

Computer Crime and Computer Fraud

University of Maryland
Department of Criminology and Criminal Justice
Fall, 2004

Report to the
Montgomery County Criminal Justice Coordinating Commission
By
Michael Kunz & Patrick Wilson

This report was prepared in part as fulfillment of requirements in CCJS 604 and CCJS 605 for the Professional Masters Degree in the Department of Criminology and Criminal Justice. We express thanks to Dr. Charles Wellford, Dr. Doris MacKenzie, and Jean McGloin for assistance with this report.

Executive Summary

The past several decades have brought a vast increase in the availability of electronic resources. With this increased availability has come a new form of criminal activity that takes advantage of electronic resources, namely computer crime and computer fraud. Currently, these new forms of crime are burgeoning and pose a new and lasting challenge to law enforcement agencies at all levels in how to prevent, investigate, and prosecute these crimes. Law enforcement agencies from the local to the federal level are beginning to institute specific units devoted to handling computer-related offenses, but there does not currently exist a uniform method to define and address computer crime and computer fraud.

With this case study, we intend to analyze what the current level of understanding is regarding computer crime and computer fraud, as well as what is being done by law enforcement agencies to deal with these offenses. Using this information, we provided specific recommendations regarding computer-related offenses in the future including:

- Uniform definition
- Organizational requirements and procedures
- Tools necessary to successful operation of computer crime units

Introduction

Throughout the past several decades there have been numerous advances in electronic resources. Technologies such as cellular phones, pagers, home computers, the Internet, websites, and palm pilots have added another dimension to crime. That dimension involves increased methods at criminals' disposal to commit certain crimes along with increased locations in which crimes can occur. For example, property crimes no longer have to involve face-to-face contact between the criminal and the victim. In the past, property crimes usually involved a criminal breaking into a victim's house or grabbing a purse from a person on the street. Today, criminals can commit property crimes from the comfort of their own homes against people who live on the other side of the world through the use of computers.

Computer crime poses a daunting task for law enforcement agencies because they are highly technical crimes. Law enforcement agencies must have individuals trained in computer science or computer forensics in order to properly investigate computer crimes. Additionally, states must update and create legislation, which prohibits computer crimes and outlines appropriate punishments for those crimes. Computer crimes will likely become more frequent with the advent of further technologies. It is important that civilians, law enforcement officials, and other members of the criminal justice system are knowledgeable about computer crimes in order to reduce the threat they pose.

Recognizing the emerging problems resulting from computer crime, the Montgomery County Criminal Justice Coordinating Commission requested the following study in order to gain a detailed understanding of the harms caused by this modern crime form. Specifically, the Commission asked that we research: the definitions of computer

crime, the different types of computer crime, the scope of the national and local problem, the legislation that was created to punish offenders, the professional organizations that combat computer crime, the resources that are available to educate the public about computer crimes, and the underlying reasons for law enforcement agencies successes in combating computer crime. In addition, we have been asked to furnish a list of recommendations for the Commission on how they should act in regards to combating computer crime.

Defining the Problem

Currently, when law enforcement agencies talk about computer crime, they may hold very different views of what that category of crime entails. Does computer crime include every crime in which a computer is involved? Should the theft of a laptop constitute computer crime? Are traditional crimes, such as stalking, theft, and fraud that are now making use of digital resources considered computer crimes, or simply traditional crimes that incorporate a new means of accomplishment? Should the existing legal framework be used as a response for these offenses, or are new laws and regulations required? These sorts of questions are what law enforcement agencies are currently addressing. Law enforcement needs to be able to adequately confront these new forms of crime, as well as determine the changing nature and form they are taking. In order to accomplish this, uniform definitions are a requirement. As stated by Marc Goodman, the former head of the Los Angeles Police Department's Internet Unit,

Defining criminal phenomena is important because it allows police officers, detectives, prosecutors, and judges to speak intelligently about a given criminal offense. Furthermore, generally accepted definitions facilitate the aggregation of statistics, which law enforcement can analyze to reveal previously undiscovered criminal threats and patterns. (Goodman, 2001)

Uniform definitions for computer crime and computer fraud are essential for an in depth discussion regarding what is currently known, as well as what is being done to address the offenses that fall in these categories. Additionally, the creation of uniform definitions will aid various law enforcement agencies in understanding their role, as well as what resources are required.

Computer Crime

The general heading of computer crime can potentially cover an array of offenses. By examining several existing definitions of computer crime, as well as elements suggested as essential to a uniform definition, a better understanding of what computer crime entails will be created. Some have defined computer crime as any offense that uses or somehow involves a computer. The Department of Justice has defined computer crime as "...any violation of the criminal law that involves the knowledge of computer technology for its perpetration, investigation, or prosecution." Understandably, critics have been quick to indicate that while this definition may encompass computer crimes, it doesn't necessarily exclude other forms of crime (Goodman, 2001). Similarly, definitions such as the one utilized by the Business Software Alliance, a public education and awareness organization, may be too restrictive. They classify computer crime as illegal activities that make use of electronic systems as a means to affect the security of computer systems and computer data. The organization delineates this from computer-related offenses, which simply use or are related to computer resources.

Other definitions have employed limitations to a broad definition to more narrowly define the term. The working definition for the National Institute of Justice was created by incorporating the idea that computers can be used as the means to commit a crime, be the target of the offense, or act as a storage receptacle for the offense. Using these parameters, they defined computer crime as offenses committed in an "electronic environment" for economic gain or to cause damage or harm to others (U.S. Department of Justice, 2001). An additional definition has utilized existing criminological theory to

clarify what is meant by computer crime. Gordon, and colleagues adapted Cohen and Felson's Routine Activities Theory – which says crime occurs when there is a suitable target, a lack of capable guardians, and a motivated offender – to determine when computer crime takes place. In their interpretation, computer crime is the result of offenders "...perceiving opportunities to invade computer systems to achieve criminal ends or use computers as instruments of crime, betting that the 'guardians' do not possess the means or knowledge to prevent or detect criminal acts." (Gordon, Hosmer, Siedsma, Rebovich, 2003)

A number of sources highlight important elements they believe essential to defining computer crime. Examining these suggested elements and considering them in a unified context would be beneficial in the creation of a uniform definition of computer crime. As defined by the California Penal Code, those who "...knowingly and without permission uses or causes to be used..." any element of a computer or its service can be held liable of committing an offense (National Security Institute, 2004). In outlining computer crime, the inclusion of an element that clearly describes the unauthorized use of computer resources is a reasonable first step. Additionally, a uniform definition should be comprehensive enough to cover the different roles a computer may take in the offense, be it the target of the offender, the instrument used to commit the offense, or simply incidental to the crime (Gordon, Hosmer, Siedsma, Rebovich, 2003). The definition should also be designed to protect and indicate violations of the confidentiality, integrity and availability of computer systems (Goodman, 2001). Thus, it should safeguard against unauthorized access to computers and the data stored on them, not allow that data to be

altered, and ensure it remains fully accessible and properly functioning when needed by the authorized user.

Using these parameters, the uniform definition for computer crime should clearly outline what constitutes an offense. Compiling these resources leads to the following working definition: using or causing the use of a computer resource for the purpose of illicitly gaining goods or resources, or causing harm to another entity. The definition should be flexible enough to apply to situations where the computer resource is the instrument of the perpetrator, the victim, or auxiliary to the crime. The definition should also be adaptable to the rapidly changing face of the digital world.

Computer Fraud

Computer fraud can be described as a subset of computer crime. Computer fraud uses electronic resources to present fraudulent or misrepresented information as a means of deception. According to the Department of Justice, the fraudulent activities currently taking place that use electronic resources are largely an extension of traditional existing fraud activities exploiting a new medium (National White Collar Crime Center, 2002). The Bureau of Justice Statistics outlines fraud as “...the intentional misrepresentation of information or identity to deceive others...” and adds the qualifier of “use of electronic means” to delineate computer fraud (Rantala, 2004). Similarly, the Department of Justice defines Internet fraud as fraud which uses any component of the Internet to accomplish the intended fraudulent activity (National White Collar Crime Center, 2003). Presumably, this definition could be adapted for computer fraud, by requiring the use of a computer or other electronic resource in the commission of the fraudulent act.

In general, computer fraud should contain the same basic definition of traditional fraud, while employing new qualifiers that adapt its use for electronic resources.

Computer Crime Types

There exists a constantly expanding list of the forms computer crime and computer fraud can take. Fortunately, these crime types fall into overarching groups of criminal actions. Many traditional crimes, such as fraud, theft, organized crime rings, prostitution, stalking, and child pornography have been incorporated into the digital world. Offenders may find new opportunities to perpetrate their crimes using this new digital medium. The National White Collar Crime Center notes, "...computers can be 'used as tools to commit traditional offenses.' This means that the functions specific to computers, such as software programs and Internet capabilities, can be manipulated to conduct criminal activity." (National White Collar Crime Center, 2002) Additionally, as explained previously, computer crimes can also be grouped into categories in which computers themselves are either the target or victim of an offense, or simply incidental to the act itself. Aside from traditional crimes that have been adapted to utilize electronic resources, there are also a number of offenses that exist specifically due to the accessibility of computer resources.

Traditional Crime Types

Some of the traditional crimes now taking place on computers include fraud, theft, harassment, and child pornography. Computer fraud consists of crimes such as online auction fraud, identity theft, financial and telecommunications fraud, credit card fraud, and various other schemes. Theft crimes, as related to computer crime, include categories such as monetary, service and data theft, and piracy. Harassment offenses include online harassment and cyberstalking. Child pornography crimes include both the transmission of

media that exploits children, as well as solicitation to commit sexual crimes against minors.

Computer Fraud

Computer fraud is one of the most rapidly increasing forms of computer crime. Computer fraud is also commonly referred to as Internet fraud. Essentially, computer/Internet fraud is “any type of fraud scheme that uses one or more components of the Internet-such as chat rooms, e-mail, message boards, or Web sites to present fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme” (Department of Justice, 2001). There are multiple forms of Internet fraud.

One type of Internet Fraud is the Nigerian e-mail fraud. In this particular crime, the victim receives e-mail from an alleged son of a deceased Nigerian head of state, who happens to be the heir to millions of dollars that are hidden in accounts all over the world. The e-mail recipient is lead to believe that they are to receive some of the fortune. All that is asked in exchange is a lawyer’s fee of several thousand dollars in order to claim the money. The people who fall prey to this crime send their money and never receive their expected fortunes (Koinange, 2002). An example of this form of fraud can be found in the appendix. Be sure to notice that the example isn’t the Nigerian e-mail fraud as the e-mail has apparently been sent from someone of Asian descent. The Nigerian e-mail fraud seems to be spreading to different parts of the world.

The Internet Crime Complaint Center has identified several other forms of Internet fraud crimes. The additional forms include:

- Advance Fee Fraud Schemes-in, which the victim is required to pay significant fees in advance of receiving a substantial amount of money or merchandise. The fees

are usually passed off as taxes, or processing fees, or charges for notarized documents. The victim pays these fees and receives nothing in return. Perhaps the most common example of this type of fraud occurs when a victim is expecting a large payoff for helping to move millions of dollars out of a foreign country. The victim may also believe he has won a large award in a nonexistent foreign lottery.

