2 Cyber Crime Cases

2.1 Fake Websites

Fake websites have become increasingly pervasive and trustworthy in their appearance, generating billions of dollars in fraudulent revenue at the expense of unsuspecting Internet users. Abbasi et al. (2010) found that the growth in profitable fake websites is attributable to several factors, including their authentic appearance, a lack of user awareness regarding them, and the ability of fraudsters to undermine many existing mechanisms for protecting against them. The design and appearance of these websites makes it difficult for users to manually identify them as fake. Distinctions can be made between spoof sites and concocted sites. A spoof site is an imitation of an existing commercial website such as eBay or PayPal. A concocted site is a deceptive website attempting to create the impression of a legitimate, unique and trustworthy entity.

Detecting fake websites is difficult. There is a need for both fraud cues as well as problem-specific knowledge. Fraud cues are important design elements of fake websites that may serve as indicators of their lack of authenticity. First, fake websites often use automatic content generation techniques to mass-produce fake web pages. Next, fraud cues include information, navigation, and visual design. Information in terms of web page text often contains fraud cues stemming from information design elements. Navigation in terms of linkage information and URL names for a website can provide relevant fraud cues relating to navigation design characteristics. For example, it is argued that 70 percent of ".biz" domain pages are fake sites. Fake websites frequently use images from existing legitimate or prior fake websites. For example spoof sites copy company logos from the websites they are mimicking. The fact that it is copied can be detected in the system (Abbasi et al., 2010).

In addition to fraud cues, there is a need for problem-specific knowledge. Problem-specific knowledge regarding the unique properties of fake websites includes stylistic similarities and content duplication (Abbasi et al., 2010).

Abbasi et al. (2010) developed a prototype system for fake website detection. The system is based on statistical learning theory. Statistical learning theory is a computational learning theory that attempts to explain the learning process from a statistical point of view. The researchers conducted a series of experiments, comparing the prototype system against several existing fake website detection systems on a test sample encompassing 900 websites. The results indicate that systems grounded in statistical learning theory can more accurately detect various categories of fake websites by utilizing richer sets of fraud cues in combination with problem-specific knowledge.

A variation of fake websites is fraudulent email solicitation where the sender of an email claims an association with known and reputable corporations or organizational entities. 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 Draw" (Nhan et al., 2009). The email proceeded to ask for the potential victim's personal information.

Nhan et al. (2009) examined 476 fraudulent email solicitations, and found that the three most frequently alleged organizational associations were Microsoft, America Online, and PayPal. Fraudsters also attempt to establish trust through associating with credit-issuing financial corporations and authoritative organizations and groups.

2.2 Money Laundering

Money laundering is an important activity for most criminal activity (Abramova, 2007; Council of Europe, 2007; Elvins, 2003). Money laundering means the securing of the proceeds of a criminal act. The proceeds must be integrated into the legal economy before the perpetrators can use it. The purpose of laundering is to make it appear as if the proceeds were acquired legally, as well as disguises its illegal origins (Financial Intelligence Unit, 2008). Money laundering takes place within all types of profit-motivated crime, such as embezzlement, fraud, misappropriation, corruption, robbery, distribution of narcotic drugs and trafficking in human beings (Økokrim, 2008).

Money laundering has often been characterized as a three-stage process that requires (1) moving the funds from direct association with the crime, (2) disguising the trail to foil pursuit, and (3) making them available to the criminal once again with their occupational and geographic origins hidden from view. The first stage is the most risky one for the criminals, since money from crime is introduced into the financial system. Stage 1 is often called the placement stage. Stage 2 is often called the layering stage, in which money is moved in order to disguise or remove direct links to the offence committed. The money may be channeled through several transactions, which could involve a number of accounts, financial institutions, companies and funs as well as the use of professionals such as lawyers, brokers and consultants as intermediaries. Stage 3 is often called the integration stage, where a legitimate basis for asset origin has been created. The money is made available to the criminal and can be used freely for private consumption, luxury purchases, real estate investment or investment in legal businesses.

Money laundering has also been described as a five-stage process: placement, layering, integration, justification, and embedding (Stedje, 2004).

It has also been suggested that money laundering falls outside of the category of financial crime. Since money-laundering activities may use the same financial system that is used for the perpetration of core financial crime, its overlap with the latter is apparent (Stedje, 2004).

According to Joyce (2005), criminal money is frequently removed from the country in which the crime occurred to be cycled through the international payment system to obscure any audit trail. The third stage of money laundering is done in different ways. For example, a credit card might be issued by offshore banks, casino 'winning' can be cashed out, capital gains on option and stock trading might occur, and real estate sale might cause profit.

