. (Eds.) *The Internet, law and society* (pp. 3-24). London: Longman.

Wall, D. S. (1999). Cybercrimes: New wine, no bottles? In P. Davies, P. Francis, & V. Jupp, (Eds.), *Invisible crimes: Their victims and their regulation*. London: MacMillan.

Wall, D. S. (2005). Digital realism and the governance of spam as cybercrime. *European journal on criminal policy and research*. *10*, 309-335.

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security. *Police Practice and Research*, *8*(2), 183-205.

Winkler, I. S. & Dealy, B. (1995). Information security technology?...Don't rely on it: A case study in social engineering. Paper presented at the Fifth USENIX UNIX Security Symposium, Salt Lake City, Utah, June, 1995.

Yar, M. (2005). The novelty of "cybercrime": An assessment of routine activity theory. *European Journal of Criminology*. 2(4), 407-424.