- Business/Employment Schemes-typically incorporate identity theft, freight forwarding, and counterfeit check schemes. The fraudster posts a help-wanted ad on popular Internet job search sites. Respondents are required to fill out an application wherein they divulge sensitive personal information, such as their date of birth and Social Security number. The fraudster uses that information to purchase merchandise on credit. The merchandise is sent to another respondent who has been hired as a freight forwarder by the fraudster. The merchandise is then reshipped out of the country. The fraudster, who has represented himself as a foreign company, then pays the freight forwarder with a counterfeit check containing a significant overage amount. The overage is wired back to the fraudster, usually in a foreign country, before the fraud is discovered.
- Counterfeit Check Schemes- a counterfeit or fraudulent cashier's check or corporate check is utilized to pay for merchandise. Often these checks are made out for a substantially larger amount than the purchase price. The victims are instructed to deposit the check and return the overage amount, usually by wire transfer, to a foreign country. Because banks may release funds from a cashier's check before the check actually clears, the victim believes the check has cleared and wires the money as instructed. One popular variation of this scam involves the purchase of automobiles listed for sale in various Internet classified advertisements. The sellers are contacted about purchasing the autos and shipping them to a foreign country. The buyer, or person acting on behalf of a buyer then sends the seller a cashier's check for an amount several thousand dollars over the price of the vehicle. The seller is directed to deposit the check and wire the excess back to the buyer so they can pay the shipping charges. Once the money is sent, the buyer typically comes up with an excuse for canceling the purchase, and attempts to have the rest of the money returned. Although the seller does not lose the vehicle, he is typically held responsible by his bank for depositing a counterfeit check.
- Credit/Debit Card Fraud-is the unauthorized use of a credit/debit card to fraudulently obtain money or property. Credit/debit card numbers can be stolen from unsecured web sites, or can be obtained in an identity theft scheme.
- Freight forwarding/Reshipping-the receiving and subsequent reshipping of an on-line ordered merchandise to locations usually abroad. Individuals are often solicited to participate in this activity in chat rooms, or through Internet job postings. Unbeknownst to the reshipper, the merchandise has been paid for with fraudulent credit cards.
- Identity theft- occurs when someone appropriates another's personal information without his or her knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business,

sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application to a fraudulent Internet job posting.

- Investment Fraud- an offering that uses fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities.
- Non-delivery of Goods/Services-merchandise or services that were purchased or contracted by individuals on-line are never delivered.
- Phony Escrow Services-in an effort to persuade a wary Internet auction participant, the fraudster will propose the use of a third-party escrow service to facilitate the exchange of money and merchandise. The victim is unaware the fraudster has spoofed a legitimate escrow service. The victim sends payment or merchandise to the phony escrow and receives nothing in return.
- Ponzi/Pyramid Schemes-investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits. However, no investments are actually made by the so called “investment firm”. Early investors are paid returns with the investment capital received from subsequent investors. The system eventually collapses and investors do not receive their promised dividends and lose their initial investment.
- Spoofing/Phishing- a technique whereby a fraudster pretends to be someone else’s email or web site. This is typically done by copying the web content of a legitimate web site to the fraudster’s newly created fraudulent web site. Phishing refers to the scheme whereby the perpetrators use the spoofed web sites in an attempt to dope the victim into divulging sensitive information, such as passwords, credit card and bank account numbers. The victim, usually via email is provided with a hyperlink that directs hi/her to a fraudster’s web site. This fraudulent web site’s name closely resembles the true name of the legitimate business. The victim arrives at the fraudulent web site and is convinced by the sites content that they are in fact at the company’s legitimate web site and are tricked into divulging sensitive personal information. Spoofing and phishing are done to further perpetrate other schemes, including identify theft and auction fraud. (National White Collar Crime Center 27-8).

Phishing

The Anti-Phishing Working Group defines Phishing as “a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.” (Anti-Phishing Working Group, 2004). An example of a phishing website can be seen in Figure 1. In this particular phishing incident, an unsuspecting person would receive an e-mail with a link

to a website. Upon clicking on the link, the victim would enter a site, such as the one below that appears to be a legitimate e-bay website. However, upon closer review, the

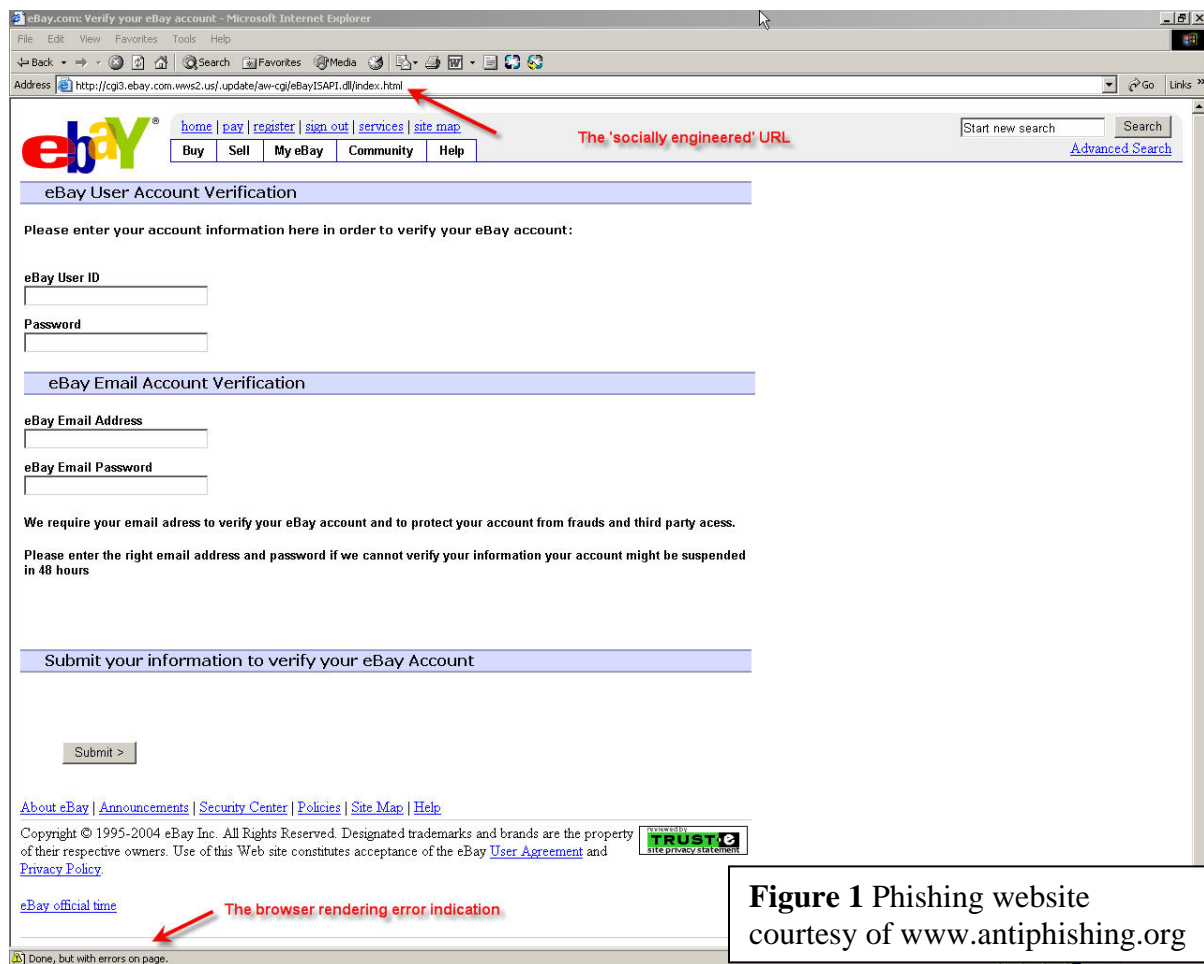


Figure 1 Phishing website
courtesy of www.antiphishing.org

URL is different. This victim, failing to notice the generic URL, would supply the Phisher with their e-bay username, password and e-mail address.

Brian Krebs recently published an example of a phishing incident in the Washington Post. Krebs explained the story of William Jackson of Katy, Texas. Jackson received e-mail from what appeared to be PayPal payment offices. The e-mail warned him that his account would be suspended until he updated it with financial information. The e-mail provided a link for Jackson to the website where he could update his information. He entered in credit card numbers, bank numbers, social security numbers

and other personal identification information. The website ended up being fraudulent and Jackson lost several hundred dollars (Krebs, 2004). William Jackson could have lost much more money as a result of the Phishing website he had inadvertently entered.

Theft Computer Crimes

Computer crimes involving theft are very diverse. The gaining of access and removal of property through the use of electronic resources generally defines theft computer crimes. This property may include money, service, programs, data, or computer output, and computer time (Rushinek & Rushinek, 1993), (Haugen & Selin, 1999). In addition, altering computer input or output without authorization, destroying or misusing proprietary information, and the unauthorized use of computer resources (theft of computer time) can be considered theft-related computer crimes.

Internet piracy is a more prominent form of theft in a digital medium. Piracy is the act of duplicating copyrighted material without authorization (Business Software Alliance, 2004). For the past few years, private and law enforcement organizations have been putting a concentrated effort on stopping this offense. Organizations such as the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) routinely engage in both civil as well as criminal lawsuits to curb piracy. The MPAA alone estimate their potential revenue lost because of piracy to be over three billion dollars a year. (Motion Picture Association of America, 2004)

An example of this type of crime can be seen locally. Kishan Singh, a Lanham, Maryland resident recently plead guilty to operating a pay-for-access website that provided pirated software with the copy-protection elements removed or disabled. The

pirated works he created and distributed using computer resources are valued at between 70,000 and 120,000 dollars (Department of Justice, 2004).

Unauthorized Access

Unauthorized access is a prerequisite to many forms of computer crimes and computer fraud. This form of crime amounts to electronic intrusion, or gaining access to resources via a computer resource without permission. Unauthorized access may occur both on individuals' personal computers, as well as in the workplace. One major form of unauthorized access is known as hacking. Hacking is "...the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access." (Rushinek & Rushinek, 1993) As stated previously, unauthorized access may be a gateway to commit other offenses.

An instance of unauthorized access recently investigated by the Federal Bureau of Investigation involves Alexey V. Ivanov, who was charged with computer intrusion, computer fraud, and extortion, among other things.

Those charges stemmed from the activities of IVANOV (sic) and others who operated from Russia and hacked into dozens of computers throughout the United States, stealing usernames, passwords, credit card information, and other financial data, and then extorting those victims with the threat of deleting their data and destroying their computer systems. (Department of Justice, 2003)

As can be seen in this case, unauthorized access to computer resources was a charge in itself, as well as a method to commit larger more elaborate computer-related crimes.

Denial of Service

A denial of service attack is a targeted effort to disrupt a legitimate user of a service from having access to the service. This may be accomplished through a number of methods. Offenders can limit or prevent access to services by overloading the available

resources, changing the configuration of the service's data, or physically destroying the available connections to the information (CERT, 2001).

Crimes of this type have been perpetrated against major online entities, such as Yahoo.com, eBay.com, CNN.com, and Buy.com. In these crimes, offenders most often attempt to overload the sites with electronic connections in order to disrupt service to legitimate users (CNNMoney, 2000).

Computer Invasion of Privacy

Computer invasion of privacy is another form of computer crime proscribed in state legislatures. Virginia Code title 18.2 chapter 5, article 7.1 section 152.5 declares:

A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit, or any other financial or personal information relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.

The full text version of this state law can be found in the appendix B.

Unauthorized Use of a Computer, Computer System, or Computer Network

Another form of computer crime that is prohibited by most states is unauthorized use of a computer, computer system, or computer network. The state of Maryland outlines this crime in Maryland Annotated Code Article 27 section 146:

a person may not intentionally, willfully and without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services. (2) A person may not intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these services to (i) cause the malfunction or interrupt the operation of a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these

systems or services; or (ii) alter, damage, or destroy data or a computer program stored, maintained, or produced by a computer, computer network, computer system, computer services, computer data base, or any part of these systems or services. (3) A person may not intentionally, willfully, and without authorization: (i) identify or attempt to identify any valid access codes; or (ii) distribute or publicize any valid access codes to any unauthorized person.

The full text version of this state law can be found in the appendix B.