The proceeds of criminal acts could be generated from organized crime such as drug trafficking, people smuggling, people trafficking, proceeds from robberies or money acquired by embezzlement, tax evasion, fraud, abuse of company structures, insider trading or corruption. The Financial Intelligence Unit (2008) in Norway argues that most criminal acts are motivated by profit. When crime generates significant proceeds, the perpetrators need to find a way to control the assets without attracting attention to them selves or the offence committed. Thus, the money laundering process is decisive in order to enjoy the proceeds without arousing suspicion.

The proceeds of crime find their ways into different sectors of the economy. A survey in Canada indicates that deposit institutions are the single largest recipient, having being identified in 114 of the 149 proceeds of crime (POC) cases (Schneider, 2004). While the insurance sector was implicated in almost 65 percent of all cases, in the vast majority the offender did not explicitly seek out the insurance sector as a laundering device. Instead, because motor vehicles, homes, companies, and marine vessels were purchased with the proceeds of crime, it was often necessary to purchase insurance for these assets.

When banks are implicated in money laundering, the computer crime is carried out in terms of financial transactions. Proceeds of crime are deposited in the bank and then transferred in such a way that trails are disguised before the money is made available to the criminal again. While it may harm a bank's reputation if it is disclosed that it handles criminal money, as we will see later in this book, criminal money may represent good business for the bank (Harvey and Lau, 2009).

2.3 Bank Fraud

Fisher (2008) describes a US banking fraud case. It involved Jeffrey Brett Goodin, of Azusa, California who was sentenced to 70 months imprisonment as a result of his fraudulent activities. Goodin had sent thousands of e-mails to America Online (AOL's) users that appeared to be from AOL's billing department and prompted customers to send personal and credit card information, which he then used to make unauthorized purchases. The e-mails referred the AOL customers to one of several web pages where the victims could in-put their personal and credit information. Goodin controlled these web pages, allowing him to collect the information that enabled him and others to make unauthorized charges on the AOL users' credit or debit cards.

Bank fraud is a criminal offence of knowingly executing a scheme to defraud a financial institution. For example in China, bank fraud is expected to increase both in complexity and in quantity as criminals keep upgrading their fraud methods and techniques. Owing to the strong penal emphasis of Chinese criminal law, harsh punishment including death penalty and life imprisonment has been used frequently for serious bank fraud and corruption. Cheng and Ma (2009) found, however, that the harshness of the law has not resulted in making the struggle against criminals more effective. The uncertain law and inconsistent enforcement practices have made offenders more fatalistic about the matter, simply hoping they will not be the unlucky ones to get caught.

Financial fraud in the banking sector is criminal acts often linked to financial instruments, in that investors are deceived into investing money in a financial instrument that is said to yield a high profit. Investors loose their money because no investment actually takes place, the instrument does not exist, the investment cannot produce the promised profit or it is a very high-risk investment unknown to the investor. The money is usually divided between the person who talked the investor into the deal and the various middlemen, who all played a part in the scheme (Økokrim, 2008).

Picard (2009) found that IT systems in banks facilitate the commitment of fraud and, at the same time, complicates the investigation. Therefore, there is an attractive opportunity for fraud associated with low risk. What looks like an opportunity from the criminal standpoint represents an inherent risk from within organizations. One opportunity issue concerns the internal operations of a bank. Fraud aims at internal operations and exploits the many weaknesses or avoids the limited controls in place.

Fisher (2008) argues that a system with one-day check clearance in the UK would increase the exposure to cyber crime. He undertook a comparative analysis of the UK and US check-clearance systems, examined the enhanced vulnerability to fraud occasioned by a one-day check clearance system and considered the resulting evidential difficulties encountered in US check fraud prosecution. The introduction of one-day check clearance in the USA heralded an increase in cyber crime banking fraud and a reduction of the ability of the prosecuting authorities to bring cases to court because of the paucity of documentary evidence.

2.4 Advance Fee Fraud

As mentioned in the Introduction, Nigeria-related financial crime is extensive and 122 out of 138 countries at an Interpol meeting complained about Nigerian involvement in financial fraud in their countries. The most notorious type attempted daily on office workers all over the world, is the so-called advance fee fraud. The sender will seek to involve the recipient in a scheme to earn millions of dollars if the recipient pays an advance fee (Ampratwum, 2009).

Fraud can be defined as intentional misrepresentation for the purpose of gain. It is a typical financial crime, often carried out by white-collar criminals. Fraud has existed since the origin of recorded history. The nature of fraud expanded with the introduction of Internet communications, electronic commerce (e-commerce) and electronic business (e-business). Much evidence suggests that technology-based fraud is increasing rapidly in frequency despite law enforcement efforts (Nhan et al., 2009).