Harmful Content Crimes

The National Institute of Justice groups offenses with an intent to cause harm to others as harmful content crimes (U.S. Department of Justice, 2001). Included in this category are child pornography and exploitation crimes, harassment, stalking, and malicious programs and use of computer resources.

Online Pornography

Online child pornography is defined by pedophiles using computer resources to distribute illegal media of and to minors, as well as engaging in actions to sexually exploit children. “According to 18 USC 2252 and 18 USC 2252A, possessing or distributing child pornography is against federal law and under 47 USC 223 distributing child pornography of any form to a minor is illegal. (Business Software Alliance, 2004) At the national level, the FBI’s Innocent Images National Initiative, an element of their Cyber Crimes Program, investigates these types of crimes and coordinates with regional authorities (FBI, 2004).

Online harassment

Online harassment is unwanted contact by offenders that may negatively impact a victim’s livelihood, well-being, and mental or emotional state. One of the most common forms online harassment takes is that of cyberstalking.

Cyberstalking

In the loosest sense of the term, cyberstalking is using a computer in the perpetration of the traditional crime of stalking. The traditional crime of stalking usually involves “harassing and threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person’s home or place of business, making harassing phone calls, leaving messages or objects, or vandalizing a person’s property” (United States 1). Cyberstalker involves the use of a computer in the perpetration of those acts. People can cyberstalk others by sending harassing or threatening messages through e-mail, instant messaging, or by posting messages on websites/chat rooms. However, there are other, unconventional ways to cyberstalk an individual.

An example of an unconventional cyberstalking incident took place in California in April of 2000. In this case, Gary Dellapenta plead guilty to charges that he tried to solicit the rape of a female social contact (Simpson, 2000). Dellapenta posed as the victim in online chat rooms and created personal ads for the woman claiming she had always fantasized about being raped. He replied to the ads responses by giving away the woman’s personal information, including tips to bypass her home’s security system. Six of the responders to the personal ad showed up at her house telling her they would like to rape her. In the end, the FBI collaborated with the LA district attorney’s office and the Sheriff to apprehend Dellapenta. He was convicted and sentenced to six years in prison (Simpson, 2000). Additionally, Spam – unwanted and uninvited electronic communications – can be interpreted as a form of online harassment.

Spam

Another form of computer crime is spam mail. Spam mail is the distribution of bulk e-mail that offers recipients deals on products or services. The purpose of spam mail is to make customers think they are going to receive the real product or service at a reduced price. However, before the deal can occur, the sender of the spam asks for money, the recipients' credit card number or other personal information. The customer will send that information and never receive the product nor hear from the spammer. The case of Jeremy Jaynes is a prime example of what a criminal can do with spam mail. Jaynes recently became the nation's first convicted purveyor of spam mail when he was found guilty in Leesburg, Virginia (AP, 2004). Apparently, Jaynes was able to send out over 10 million spam e-mails a day offering such products as software to remove personal information, and investment strategies (AP, 2004). During his trial, lawyers learned that Jaynes would receive anywhere between 10,000 to 17,000 responses a month to his spam mail. Depending on the number of responses Jaynes received, he could earn up to \$750,000 per month (AP, 2004). The details of his apprehension have not been revealed (AP, 2004).

Malicious Programs and Computer Resource Use

In addition to traditional crimes occurring on the electronic resources, there are crimes that exist explicitly due to the availability of technology. These crimes, which include denial of service attacks, malicious programs, viruses, and instances of cyberterrorism are designed to disrupt and negatively impact entities in both the digital and real world. As explained in the FBI Law Enforcement Bulletin, "...crimes which represent traditional offenses, perpetrated in new and, perhaps, more effective ways,

differ from pure-play computer crimes, which involve a computer system as the direct target of attack.” (Goodman, 2001)

Malicious Programs/Viruses

Viruses and malicious programs can potentially impact a massive amount of individuals and resources. These programs are intended to cause electronic resources to function abnormally and may impact legitimate users access to computer resources. For instance, the “Melissa” virus released in early 1999 contaminated 1.2 million computers used by U.S. businesses, impacted computer resources throughout the U. S. and Europe, and is estimated to have created eighty million dollars in damages worldwide (Computer Crimes and Intellectual Property Section, 2003).

An example of a malicious program can be seen in the investigation of Claude R. Carpenter, an Internal Revenue Service systems technician who plead guilty to inserting malicious code into IRS three computer systems, which was designed to erase all of the data from these systems. Carpenter’s motivation for these actions was a result of learning of plans for him to be dismissed from his position. He discovered a draft of his dismissal letter after gaining unauthorized access to his supervisor’s computer (Department of Justice, 2001).

Cyberterrorism

Cyberterrorism is the adaptation of terrorism to computer resources, whose purpose is to cause fear in its victims by attacking electronic resources.

...[Cyberterrorism] is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. (Denning, 2000)

What Has Been Done to Combat Computer Crime

Legislation

Perhaps the biggest efforts that have been taken to combat computer crime come in the form of state legislation that outlines different computer crimes and punishments. Crimes outlined in state legislation are similar to the crimes listed above in the types of computer crimes. Crimes such as: cyberstalking, computer fraud, spam, and unauthorized access are proscribed in multiple states legislature. A number of state laws on computer crime can be found in Appendix B. In addition to the state legislation, there have been a number of federal laws created to battle computer crime. For example, the Computer Fraud and Abuse Act established in 1986, defines the federal punishments for certain types of crimes involving the use of a computer.

The USA PATRIOT Act passed in October 2001 provided several sections which expanded the capabilities of law enforcement officials in investigating computer crime. Section 217 allows victims of computer trespassing to have law enforcement officials monitor the computer trespasser(s). Section 220 allows law enforcement officials to seek nationwide warrants for e-mail. Section 814 provides penalties for cyberterrorism. Finally, section 816 calls for the development of computer forensics laboratories and training for law enforcement officers in computer-crime related investigations. The full text version of the aforementioned sections of the USA Patriot Act can be found in appendix C.

Internet Crime Complaint Center

In May of 2000, the FBI with the assistance of the White Collar Crime Center opened the Internet Crime Complaint Center or as it was formerly known, the Internet

Fraud Complaint Center. Since its inception, the ICCC has developed in to the main collection center for Internet fraud complaints (Online Fraud and Crime: Are Consumers Safe? 6). When complaints are made online to the ICCC, “supervisory Special Agents, along with Internet fraud specialists review those complaints when they come in and they link those complaints with others that may have been previously received.” (Online Fraud and Crime: Are Consumers Safe? 7). Subsequently, the ICCC disseminates all pertinent information to the appropriate law enforcement agencies on the Federal, State, and local level (Online Fraud and Crime: Are Consumers Safe? 7).

During its first year, the ICCC received roughly 30,500 valid criminal complaints concerning computer/Internet fraud (Online Fraud and Crime: Are Consumers Safe? 11). Of these complaints, the ICCC was able to submit “545 investigative reports encompassing over 3,000 complaints to 51 of 56 FBI field divisions and 1,507 local and state law enforcement agencies. ICCC has also referred 41 cases encompassing over 200 complaints to international law enforcement agencies. The ICCC has received complaints of victims from 89 different countries” (Online Fraud and Crime: Are Consumers Safe? 11). The ICCC has continued to help law enforcement over the past couple of years. Those who are victims of Internet fraud can file a complaint at the ICCC’s website.

Professional Organizations

There exists a number of professional law enforcement organizations designed to provide training and investigative resources for computer crime and computer fraud. These agencies work independently, as well as with regional law enforcement. Many of these organizations are elements of federal law enforcement agencies.

The Department of Justice's Computer Crime and Intellectual Property Section maintains the National Cybercrime Training Partnership. The purpose of this group is to "...provide guidance and assistance to local, state, and federal law enforcement agencies in an effort to ensure that the law enforcement community is properly trained to address electronic and high technology crimes." (National White Collar Crime Center, 2002) This consortium is made up of law enforcement members from federal, state, and local agencies, and aims to improve the ability of law enforcement agencies to address computer crimes. They have designed a number of training programs for officers and prosecutors related to computer crime and computer fraud. The major areas of focus of these training courses are electronic crime scene investigation, data recovery and analysis, use of the Internet as an investigative tool, and training for instructors (Williams).

The National Institute of Justice's National Law Enforcement and Corrections Technology Center (NLECTC) is also a training and preparations resource for law enforcement agencies. The NLECTC's focus is on providing information on tools available to law enforcement. They operate an equipment standards and testing program, offer training for the use and incorporation of new equipment into agencies, and act as a clearinghouse for resources related to these topics. Additionally, NLECTC offers

electronic crime information and training to regional agencies. Their resources include computer forensics, a guide to implementing information technology in law enforcement agencies, collaborating to address computer crime issues, and coordinating computer crime training programs. (National Institute of Justice, 2004)

A number of organizations also exist to provide investigative support to law enforcement agencies. One such group is the National Infrastructure Protection Center, which operates under the FBI. The group, which was created in 1998, exists to address reports of criminal attacks on computer systems, as well as coordinate investigations with other agencies (Wood, 2000). The Internet Fraud Initiative (IFI) and the Internet Fraud Complaint Center (IFCC) also work to help law enforcement agencies conduct investigations. These organizations function as a referral center for computer crime and computer fraud, ensuring information is delivered to the appropriate resource. Additionally, the IFI and the IFCC compile information on the nature and scope of computer crime and computer fraud, as well as create a public awareness and prevention programs (Internet Fraud Complaint Center, 2003) (Department of Justice, 2001).

Community Education and Protection

A handful of independent organizations also exist to educate consumers and businesses on the risks of computer crime and computer fraud, as well as ways to avoid victimization. These groups range in focus from general computer crime awareness and prevention strategies, to specific forms of computer-related crime. In addition to providing methods to prevent victimization, many of these organizations also provide contact information for those who believe they have been victimized. Thus, these consumer education groups teach computer users the potential dangers of electronic

resources, and also provide methods to minimize the damage done in the event a crime occurs. As one source explains, “As online usage continues to climb, education must focus only on preventative strategies...but also on where an individual can turn for help should a crime occur.” (Internet Fraud Complaint Center, 2003)

The Business Software Alliance (BSA) is one such community education organization. This group’s agenda is to provide the public with information regarding intellectual property rights, computer security and electronic commerce issues. Additionally, the BSA heads the Cyber-Crime and Intellectual Property Theft Prevention and Education Project, funded by the Department of Justice. This initiative is designed to teach the public about computer crime, as well as intellectual property crime. A central element of the project is to create educational tools for school-age children on these issues The Business Software Alliance has provide materials to thirteen million parents, educators and students since 2002 (Business Software Alliance, 2004).

Another group promoting education and computer crime prevention strategies for parents, teachers, and children is CyberAngels. This group provides centralized information regarding online safety and potential threats for young computer users (CyberAngels, 2004). Aside from providing preventative education, the group also offers victim support services, such as aiding in the identification and location of offenders, and coordinates with law enforcement agencies to arrest computer crime perpetrators. Furthermore, CyberAngels monitors legal issues related to computer resources, interpreting and disseminating this information to consumers (CyberAngels, 2004). By providing this information CyberAngels and similar groups, act as a comprehensive

resource, informing computer users of potential risks, and providing avenues available in the event a crime does occur.

Alternatively, some organizations focus exclusively on technical research of computer crime and computer fraud issues. These groups, such as the Computer Crime Research Center, and the Cyber Security Policy and Research Institute, bring together professionals and educators to advance the understanding of computer-related issues and policies. (Cyber Security Policy & Research Institute, 2002) These groups promote and compile research on these subject areas, which may in turn be used by policy-makers and researchers. In the case of the Computer Crime Research Center, their research has been incorporated into the larger International Anticriminal and Antiterrorist Committee (Computer Crime Research Center, 2004).

In addition to public education and research groups, there are also organizations who act as consumer protection agencies, providing the public with specific resources to use in the event of computer crime and computer fraud. Many of these organizations also have a preventative consumer education element, but their primary focus is to provide a means to protect computer users.

The Internet Fraud Complaint Center (IFCC) is a government entity focused on computer fraud. While the main focus of this group is to act as an intermediary between victims and appropriate law enforcement agencies, they also offer a range of education resources related to computer crime and computer fraud. For example, the IFCC outlines specific steps individuals should take if they become victims of computer crime. These steps act as a checklist for victims. Contacts range from the online auction house – for victims of online auction fraud – to notifying local and federal law enforcement

representatives, to contacting representatives in the offender's area, if the information is known (Internet Fraud Complaint Center, 2003).

The IFCC's main purpose is to act as a reporting mechanism for computer crime and computer fraud victims. This information is compiled for statistical purposes, and referred to the appropriate authorities for investigation (Internet Fraud Complaint Center, 2004). Complaints regarding child pornography are referred to the National Center for Missing and Exploited Children, computer intrusion complaints are sent to the National Infrastructure Protection Center, unsolicited email and SPAM complaints are referred to the Federal Trade Commission, and complaints of computer and credit card fraud are forwarded to the U.S. Secret Service (Internet Fraud Complaint Center, 2003).

Similarly, non-profit groups such as the National Consumers League's National Fraud Information Center and Internet Fraud Watch (NFIC), and the Anti-phishing Working Group (AWG) provide educational resources and reporting mechanisms for computer crimes. NFIC focuses on electronic fraud. Their website offers an online complaint center, in addition to statistical information on reported fraud, and extensive information on different computer fraud schemes (National Fraud Information Center, 2004). Similarly, AWG hosts a number of resources specifically related to phishing – the creation of misleading versions of legitimate websites and contacts in order to illegally obtain personal information for fraudulent purposes. AWG provides a selection of research reports on computer crime and fraud, and maintains an archive of phishing schemes submitted to the group by the public. Like the IFCC and the NFIC, AWG also has a method to submit complaints of phishing to be referred to authorities.

The existence of the governmental and private groups who strive to educate and protect the public is an essential element to minimizing the threats of computer crime and computer fraud. It encourages individuals and businesses to be proactive in their use of electronic resources, and provides countless resources to both prevent crimes as well as respond to victimizations. Additionally, it encourages a link between the public and law enforcement agencies by easing the burden of reporting for computer users by directing complaints to the appropriate entity, and alerts agencies to computer crime incidents in an efficient manner.

Computer Crime Statistics

Cyberstalking

National Problem:

There is evidence indicating that cyberstalking incidents are increasing. The “Los Angeles District Attorney’s Office estimated recently that e-mail or other electronic communication is a factor in approximately 20 percent of the roughly 600 cases referred to its Stalking Threat Assessment Unit” (United States 4). In addition, “the chief of the Sex Crimes Unit in the Manhattan District Attorney’s Office also estimates that about 20 percent of the unit’s cases involve cyberstalking” (United States 4). Furthermore, “the Computer Investigations and Technology Unit of the New York City Police Department estimates that almost 40 percent of its caseload involves electronic threats and harassments-and virtually all of these have occurred in the past 3 or 4 years”(United States 4). In addition to police departments and prosecutors offices, Internet Service Providers have begun to receive more complaints about cyberstalking. A large ISP “reported receiving approximately 15 complaints per month of cyberstalking, in comparison to virtually no complaints of cyberstalking just 1 or 2 years ago” (United States 4).

A study conducted by researchers at the University of Cincinnati concluded that approximately twenty-five percent of stalking incidents involving women in college could be classified as cyberstalking. This study sampled 4,446 random women currently attending college and asked if they had been stalked. Approximately 581 of the respondents reported that they had been stalked for a total of 696 individual incidents. Out of the 696 stalking incidents, 166 involved the use of threatening or harassing e-

mails (United States 4). Cyberstalking is a serious crime and it is occurring more frequently.

Maryland Cyberstalking Statistics

There are no statistics available for the state of Maryland regarding cyberstalking.

Internet Fraud

National Problem

Recent data published by the Internet Crime Complaint Center and the Federal Trade Commission's *Consumer Sentinel* demonstrates the seriousness of the nation's computer fraud problem. The Internet Crime Complaint Center received approximately 124,500 complaints during 2003. This was "a 60% increase over 2002 when 75,063 complaints were received" (National White Collar Crime Center 4). In fact, for each of the past four years, the number of complaints received by the Internet Crime Complaint Center has consistently increased each year as can be seen in Figure 2.

Yearly amount of Complaints Received by the Internet Crime Complaint Center

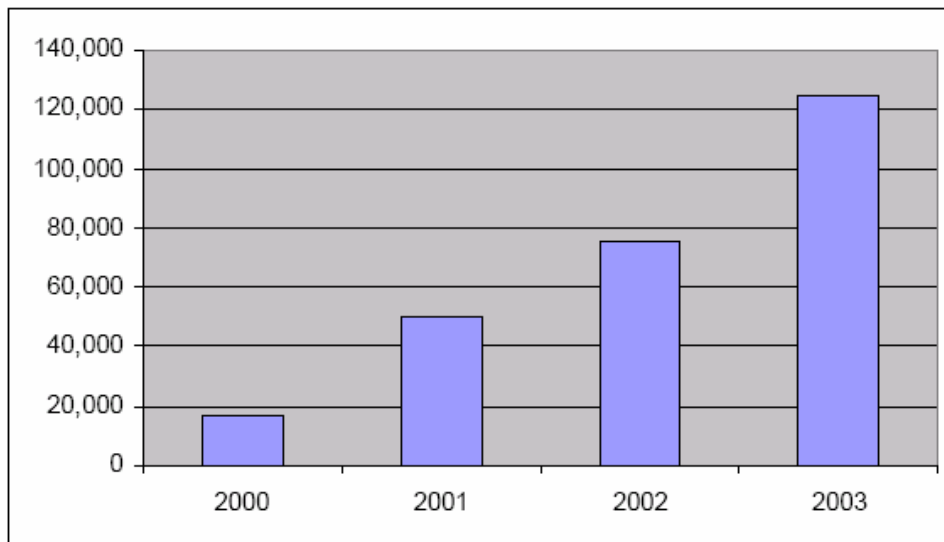


Figure 2 yearly amounts of complaints reported to the Internet Crime Complaint Center courtesy of http://www1.ifccfbi.gov/strategy/2003_IC3Report.pdf

In addition, the *Consumer Sentinel* produced by the Federal Trade Commission has indicated that the number of computer fraud complaints has increased over the past three years. Furthermore, computer fraud complaints are more frequently reported than other fraud complaints as can be seen in Figure 3.

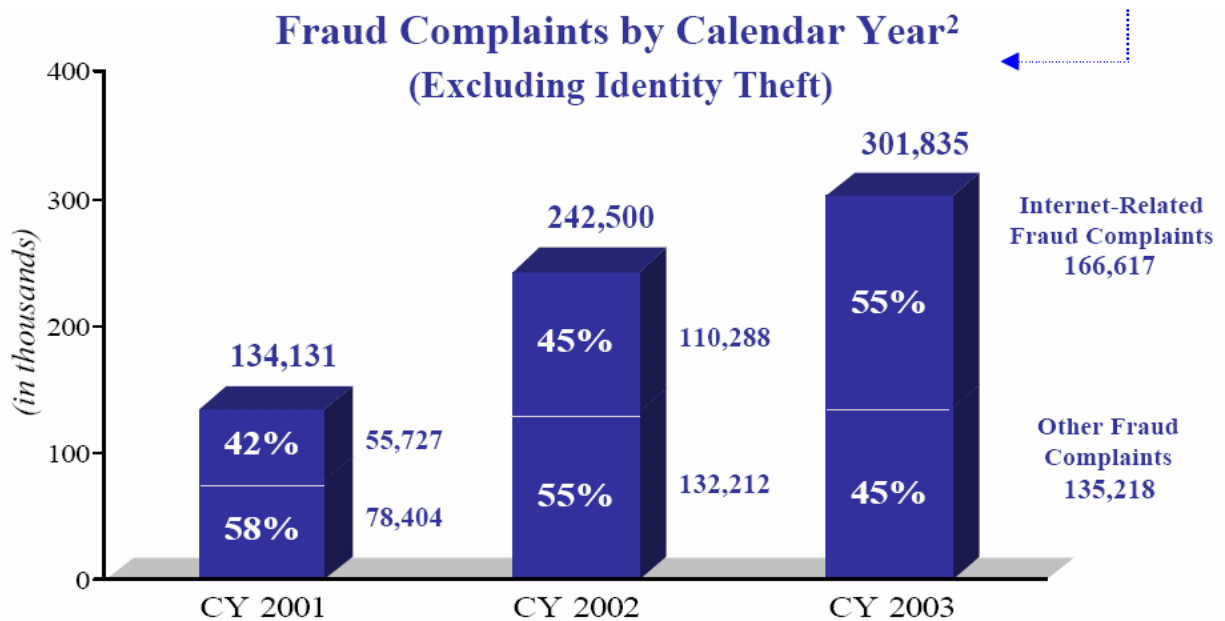


Figure 3 yearly amounts of fraud complaints received by the FTC's *Consumer Sentinel* courtesy of http://www.consumer.gov/sentinel/states03/3year_trends.pdf

Internet Crime Complaint Center data from 2003 indicates the most common forms of computer fraud. Approximately 61% of all complaints received by the ICCC during 2003 were auction fraud complaints. Additionally, 20.9% of received complaints were for non-delivery or services or merchandise. The third most frequent form of computer crime reported to the ICC during 2003 was credit/debit card fraud, which accounted for 6.9% of all complaints received (NWCCC 6).

Moreover, the *Consumer Sentinel* listed the frequency distribution of ages among the victims of computer fraud during 2003. The frequency distribution can be seen in

figure 4. As it can be seen, the most common ages victimized by computer fraud are those in the 20-29, 30-39, and 40-49 years old age brackets (Consumer Sentinel 8).

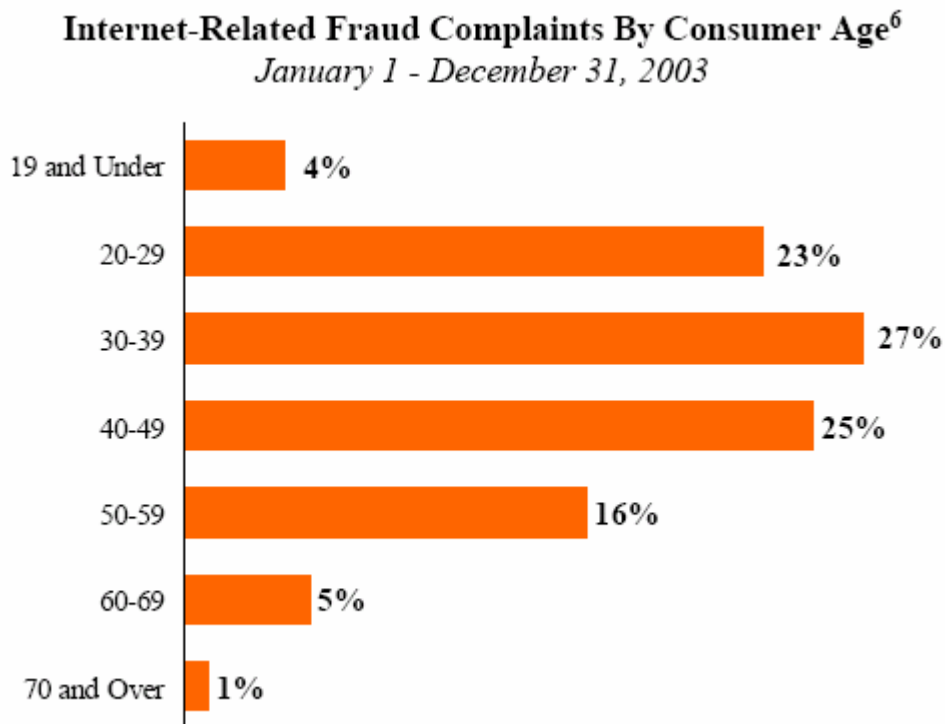


Figure 4 Internet-related fraud complaints by consumer age for 2003 courtesy of http://www.consumer.gov/sentinel/states03/internet_related_trends.pdf

Maryland Computer Fraud Statistics

The trends for computer fraud in the state of Maryland are similar to the trends of

Maryland	Number of Internet-related fraud complaints	Percentage of total fraud reported	Average amount of money lost per incident
<i>2001</i>	781	31%	\$1,196
<i>2002</i>	1,558	38%	\$1,794
<i>2003</i>	2,234	38%	\$1,925

Figure 5 data courtesy of the FTC *Consumer Sentinel*
<http://www.consumer.gov/sentinel/trends.htm>

the United States. Over the past several years, the yearly amount of computer fraud complaints has steadily increased. In addition, the average amount of money loss per each computer fraud incident has increased as can be seen in figure 5.