Nigerian criminals are approaching potential victims of advance fee fraud e-mail without prior contact. Victims' addresses are obtained from telephone and e-mail directories, business journals, magazines, and newspapers. A typical advance fraud letter describes the need to move funds out of Nigeria or some other sub-Saharan African country, usually the recovery of contractual funds, crude oil shipments or inheritance from late kings or governors (Ampratwum, 2009). This is an external kind of fraud, where advance-fee fraudsters attempt to secure a prepaid commission for an arrangement that is never actually fulfilled or work that is never done.

Victims are often naïve and greedy, or at worst prepared to abet serious criminal offences such as looting public money from a poor African state. The advance fee fraud has been around for centuries, most famously in the form of the Spanish prisoner scam (Ampratwum, 2009: 68):

> In this, a wealthy merchant would be contacted by a stranger who was seeking help in smuggling a fictitious family member out of a Spanish jail. In exchange for funding the "rescue" the merchant was promised a reward, which of course, never materialized.

Advance fee fraud is expanding quickly on the Internet. Chang (2008) finds that this kind of fraud is a current epidemic that rakes in hundreds of millions of dollars per year. The advent of the Internet and proliferation of its use in the last decades makes it an attractive medium for communicating the fraud, enabling a worldwide reach. Advance fee fraudsters tend to employ specific methods that exploit the bounded rationality and automatic behavior of victims. Methods include assertion of authority and expert power, referencing respected persons and organizations, providing partial proof of legitimacy, creating urgency, and implying scarcity and privilege.

Holt and Graves (2007) studied schemes applied in advance fee fraud e-mail. Their study explored the mechanisms employed by scammers through a qualitative analysis of 412 fraudulent e-mail messages. Their findings demonstrate that multiple writing techniques are used to generate responses and information from victims. Half of the messages also requested that the recipient forwarded their personal information to the sender, thereby enabling identity theft as well.

The findings by Holt and Graves (2007) suggest that fraudsters employ deceptively simple messages in an attempt to identify and victimize individuals. Fraudsters 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. Frequent subject lines include "Urgent Attention", "Read and Reply as soon as possible", "Attention Friend", and "From Dr. Mariam Abacha". Lottery notifications typically employ expressions such as "Congratulations" or "Attention Winner", while business messages use expressions like "Payment Agent Needed".

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. Fraudsters 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 messages. In addition to confidentiality, the senders request that they be contacted as quickly as possible. Half of the e-mails examined by Holt and Graves (2007) asked the recipient to provide the sender with personal information.

Nhan et al. (2009) studied fraudulent email solicitation. They analyzed the nature of the solicitation, the nature of the solicitor, and the information asked of the target. Their research was based on two email accounts that captured a total of 476 unsolicited emails identified as suspect in intent over a three-month period. The large majority of emails originated from the United Kingdom (37%) Nigeria (33%). Emails also cam from Taiwan, Russia, China, the Ivory Coast, and France. Many solicitors claimed to be a bank officer (29%), lawyer (27%), and politician (17%).

To generate the trust of targeted victims, solicitors typically generate and include a presentation expected to be appealing to the victim's concern for others. Therefore, many offenders include alleged personal information in their emails. Most commonly, solicitors mentioned that they were married (32%), or they were sick (23%). Others reported being a victim of some social or political event (15%), having children (12%), being somehow related to a victim of a tragic incident (10%), or being the heir (7%) who will soon collect a large sum of money that they will allegedly share (Nhan et al., 2009).

2.5 Malicious Agents

The primary motivation of malicious agents attacking information systems has changed over time from pride and prestige to financial gain (Galbreth and Shor, 2010). A malicious agent is a computer program that operates on behalf of a potential intruder to aid in attacking a system or network. While a computer virus traditionally was the most prominent representative of the malicious agent species, spying agents have become more common. Spying agents transmit sensitive information from the organization to the author of the agent. Another kind of agent is the remotely controlled agents, which provides the attacker with complete control of the victim's machine.

Software is classified as malicious software (malware) based on the perceived intent of the creator rather than any particular features. Malware for profit includes spy ware, botnets, keystroke loggers, and dialers. In a botnet, the malware logs in to a chat system, while a key logger intercepts the user's keystrokes when entering a password, credit card number, or other information that may be exploited. Malicious software can automate a variety of attacks for criminals and is partially responsible for the global increase in cyber crime (Bossler and Holt, 2009).