The *Consumer Sentinel* ranked the most frequent forms of computer fraud for each state during the 2003 calendar year. For Maryland the most frequently reported forms of computer fraud in decreasing order are as follows: Internet auctions, shot-at-home/catalog sales, Internet services and computer complaints, advance-fee loans and credit protection/repair, and foreign money orders (NWCCC 36). In addition, the top locations in Maryland for computer fraud complaints in descending order are as follows: Baltimore, Silver Spring, Rockville, Gaithersburg, and Columbia (Consumer Sentinel 36).

Phishing

Statistics provided by the Anti-Phishing Working Group indicate that from January to July of 2004, the number of monthly reported phishing attacks to the APWG increased from 176 to 1,974 incidents per month as can be seen in figure 6.

Figure 7 displays the number of reported Phishing sites by month for July through October

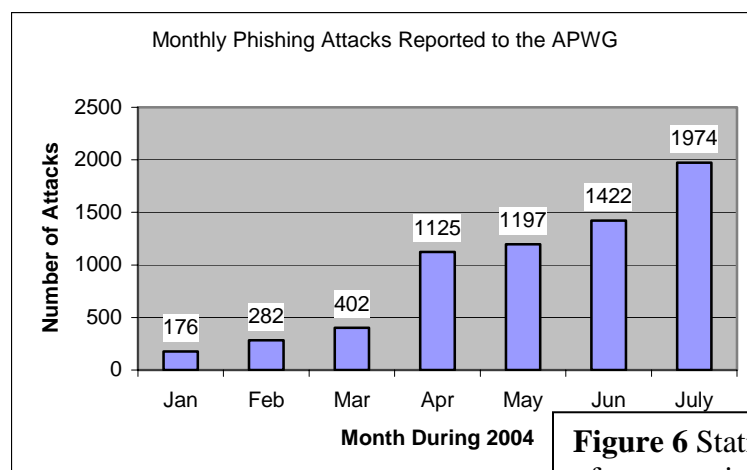


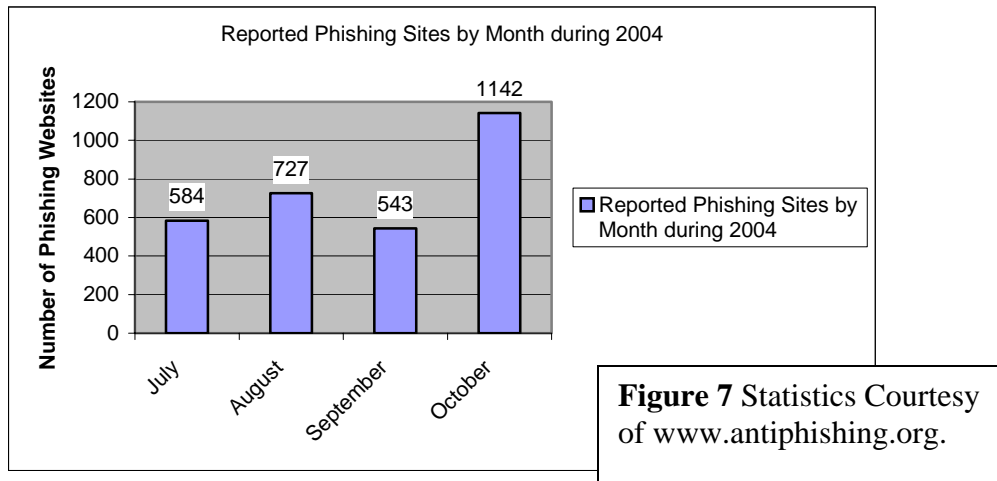
Figure 6 Statistics Courtesy of www.antiphishing.org.

of 2004. As it can be seen the number of monthly phishing attacks along with the number of reported phishing websites has increased each month. The following are the

only available statistics regarding the Phishing problem in the United States. It appears as though Phishing incidents and Phishing websites are on the rise.

Maryland Phishing Statistics:

There are no available statistics about the Phishing problem in the state of Maryland.



Problems and Suggestions found in the Literature Review

Throughout the analysis of the written literature pertaining to computer crime, researchers have noted a number of specific problems and recommendations regarding computer crime and computer fraud. Many of these issues are commonalities across the literature, and highlight some of the most important topics related to this crime type. By examining these issues, the most frequent concerns of past researchers can be seen, providing a checklist of items to be considered in the future.

The noted problems found in the ways computer crime and computer fraud are currently addressed are broad in range and address both issues of law enforcement agencies as well as external considerations. The most basic issue raised in the literature regards the lack of a uniform definition for both computer crime and computer fraud. As was previously mentioned, the lack of a uniform way to delineate what constitutes a computer crime makes enforcement difficult. Additionally, without a uniform definition, the true scope and nature of the computer crime and fraud trends cannot be assessed, which also poses a further challenge for agencies as they determine their staffing and resource needs regarding computer crime issues (Goodman, 2001).

Aside from definitional issues, law enforcement also faces a jurisdictional challenge. Computer crime and fraud often involve crossing boundaries and borders not seen in traditional crimes. This poses a new set of challenges for state and local agencies as they struggle to investigate cases that often take them outside of their jurisdiction. As one source states,

While most law enforcement has historically been left to the states, states are ill-equipped to deal with the extraterritoriality of computer crime. State law enforcement agencies cannot execute search warrants, subpoena witnesses, or

make arrests beyond their own borders. Yet computer crimes are hardly ever confined to a specific locality (PBS, 2001).

Furthermore, because of the nature of computer crimes, agencies are often required to involve other law enforcement organizations in the investigation. This involvement may pose challenges such as making cases a priority for other jurisdiction's officers, or dealing with agencies that have fewer resources available to devote to computer-related crimes. This difficulty is made clear by a recent study which revealed that half of the agencies involved in the study – 62 of 124 – didn't have formal computer crime units. Moreover, three-fourths of the agencies didn't have the tools to identify and investigate computer crimes, and nearly two-thirds faced staffing and training issues (U.S. Department of Justice, 2001).

Another issue addressed by the researchers was the overall lack of importance placed on computer crimes. Several studies revealed that computer crimes were not given significance by law enforcement agencies, and when they were, crimes that could be considered low level were often ignored. This lack of interest is explicitly seen in the National Institute of Justice (NIJ) study that showed that seventy-seven percent of law enforcement respondents stated that electronic crimes were given only low to medium importance within their agency, with the exception of child pornography (U.S. Department of Justice, 2001). In one specific case, a counterfeiting victim went so far as to track down the offender and notify local and federal officials, but couldn't get them to go out and make an arrest because they were otherwise focused on larger cases, and this specific incident didn't meet FBI or Secret Service thresholds (Computer Security Institute, 2003). Other reasons given by respondents to the NIJ study for their failure to investigate computer crimes and fraud include insufficient prosecutorial knowledge or

judicial interest, the aforementioned extraterritorial and priority issues, and a lack of sufficient officer training (U.S. Department of Justice, 2001).

Aside from issues specific to law enforcement agencies, another problem area highlighted by researchers is the overall lack of reporting of computer crimes and fraud. A number of rationales were found in the literature to explain the lack of reporting. One of the most common responses by businesses was the fear of losing credibility in the eyes of the public. For example, in one survey nearly all of the companies were victims of computer-related offenses, yet only seventeen percent of them reported the incidents to law enforcement officials (U.S. Department of Justice, 2001). Similarly, in an Australian study, only nineteen percent of those victimized reported the incident (Thompson, 1998). The annual Computer Crime and Security Survey, coordinated by the Computer Security Institute and the FBI, reported in the 2004 survey that reporting of offenses to law enforcement agencies were declining, and the nearly half of the reasons given for this lack of response were the fear of negative publicity (Gordon, Hosmer, Siedsma, Rebovich, 2003). This non-reporting also affects individuals. It has been found that only twenty-five percent of those who file a complaint with the Internet Fraud Complaint Center had previously contacted a law enforcement agency regarding the issue. However, the lack of reporting may also be due to other factors. As shown in the 2003 Computer Crime and Security Survey, nearly half of those responding to a question regarding not reporting an incident to officials stated their reason as not knowing that they could report the offense (Computer Security Institute, 2003). The general public, and law enforcement itself may be unclear or unaware of the available channels to report computer crime and computer fraud incidents. Additionally, they may not believe their case merits

investigation, or may fear the consequences of the information becoming public knowledge. Either way, law enforcement officials and private organizations need to consider the existing reporting mechanisms in regards to their availability and ease of use for future crime reporting.

In addition to the issues raised by researchers, a number of recommendations were suggested as key areas to develop, as related to computer crime and computer fraud. The NIJ study surveyed a number of law enforcement officials and culled a list of needs for handling computer-related offenses. This list includes a public awareness campaign aimed at the public and private sector, more comprehensive statistical data and reporting, uniform training and certification for investigators and prosecutors, cooperation with the high-tech industry, and assistance in developing and maintaining regional computer crime units. Also, the list noted the need for review of the existing legal infrastructure, specific research and publications for computer crimes, increased managerial support, and updated investigative tools and resources for law enforcement officials. The study also suggested the creation of means to allow agencies to enforce out of state subpoenas, thus eliminating the jurisdictional dilemma many units currently face (U.S. Department of Justice, 2001). Another researcher suggested the simple addition to crime report questionnaires of a question regarding the use of computers to perpetrate the crime (Goodman, 2001). Still others stress the importance of interagency support by stating,

The global nature of the Internet, and law enforcement experience in conducting Internet fraud investigations, have made it increasingly clear that law enforcement authorities need to work in closer coordination to have a substantial effect on all forms of Internet fraud (Department of Justice, 2001).

In general, law enforcement agencies need to take a comprehensive look at all aspects of addressing computer crime and computer fraud, and need to consider a variety

of improvements, from the structure of their agency, to their partnerships with industry and other jurisdictions. From the literature, it is clear there is much work to be done regarding the ways in which computer crime and computer fraud are currently addressed.

Further Research

As computer crime and computer fraud become more widely recognized as a legitimate criminal threat, more agencies will begin to incorporate a specific element within their agency to address this form of crime. A number of law enforcement agencies at various levels already have or have begun to establish a computer crime unit. However, because computer crime and computer fraud are relatively new threats, a standard operating procedure based on uniform definitions and expectations does not currently exist to address these computer-related threats. Through this study, a better understanding of the current state of affairs can be gained in regards to how law enforcement agencies at different levels currently address computer crime. Additionally, from this research, specific recommendations can be formed on how to handle this crime type for existing and future efforts, including the formation of a uniform definition for computer crime and computer fraud, successful investigative procedures, and potential improvements to create more effective and efficient computer crime units.

Methodology

At the request of the Montgomery County Criminal Justice Coordinating Commission, a questionnaire was constructed for distribution to law enforcement agencies regarding computer crime and computer fraud. After completing a review of the available literature, the researchers constructed a list of twenty-eight questions for law enforcement agencies to answer regarding their efforts in addressing computer crime and fraud. These questions were designed to provide a comprehensive understanding of each agency's specific actions and motivations, and are based on the major areas of consideration found in the literature review. Once the initial list of questions was

constructed, the researchers had two professors of criminology, Dr. Charles Wellford, and Dr. Doris MacKenzie examine the list and provide feedback. The final list of questions included in the survey are as follows:

1. What is the official title of your agency? What is your position?
2. Does your agency have a definition for computer crime? What are the origins of this definition?
3. Does your agency have a definition for computer fraud? What are the origins of this definition?
4. What are the major forms the crimes in these categories take? (i.e. online auction fraud, etc.)
5. Is computer crime / computer fraud a major emphasis in your agency? In what ways is it emphasized? (i.e., prevention / education / investigation / prosecution)
6. What crimes related specifically to computer crime / computer fraud fall within your agency's jurisdiction?
7. Are there specific levels or value amounts that must be met regarding these crimes in order for your agency to address them? (i.e. \$500 dollars and up)
8. In your best estimate, annually, how many cases of computer crime / computer fraud are reported by your agency?
9. In your best estimate, annually, how many cases of computer crime / computer fraud are investigated by your agency?
10. What types of computer crime / computer fraud are most often addressed by your agency?
11. What are the most frequent types of computer crimes reported to your agency?
12. How do you initiate an investigation into these crimes?
13. Does your agency actively seek out computer crimes / computer fraud or do you rely on outside sources (another agency, complaints, etc)?
14. What resources do you regularly use in addressing these types of crimes?
15. Does your agency have a computer crimes unit? If so, how many officers are in it? What are their official duties?
16. What backgrounds do those who deal with computer crime / computer fraud have in your agency?
17. Do these individuals receive special training to handle computer crime / computer fraud? If so, outline these courses.
18. Are the individuals who deal with computer crime/computer fraud solely responsible for addressing this type of crime, or do they also work on other crime types?
19. What techniques has your agency found to be successful in investigating/preventing/prosecuting computer crime / computer fraud?
20. Where do you/your agency have the most difficulty dealing with computer crime/computer fraud?
21. What resources would you like to see available to use in addressing computer crime / computer fraud?

22. What do you think is needed in order to be more effective in combating this type of crime?
23. Are existing statutes broad enough to cover all forms of criminal activity committed with the use / aid of a computer? Why or why not?
24. What liaisons do you have with other agencies? (Both law enforcement and other forms.)
25. Does your agency refer computer crime / computer fraud investigations or complaints to other agencies? Why?
26. How successful has your agency been in addressing computer crime / computer fraud this far?
27. What do you see as the major areas of attention regarding computer crime / computer fraud in the future?
28. Do you have any contacts that you believe would be able to provide helpful information regarding this study? If so, who?

Once the questionnaire was finalized, the researchers decided how to contact law enforcement representatives and solicit their participation. The researchers planned to study no less than three agencies, and targeted agencies at the local, state, and federal level. The researchers decided on a two-pronged approach to encourage greater response rates. Using a list of contacts gathered from the literature review, as well as law enforcement contacts suggested by both the Montgomery County Criminal Justice Coordinating Commission and the advising professor, the researchers emailed and telephoned each potential participant.

The researchers desired to include interviewees from a variety of jurisdictions. The researchers attempted to include representatives from federal, state, and local law enforcement agencies. Additionally, the researchers wanted to include a prosecutorial perspective and a representative from a support organization. The interviews consist of a Maryland State Police representative, two local police representatives – Prince George’s County and Montgomery County – a Maryland State’s Attorney, and a representative from the National White Collar Crime Center, a support organization. At the Federal

level, the researchers were also able to conduct an interview with the United States Secret Service's computer crime unit. Additionally, the researchers contacted the FBI who were initially interested in participating but were ultimately unable to due to time constraints because of their current terrorism initiative.

The respondents from the Maryland State Police Computer Crime Unit, Prince George's County Police Department, and Maryland States Attorney's office opted to conduct a telephone interview. The respondents from the Montgomery County Department of Police Computer Crimes Unit, as well as the National White Collar Crime Center and the United States Secret Service choose to complete the questionnaire by email.

Based on the responses to the questionnaire and on the literature review, the researchers were able to make recommendations regarding the definitions of computer crime and computer fraud, as well as specific elements and areas for consideration to ensure the success of current and future computer crime focused endeavors.

Findings

Each respondent provided a reply to the twenty-eight questions. These responses have been compiled below. Due to the differences in size and jurisdiction, each respondent's answers had a number of noticeable differences, specifically in the types of cases handled, as well as obstacles faced. However, there also exist a number of commonalities across each of the different agencies actions and computer crime efforts.

What is the official title of your agency? What is your position?

Sergeant Robert Smolek is the supervisor of the Computer Crimes Unit within the Maryland State Police Criminal Investigation Division Computer Crimes Unit

(MSPCCU). He is also the Director of the Maryland Internet Crimes Against Children Task Force. He has eight years experience working on computer crime and fraud, and considers himself to be one of the best law enforcement resources in the area for dealing with computer crimes (Sgt. R. Smolek, personal communication, 11/18/2004).

Sergeant Gary Renninger works for the Montgomery County Computer Crimes Unit (MCCCU) within the Department of Police, Montgomery County, Maryland (Sgt. G Renninger, personal communication, 11/18/2004). As stated on their website, "The goals of the Computer Crime Unit are to aggressively investigate computer related crimes and to educate the community on how to avoid becoming a victim in the first place." (Montgomery County Department of Police, 2004)

Allen Lee is a Lieutenant with the Prince George's County Police Department (Lt. Allen Lee, personal communication, 11/19/2004). Because PGPD does not have a specific computer crimes unit, Allen Lee was not able to provide answers to some of the questions in the interview.

Bill Crane is the Manager of the Computer Crime Section of the National White Collar Crime Center (NW3C), which is a federally funded non-profit organization that works alongside law enforcement agencies in coordinating the prevention, investigation, and prosecution of economic and high-tech crimes (National White Collar Crime Center, 2004). Because the NW3C is a supporting organization, rather than a true investigative law enforcement agency, several of the survey questions fell outside of the organization's scope (B. Crane, personal communication, 11/27/2004). However, due to their intimate working relationship with agencies at various levels that address computer crime and computer fraud, the responses that have been provided should prove to be beneficial.

Peter Feeny is an attorney for the Maryland States Attorney office for Montgomery County. He is the team head of the Computer Crime Unit (P. Feeny, personal communication, 12/1/2004).

The respondent from the United States Secret Service, Baltimore Field Office (USSS) is Special Agent Chris LeFever. He is a member of the Electronic Crimes Special Agent Program, which is the title for USSS agents trained to deal with computer crimes (C. LeFever, personal communication, 12/6/2004).

Does your agency have a definition for computer crime? What are the origins of this definition?

Sgt. Smolek explained the definition the MSPCCU utilize is a generic one. They define computer crime as, “criminal activities facilitated by the Internet, computers, and other areas of digital technology.” (Sgt. R. Smolek, personal communication, 11/18/2004)

Similarly, MCCCCU uses a very broad definition for computer crime. This agency categorizes computer crime as “...crimes committed by use of a computer.” (Sgt. G. Renninger, personal communication, 11/18/2004)

Allen Lee said that the PGPD did not have a definition for computer crime (Lt. Allen Lee, personal communication, 11/19/2004).

The NW3C has a more specific working definition for computer crime. This definition is comprehensive in that it considers the various ways a computer may be involved in the crime. The definition used by NW3C is: “Crime committed wherein a computer is involved as the target of the crime, an instrumentality of the crime, a storage device for criminal activities or as contraband.” (B. Crane, personal communication,

11/27/2004) This definition was created following reviews of the Federal Computer Search and Seizure Guidelines, as well as other sources (B. Crane, personal communication, 11/27/2004).

Peter Feeny was unable to provide the specific definition at the time of interview. He plans to send the Maryland States Attorney's office definition of computer crime to the researchers at a later date (P. Feeny, personal communication, 12/1/2004).

Chris LeFever did not provide a working definition for computer crime currently adopted by the USSS (C. LeFever, personal communication, 12/6/2004).

The definitions used across the groups for computer crime are generally broad. For the most part, they refer to crimes that involve some form of electronic resource. However, even at this broad level, disparity can be seen between the responses given, such as the role the computer plays in the crime. Additionally, it is important to note that several of the agencies interviewed could provide no working definition of computer crime at all.

Does your agency have a definition for computer fraud? What are the origins of this definition?

While MSPCCU doesn't have a specific definition for computer fraud, Sgt. Smolek explains the unit looks at large fraud schemes perpetrated through the use of computers and the Internet. Further, Sgt. Smolek stated the MSPCCU's use of broad, adaptive definitions is due to the changing nature of the digital world. The frequently changing nature of computer crimes makes it difficult to pin down a very specific definition, and facilitates the need for generic definitions (Sgt. R. Smolek, personal communication, 11/18/2004).

The MCCCCU does not have a separate working definition for computer fraud. Sgt. Renninger states MCCCCU uses the same definition for computer crimes as it does for computer fraud. This definition simply refers to offenses where a computer is utilized (Sgt. G. Renninger, personal communication, 11/18/2004). Similarly, both the PGPD and the NW3C said they do not have a specific definition for computer fraud (Lt. Allen Lee, personal communication, 11/19/2004) (B. Crane, personal communication, 11/27/2004).

Peter Feeny defined computer fraud as the use of a computer to commit fraud (P. Feeny, personal communication, 12/1/2004).

Similar to their response for a definition of computer crime, the USSS did not provide a definition for computer fraud (C. LeFever, personal communication, 12/6/2004).

Like the explanations given regarding computer crime, the groups for the most part did not have specific definitions for this form of crime. This is interesting to note considering their responses concerning their involvement in investigating computer frauds.

What are the major forms the crimes in these categories take?

MSPCCU deals with a wide variety of computer-related offenses. A few of the frequent crimes addressed by this agency include online auction fraud, reshipping scams, money wiring and laundering fraud, failure to deliver goods schemes, and internet crimes against children, including both child pornography and online solicitation of minors. Many of the offenses fall into the categories of large fraud and crimes against children (Sgt. R. Smolek, personal communication, 11/18/2004).

MCCCU also handles a variety of computer-related crimes. This agency is responsible for investigating incidence of hacking, online auction fraud, and hate crimes – described by Sgt. Renninger as specifically hate email, and child pornography (Sgt. G. Renninger, personal communication, 11/18/2004).

The NW3C, in collaboration with the FBI, runs the Internet Crime Complaint Center (IC3). The IC3 accepts and refers complaints regarding computer crime and fraud to appropriate agencies so that it may be investigated. Additionally, IC3 maintains statistics on the amount and forms these complaints take (Internet Crime Complaint Center, 2004). Based on the statistical information from IC3, the major forms of computer crime and computer fraud are online auction fraud, credit card fraud and identity theft (B. Crane, personal communication, 11/27/2004).

Peter Feeny said that ID theft and online auction fraud are the major forms in these categories (P. Feeny, personal communication, 12/1/2004).

The USSS cited a number of different computer crimes they regularly encounter. These include a number of fraud crimes, such as counterfeiting, credit card fraud, and identity theft, as well as more traditional crimes, such as child pornography and network intrusions (C. LeFever, personal communication, 12/6/2004).

Is computer crime/computer fraud a major emphasis in your agency? In what ways is it emphasized?