Bossler and Holt (2009) applied routine activities theory to study malicious agents. According to routine activities theory, direct-contact predatory victimization occurs with the convergence in both space and time of three components: a motivated offender, the absence of a capable guardian, and a suitable target. As opposed to the physical world, the virtual world often ignores the times of criminal activities. Therefore, the activities of potential victims and the websites or files they come in contact with are more important than the times of such activities.

2.6 Stock Robot Manipulation

A computer program was able to manipulate a stock-trading robot linked to Oslo Stock Exchange in Norway. The program generated fake buying and selling orders that terminated each other, while at the same time influencing stock prices. Then the program performs real buying and selling orders where stocks were bought at low prices and sold at high prices. This kind of stock value manipulation is illegal in Norway, and two stock traders were caught in 2010 (DN, 2010).

2.7 Identity Theft

Miri-Lavassani et al. (2009) found that identity fraud is the fastest growing white-collar crime in many countries, especially in developed countries. In 2008, the number of identity fraud victims increased by 22 percent to 9.9 million victims.

Intelligence is important as a source of information for crime analysis. An example of crime analysis is the identity fraud measurement model developed by Miri-Lavassani (2009). The five-dimensional measurement model is concerned with: (i) types of identity fraud, (ii) impact of identity fraud, (iii) methods of identity fraud, (iv) transnational identity fraud, and (v) business identity fraud risks. Financial institutions in Canada were surveyed for empirical data collection. Factor analysis was employed on the data for evaluating dimensions and contents of each dimension in the model, resulting in a four-dimensional rather than five-dimensional measurement model, where methods of identity fraud includes transnational identity fraud.

Types of identity fraud reflect the way in which identity thieves use the stolen or forged identities of other individuals to commit unlawful acts without the knowledge of the victims. Types of identity fraud can be measured by the numbers of credit card fraud; unauthorized use of utilities or services; insurance fraud; investment fraud; fraudulent loans and mortgages; bank fraud; new credit cards and utility (internet, phone, etc.) applied for, insurance policies issued, bank accounts opened by identity thieves; misuse of existing credit cards, utility insurance policies, and bank accounts by identity thieves.

Impact of identity fraud can be measured in terms of direct costs of identity fraud to business; direct costs of fraud to customers; direct non-financial impact of fraud on business (such as damaged reputation); direct non-financial impact of fraud on customers (such as damaged credit records and record history); the amount of time individual fraud victims spend to resolve problems; the amount of time business spend to resolve fraud problems; emotional and psychological impact of fraud on victims; and emotional and psychological impact of fraud on victims families.

Methods of identity fraud refer to the methods that have been used by identity thieves for acquiring the identifiers of identity fraud victims. Methods include main theft; filling fraudulent address changes; theft or loss of wallet or purse; phishing; vishing; employment records; theft by breaking and entering; theft through internet, computer viruses, spy ware, and worms; telephone solicitation; extortion or sabotage by an insider; and extortion or sabotage by an outsider. Transnational methods include measuring identity fraud incidents in the country while the identity thieves are located in other countries; and measuring worldwide identity fraud originating from Canada.

Business identity fraud risks includes the business itself; the employee of the organization; and other organizations and customers that work with the organization.

The study by Miri-Lavassani et al. (2009) resulted in a measurement model that includes 27 indicators and four factors. They argue that in the absence of a widely developed and employed identity theft measurement model, many misconceptions about the problem of identity fraud have emerged. One example is the biased perception that the use of the Internet for electronic business increases the risk of exposure to identity fraud.

2.8 Digital Piracy

Digital piracy is defined as the illegal copying of digital goods, software, digital documents, digital audio (including music and voice), and digital video for any other reason other than to backup without explicit permission from and compensation to the copyright holder (Higgins, 2007). The Internet facilitates digital piracy because the network allows crime to take place detached from the owner. For example, digital music piracy is committed through a multitude of modus operandi (Higgins et al., 2008). The issue of digital piracy has become a topic of immense concern, such that it has attracted the attention of legislators, academics as well as business executives (Moore and McMullan, 2009).

Higgins (2007) studied the links between low self-control, rational choice, value, and digital piracy. His results show that low self-control has direct and indirect effects on intentions to digital piracy. Further, his study shows that low self-control has indirect links with a modified version of situational factors such as value. These results indicate that low self-control and rational choice theory maybe compatible theories that can explain digital piracy.

For the established music recording and distribution industry, the appearance of Napster, the first peer-to-peer (P2P) network software, was a disruptive event with substantial impact. Napster was created in 1999 by the 18 year-old Shawn Fanning as a software application aimed at simplifying the process of finding and sharing music files online. The software application made it possible to replicate and circulate highly compressed music files at no cost. Napster network gained enormous popularity and generated an enormous selection of downloadable music. Millions of users connected to the network to share and swap copyright-protected music without explicit permission (Bachmann, 2007).

In 2003, the recording industry in the US initiated a number of lawsuits against P2P network users to stop them from illegally sharing music files. A lawsuit was also filed against Napster. The accusations against Napster, Inc. were based on the architecture of the system. Napster used centrally located and company owned servers to generate and maintain lists of connected users and the music files they provided (Bachmann, 2007: 214):

> While the actual file transactions were conducted directly between the users, these central servers also facilitated the connections between users and initiated the music file downloads.

Because of the centralized architecture, the recording industry defined Napster as a listing service that offered a search engine, a directory, an index, and links, and was thus seen as being ultimately responsible for the music file transactions and the copyright violations they caused.

In an empirical study of online music pirates, Bachmann (2007) found that file sharing and music downloading have to be analyzed separately when studying impacts of the enforcement of copyright laws on file sharing communities and the music downloading individuals. The results show that Internet users in the US are well aware of the circumstance that legal prosecution is only targeting the sharing of music files.

In a different study of online music pirates, Higgins et al. (2008) found that trajectories of digital piracy are tied to neutralization toward digital piracy. Neutralization includes denial of responsibility, denial of injury, denial of victim, condemnation of condemners, and appeal to higher loyalty. The findings of their study indicate that many individuals will take a deviant behavior from social controls to allow themselves to pirate music without developing a pirating identity. Individuals apply different forms of neutralization for a self-serving purpose as they detach themselves from the criminality of the behavior.

While Higgins et al. (2008) studied neutralization in relation to social control, Moore and McMullan (2009) studied neutralization in direct relation to digital piracy. They found that all participants in their study indicated support, though to varying extent, for neutralization techniques. One of the neutralization techniques found was that everyone else is doing it. However, only sixteen percent of the study participants indicated this technique, which surprised one of the study's authors as they expected more individuals to associate with this belief.

2.9 Intellectual Property Crime

Intellectual property crime is a serious financial concern for car manufacturers, luxury goods makers, media firms and drug companies. Most alarmingly according to Interpol (2009), is that counterfeiting endangers public health, especially in developing countries, where the World Health Organization estimates more than 60 percent of pharmaceuticals are fake goods.

Interpol (2009) launched a new database on international intellectual property crime, which was created to fill the void in seizure data collated by various international bodies and the private sector. Of 1,710 entities in the database, checks against other Interpol databases revealed links to credit card and currency counterfeiting, fraud, money laundering, theft, violent crimes and trafficking in human beings, weapons and drugs. This demonstrates the role of organized crime in large-scale counterfeiting and piracy.

Intellectual property's rising value in the production of wealth has been mirrored by its increasing vulnerability to crime. Snyder and Crescenzi (2009) found that intellectual property crime is often linked to cyber crime, and they explored the risks of crime inherent in intellectual capital and a distributed cyber environment to demonstrate that traditional legal remedies are largely ineffective to protect property rights. Unlike cash or paintings, for example, which require the criminal to enter a vault or museum and subsequently carry off the stolen objects, intellectual property crime requires only that the criminal make an electronic copy. The classic remedy in cases of theft is to return the property to its original owner. Today, downloaded movies and music files are as useful as the originals.

2.10 Internet Gambling

Internet gambling is a global issue that has an effect upon all countries independent of their local laws prohibiting or allowing gambling to take place. Fidelie (2009) asked the question whether Internet gambling is an innocent activity or cyber crime. She found a very unclear legal status of Internet gambling. Gambling is an industry that has undergone many changes throughout its existence. Gambling is generally controlled by state governments in an exercise of their police powers. However, Internet gambling's interstate and international scope necessitates its governance by international law.

Pontell et al. (2007) studied the case of Antigua for illegal offshore Internet gambling. Antigua is a small Caribbean island that gained its independence from Britain in 1981. An Internet gambling site called World Sports Enterprise (WSE) was launched in 1997 and is located on the island. Customers were required to transmit $300 before they were permitted to gamble, and the WSE exacted ten percent off the top of each wager. In its first fifteen months of operation the company took in $3.5 million. It is argued that organized crime has infiltrated the Antiguan gambling endeavor and that underage participants are allowed to play.

Because of the great difficulty in banning Internet gambling, Fidelie (2009) recommends that governments all over the world should regulate and tax online business ventures. She suggests that because of the unclear legal status of Internet gambling, there must be a legislation explicitly defining what is and is not permissible activity, as well as an emphasis on regulation by world governments and self-regulation by the Internet gambling businesses.