Sgt. Smolek noted a difficulty in the priority MSPCCU gives cases versus the order of importance placed on cases by the larger law enforcement and governmental community. MSPCCU, as well as Sgt. Smolek himself, typically place crimes against individuals over economic crimes. However, those priorities are often at odds with the

“real world” – presumably supervisory governmental agencies – which places importance on crimes involving economic loss (Sgt. R. Smolek, personal communication, 11/18/2004).

Sgt. Renninger explained computer crimes and computer fraud are the focus within MCCCUC, and the emphasis is placed on investigation of these offenses (Sgt. G. Renninger, personal communication, 11/18/2004).

Lt. Lee indicated that computer crime was not emphasized at his agency. (Lt. Allen Lee, personal communication, 11/19/2004).

The Computer Crimes Section of the NW3C does have a focus on computer crime and fraud. The focus of this agency is on addressing computer crime scenes and evidence, in that they provide computer forensics training to state and local law enforcement officers (B. Crane, personal communication, 11/27/2004).

Computer crimes are important to the Maryland States Attorney’s office but there are a limited number of cases referred to the office. There are just two prosecutors dedicated to computer crime. They are aware it is a growing problem, and the office has requested funding for an additional computer crime prosecutor (P. Feeny, personal communication, 12/1/2004).

Chris LeFever commented that while computer crimes are not currently a major emphasis within USSS, he believes it will become a more important focus due to the increasing number of cases involving both computer crime and computer fraud that are being brought to the Secret Service (C. LeFever, personal communication, 12/6/2004).

As can be seen from the responses, the attention given to computer crimes by different agencies varies greatly. This varying emphasis indicates the difficulty an agency

may have in cooperating with other jurisdictions in the investigation and prosecution of computer crimes.

What crimes related specifically to computer crime/computer fraud fall within your agency's jurisdiction?

MSPCCU are not precluded from dealing with any form of computer crime. The Maryland State Police have full jurisdiction to address any type of crime or fraud. Interestingly, they also have jurisdiction in cases of cyberterrorism (Sgt. R. Smolek, personal communication, 11/18/2004).

Unlike the State Police Computer Crime Unit, MCCCUC's jurisdiction is significantly more limited. Their jurisdiction deals with hate email and online auction fraud (Sgt. G. Renninger, personal communication, 11/18/2004).

Unlike the state and local agencies, the NW3C is not an operational law enforcement agency, and therefore does not have jurisdiction over any form of crime. Rather, NW3C provides support functions, such as computer forensics training, to agencies so that they may more adequately address computer crimes. (B. Crane, personal communication, 11/27/2004).

Any sort of theft committed through the use of a computer such as ID theft, credit card fraud, online exploitation of children, or solicitation of a minor fall within the jurisdiction of the States Attorney's office (P. Feeny, personal communication, 12/1/2004).

The USSS has jurisdiction over fraud and white-collar crimes, such as counterfeiting, identity theft, systems intrusion, and credit card fraud. They point out that

child pornography cases are handled primarily by the FBI and U.S. Immigrations and Customs Enforcement (C. LeFever, personal communication, 12/6/2004).

The emphasis placed on computer crimes, as well as the crimes addressed by each group show the differences at each level. Furthermore, the local agencies are the most limited in their investigations, while agencies with larger jurisdictions and involvement cover larger and more significant crimes.

Are there specific levels or value amounts that must be met regarding these crimes in order for your agency to address them?

The focus within MSPCCU is on Internet theft in the felony range with suspects within Maryland state lines. Sgt. Smolek noted repeatedly the difficulty in investigating computer crimes is due to their complex nature. These crimes are frequently not restricted to any one jurisdiction and may involve several stages between the victim and the offender. Additionally, Sgt. Smolek remarked on the difficulty of investigating and prosecuting crime using decades-old laws. Due to this, MSPCCU attempt to use practicality in deciding which crimes to investigate. They consider extradition and jurisdictional issues, as well as victim and offender locations. Additionally, Sgt. Smolek explained the need to investigate for the suspect rather than the victim. Thus, rather than the agency arresting a suspect and transporting them to the victim, they arrest suspects and have victims come to MSPCCU's jurisdiction. Again, the purpose of this method of operation is practicality (Sgt. R. Smolek, personal communication, 11/18/2004).

There are no stipulations to the crimes MCCCUC address. They do not choose to meet specific levels or values in order to investigate a computer-related offense (Sgt. G. Renninger, personal communication, 11/18/2004).

There are no specific value amounts that must be met regarding these crimes in order for the States Attorney's office to address them. Sizeable amounts of money with many victims will definitely be investigated. Realistically, amounts under \$500 would be investigated as well. Usually county police departments have a screening process to determine which cases should be investigated and then refer those to the States Attorney's office (P. Feeny, personal communication, 12/1/2004).

Responses to this question were mixed. Agencies primarily did not limit the cases they investigated, but did not stipulations and determining factors in how cases are prioritized and chosen.

In your best estimate, annually, how many cases of computer crime/computer fraud are reported by your agency?

Sgt. Smolek was unable to quantify the amount of crime reported by the Maryland State Police. This is specifically due to communication breakdowns across the twenty-eight Maryland State Police barracks. Each barrack has their county's report information, but the sum of this information is not compiled (Sgt. R. Smolek, personal communication, 11/18/2004).

Unlike the Maryland State Police, the MCCCUC was able to quantify the amount of computer crime and fraud cases it reports annually. Sgt. Renninger estimates the amount of reports to be over one hundred reported cases a year (Sgt. G. Renninger, personal communication, 11/18/2004).

Lt. Lee said that computer crimes are seldom reported to PGCPD (Lt. Allen Lee, personal communication, 11/19/2004).

Peter Feeny reported that a couple dozen cases are referred by county or state police to the State Attorney's office each year (P. Feeny, personal communication, 12/1/2004).

Chris LeFever did not know how many cases of computer fraud and crime were reported to the USSS annually, nor was he able to provide a figure for the number of cases investigated annually (C. LeFever, personal communication, 12/6/2004).

The range of reported cases and inability to specify specific amounts indicates the need for more uniform reporting and recording mechanisms. Agencies should be able to identify the amount and types of crimes either reported or referred to them within a given time frame.

In your best estimate, annually, how many cases of computer crime/computer fraud are investigated by your agency?

The MSPCCU investigated 360 individual computer-related cases in 2003. Roughly sixty percent of these were crimes against children, and roughly thirty-eight percent were Internet fraud cases. The remaining cases were a variety of offenses, including harassment involving electronic resources, as well as instances of intrusion (Sgt. R. Smolek, personal communication, 11/18/2004).

MCCCU investigates substantially fewer computer-related cases per year. Sgt. Renninger's best estimate of computer crime and computer fraud cases investigated on a yearly basis is approximately sixty cases (Sgt. G. Renninger, personal communication, 11/18/2004).

Lt. Lee explained that no computer crime cases are investigated by his agency. He said that currently they are working on updating their records management system

and settling some use of force issues. Computer crime was not an issue for the PGPD but he thought it would be in the near future (Lt. Allen Lee, personal communication, 11/19/2004).

While he didn't provide a specific amount, Peter Feeny did state that all of the computer crimes referred to the States Attorney office are investigated (P. Feeny, personal communication, 12/1/2004).

What types of computer crimes/computer fraud are most often addressed by your agency?

The majority of MSPCCU caseload involves Internet crimes against children (Sgt. R. Smolek, personal communication, 11/18/2004).

While they include other forms of computer crime and fraud in their definition of computer crime, MCCCUC primarily addresses hate email and online auction fraud. This may be due to the jurisdictional limitations of the unit (Sgt. G. Renninger, personal communication, 11/18/2004).

While the NW3C does not address computer crimes and computer fraud themselves, the students who train with the NW3C address a variety of computer-related crimes. Most frequently, the crimes they are handling involve cases of child pornography, credit card fraud, and instances of counterfeiting (B. Crane, personal communication, 11/28/04).

Identity theft and online auction fraud are the crimes most often addressed by the States Attorneys office (P. Feeny, personal communication, 12/1/2004).

Similarly, the USSS also primarily deals with cases of identity theft, in addition to crimes of counterfeiting and credit card fraud. Not surprisingly, these are also the types of

crimes most often reported to this agency (C. LeFever, personal communication, 12/6/2004).

When examining the focuses of each agency, it can be seen that many of the cases noted by the agencies were either child exploitation and pornography issues, or computer fraud cases, specifically online auction fraud.

What are the most frequent types of computer crimes reported to your agency?

The most frequent types of computer crimes reported to MSPCCU are computer theft and fraud crimes. These generally are referred from local police agencies to Maryland State Police barracks. Sgt. Smolek commented that while some local police agencies do have good skill sets in regards to computer crime and computer fraud, they may have difficulty in getting others involved in these investigations, and so the cases are referred to the state police (Sgt. R. Smolek, personal communication, 11/18/2004).

Similarly, the most reported form of computer crime reported to MCCCCU is online auction fraud (Sgt. G. Renninger, personal communication, 11/18/2004).

How do you initiate an investigation into these crimes?

MSPCCU has two goals in conducting an investigation. The first goal is to identify the account that was responsible for the offending deed. This may include items such as an email address, IP address, or other online identifiers. From there, MSPCCU attempts to locate the person behind the responsible account. Sgt. Smolek commented that completing the first goal – finding the account – was not particularly difficult. The difficulty instead lies in connecting an individual to the account. Examples such as Internet accounts used by multiple individuals, and wireless networks lacking security to block outsiders were given to illustrate this point. Sgt. Smolek stated that once the

account was located, traditional investigative techniques are often required to connect the remaining elements of the criminal act (Sgt. R. Smolek, personal communication, 11/18/2004).

MCCCU, unlike the Maryland State Police unit, relies on referrals from another agency to initiate an investigation. MCCCU has cases sent from the National White Collar Crime Center, which it then investigates (Sgt. G. Renninger, personal communication, 11/18/2004).

Peter Feeny explained that investigations into these crimes are initiated by complaints that are referred to the office by county and state police. Periodically, the States Attorney's office receives civilian complaints, which can initiate investigations (P. Feeny, personal communication, 12/1/2004).

Investigations by the USSS also primarily rely on referrals from local agencies (C. LeFever, personal communication, 12/6/2004).

Many of the investigations conducted by the agencies are a result of referrals or complaints, rather than being initiated by the agency themselves. However, some cases are proactively initiated by the agencies.

Does your agency actively seek out computer crimes/computer fraud or do you rely on outside sources?

Sgt. Smolek explained that crimes against children are handled in a different investigative way than other computer-related crimes. Additionally, he noted actively seeking out crimes against children is a large portion of the crimes against children grant that MSPCCU receives. Thus, MSPCCU relies on a combination of reactive and proactive methods. In cases involving crimes against children, online stings are often

utilized; where Maryland State Troopers go onto online message boards, chat rooms and other forms of online communication posing as children, or those seeking to take advantage of minors. When outside sources are used, it is often to acquire online records, or to collaborate with allied police agencies with relevant expertise, particularly for cases involving multiple jurisdictions (Sgt. R. Smolek, personal communication, 11/18/2004).

As stated previously, MCCCUC does not proactively seek out computer crimes to investigate. It relies solely on cases of computer crime and computer fraud sent from the National White Collar Crime Unit (Sgt. G. Renninger, personal communication, 11/18/2004).

The approach taken by the USSS involves a mixture of both proactively seeking out crimes, as well as investigating incidents referred by local agencies (C. LeFever, personal communication, 12/6/2004).

What resources do you regularly use in addressing these types of crimes?

Resources employed by MSPCCU including traditional policing as well as a variety of other resources. One major resource used is the court order for the discovery of records. Similarly, the local state's attorney office is drawn on to get court orders. Additionally, Sgt. Smolek noted online investigative infrastructures, such as the investigative resources of PayPal, an online payment mediator, as well as other online entities, such as America Online. Sgt. Smolek highlighted the Internet itself as being an essential tool for investigation, where a suspect's online presence may aid in determining their location. MSPCCU has used search engines, such as Google, to help find information regarding suspects of computer crime and computer fraud. Sgt. Smolek said MSPCCU is reluctant to use private industry resources, due to lack of confidence that

individuals will fully complete assigned work (Sgt. R. Smolek, personal communication, 11/18/2004).

Sgt. Renninger states that the MCCCUC simply uses basic investigative resources to investigate and address computer crimes that are provided to them by the National White Collar Crime Center (Sgt. G. Renninger, personal communication, 11/18/2004).

The State's Attorney's office does not regularly use any resources other than county and state police in addressing computer crimes. Sometimes they obtain assistance of trained investigators and forensic examiners (P. Feeny, personal communication, 12/1/2004).

The USSS has a group of Special Agents specifically trained in handling computer-related crimes. These individuals are referred to as Electronic Crimes Special Agent Program agents, and they often utilize the knowledge and skills of each other in the investigation of computer crimes (C. LeFever, personal communication, 12/6/2004).

The resources used by agencies vary by jurisdiction. These can include basic police resources, as well as the inclusion of additional external resources, such as support agencies and field professionals.

Does your agency have a computer crimes unit? If so, how many officers are in it? What are their official duties?

MSPCCU is the computer crimes unit for Maryland State Police. While there is no set number of officers who work in the computer crimes unit, there are currently ten officers working within the unit. Five of the officers are digital media analysts and five are responsible for Internet investigation. Sgt. Smolek explained the current number of employees is an average number for the agency. He went on to say the amount of officers

in the computer crimes unit is determined largely by government representatives, such as the Governor and the Superintendent. Sgt. Smolek believes the number of officers currently working in the unit will not be reduced, but stated that when the number of officers are reduced – as recently occurred with the loss of two officers from the unit – the average workload increases (Sgt. Smolek, personal communication, 11/18/2004).

The MCCCCU is a substantially smaller investigative agency than the MSPCCU, with a much narrower jurisdiction. As such, the MCCCCU consists of only one investigator (Sgt. G. Renninger, personal communication, 11/18/2004).

The Maryland States Attorneys office has a Computer Crime Unit comprised of 2 prosecutors (P. Feeny, personal communication, 12/1/2004).

The USSS' computer crime unit, formally titled the Electronic Crimes Special Agent Program, currently consists of just Special Agent Chris LeFever, but is soon expected to expand to include a number of agents who will form a working group (C. LeFever, personal communication, 12/6/2004).

What backgrounds do those who deal with computer crime/computer fraud have in your agency?

Officers selected to work in MSPCCU are chosen for a number of characteristics. They must have a criminal investigation background. Sgt. Smolek commented this helps prove they are self-motivated and have investigative experience. In addition, MSPCCU looks for individuals who are computer hobbyist and hold a personal interest in the field. Furthermore, officers with an analytical mind are desired. Sgt. Smolek explained that computer crime work is often slow-paced analytical work. As such, he stated that

MSPCCU is not the place for “action junkies.” (Sgt. Smolek, personal communication, 11/18/2004)

The investigator in the MCCCUC has a background in basic investigative experience, as well as specialized training in Internet investigations (Sgt. G. Renninger, personal communication, 11/18/2004).

The training instructors at the NW3C for the most part have military and law enforcement backgrounds. In addition to instructors with prior experience, the NW3C has recently begun to hire recent graduates with Master’s degrees in the forensics sciences (B. Crane, personal communication, 11/28/04).

As previously stated, Lt. Lee explained that there is no computer crime unit at the PGCPD (Lt. Allen Lee, personal communication, 11/19/2004).

The members of the Maryland State Attorneys office Computer Crime Unit have a legal background, and one member has an MBA (P. Feeny, personal communication, 12/1/2004).

Special Agent LeFever background for his position with the USSS consists of three and a half weeks of training on computer hardware and software. Additionally, he was trained for a similar amount of time on computer forensics. He has also received a number of industry certifications, and has completed two years worth of practical experience in the information technology industry (C. LeFever, personal communication, 12/6/2004).

As can be seen, backgrounds generally included basic police training, prior experience, and often specialized training for addressing computer crimes and fraud.

Do these individuals receive special training to handle computer crime/computer fraud?

Individuals working for MSPCCU receive a lot of training. They receive in-house training, as well as have access to area resources. Sgt. Smolek described the close proximity of training facilities at the FBI, National White Collar Crime Center, and Department of Defense as a “geographical advantage.” The training covers a wide variety of elements, because computer crimes are primarily “...old crimes with new technologies...[incorporating] new types of evidence and new investigative strategies.” (Sgt. Smolek, personal communication, 11/18/2004) In addition, the officers teach “boot camps” for investigating computer crimes. MSPCCU does not utilize commercial computer crime programs because of the belief that they do not deliver the quality of training advertised. The only private courses valued by MSPCCU are ones specifically designed with a law enforcement focus and run by respected entities (Sgt. Smolek, personal communication, 11/18/2004).

Investigators in MCCCUC also receive training in their position. Sgt. Renninger was less forthcoming with details regarding this training and simply referred to it as Internet investigative training (Sgt. G. Renninger, personal communication, 11/18/2004).

The instructors’ training at the NW3C consists of several elements. Instructors are given on-the-job training, as well as provided with training outside of NW3C. In addition, NW3C also utilizes an internship program to provide special training to its employees (B. Crane, personal communication, 11/28/04).

Peter Feeny has received extensive training to handle computer crime. He has taken courses at the NW3C on “Basic Data and Analysis”, which is a course in recovering data from computers. He has taken “Cybersleuth1” and “Cybersleuth2” which were put on by the National District Attorney’s Association. Additionally, he has

taken courses put on by the National Center for Exploited and Missing Children called “SafetyNet”, an introduction to computer crime course put on by the National Association of Attorney Generals. Finally, he has taken a course on computer crime by the DOJ (P. Feeny, personal communication, 12/1/2004).

The training regime for the USSS consists of the aforementioned multi-week training on both computer technology and forensics, as well as additional optional courses on specific specialized technology and information, such as network intrusions and Personal Data Assistants (C. LeFever, personal communication, 12/6/2004).

Are the individuals who deal with computer crime/computer fraud solely responsible for addressing this type of crime, or do they also work on other crime types?

Officers within MSPCCU are primarily dedicated to addressing computer crime and fraud. However, as Maryland State Police officers, they can be pulled to aid in other efforts, such as the 2001 sniper incident (Sgt. Smolek, personal communication, 11/18/2004).

The investigator in MCCCCU is also specifically responsible for computer crime and computer fraud investigations. However, he is not involved in other investigative matters within the Montgomery County Department of Police. The MCCCCU investigator deals directly with computer crime and data recovery issues (Sgt. G. Renninger, personal communication, 11/18/2004).

Similarly, the instructors at the NW3C are specifically responsible for work involving computer crime and computer fraud. This is understandable, considering their positions are as investigators in an auxiliary training organization for law enforcement

agencies. Specifically, these investigators train solely in computer forensics and Cybercrime investigations (B. Crane, personal communication, 11/28/04).

Everyone at the Maryland States Attorneys office has other responsibilities in addition to working on computer crime cases. Computer crime cases account for twenty-five percent of their workload (P. Feeny, personal communication, 12/1/2004).

Similarly, agents within the USSS are involved in each type of case brought to them, rather than having specific agents who focus solely on computer crime and computer fraud (C. LeFever, personal communication, 12/06/2004).

What techniques has your agency found to be successful in investigating/preventing/prosecuting computer crime/computer fraud?

Techniques found to be successful by MSPCCU are identifying the account and user responsible for specific offenses, as well as gather evidence. Essential to a successful investigation is gathering enough evidence to develop sufficient probable cause. This also relates to getting judicial approval to get to probable cause (Sgt. Smolek, personal communication, 11/18/2004).

The jurisdiction and computer crime unit resources of MCCCUC are much more limited than those of the Maryland State Police. MCCCUC relies on finding local victims who are willing to come to court as a successful means of addressing computer crimes they are investigating (Sgt. G. Renninger, personal communication, 11/18/2004).

Preparation is the only technique that the Maryland States Attorney office have found successful in prosecuting these crimes (P. Feeny, personal communication, 12/1/2004).

Gathering evidence and having sufficient preparation were common themes of the agencies. Also, the ease of investigating is considered, such as the location of offenders and victims.

Where do you/your agency have the most difficulty dealing with computer crime/computer fraud?

The most difficult element MSPCCU faces is outsourcing to get information. The process required to get records and the jurisdictional aspect describes this outsourcing. In order to get records, MSPCCU must go to first get a subpoena from the appropriate state's attorney office. This subpoena is then given to the source that has the required records, such as Internet service providers. Sgt. Smolek describes this as a "stop and go" process that can take upwards of three weeks. Again, Sgt. Smolek noted computer crime and fraud cases for MSPCCU are detail-oriented and not quickly consummated (Sgt. Smolek, personal communication, 11/18/2004).

Similarly to MSPCCU, Sgt. Renninger comments about the difficulties jurisdictional issues bring to investigating instances of computer crime and computer fraud (Sgt. G. Renninger, personal communication, 11/18/2004).

Getting cases, case referrals, and the like seems to be the major difficulties in dealing with computer crime for the States Attorney's office (P. Feeny, personal communication, 12/1/2004).

The respondent from USSS also highlighted the difficulty of retrieving information from third party sources in the interest of advancing cases. Specifically, he mentioned the difficulty in dealing with overseas Internet Service Providers (C. LeFever, 12/6/2004).

What resources would you like to see available to use in addressing computer crime/computer fraud?

The element most desired by the MSPCCU is to ease the legal process of acquiring a subpoena. Sgt. Smolek comments, "The reality of it is Internet crime is a fact, not a trend." (Sgt. R Smolek, personal communication, 11/19/2004) Attempting to address these new crimes with the current legal infrastructure is complicated and places a burden on law enforcement and those involved in a case to acquire the required subpoenas from the correct jurisdiction. Administrative subpoena authority would allow officers to create the subpoena for cases themselves, effectively eliminating one of the most cumbersome and demanding parts of the investigative process. Additionally, he suggests extraterritorial search warrants for judges, which would allow search warrants to not be confined to a single jurisdiction. Sgt. Smolek feels these resources would make a significant contribution to MSPCCU in addressing computer crimes and computer fraud in the future by eliminating the involvement of representatives from multiple jurisdictions (Sgt. R. Smolek, personal communication, 11/19/2004).

Alternatively, Sgt. Renninger does not feel MCCCUC needs any additional resources to investigate computer crime issues. He notes that all of the resources he believes are necessary are already available to his agency (Sgt. G. Renninger, personal communication, 11/18/2004).

The manager of the Computer Crimes Section of the NW3C feels additional funding would be the best benefit for addressing computer crime and computer fraud in the future. By having additional funding available for law enforcement training, officers from around the country would have a greater opportunity to attend training offered by

the NW3C (B. Crane, personal communication, 11/28/04). Currently, funding for specific elements of training, such as the travel and accommodations of officers may limit the amount and variety of officers who can receive NW3C instruction.

Peter Feeny would like to have an additional prosecutor in the Computer Crime unit. Also, he would like to see more correspondence and dedication of resources with county and state police agencies. Finally, he suggests there needs to be more manpower to fight computer crime (P. Feeny, personal communication, 12/1/2004).

Special Agent LeFever desires to see more standardized training across different government agencies. Additionally, he believes more abundant input from computer investigators in development of software programs would be beneficial for fighting computer crime and fraud (C. LeFever, personal communication, 12/6/2004).

What do you think is needed in order to be more effective in combating this type of crime?

The MSPCCU believes several items are required for their agency to become more effective against computer crime. At the most general level, they believe there needs to be a "...top-down realization that Internet crime is a fact, not a trend." (Sgt. R. Smolek, personal communication, 11/19/2004) Once all levels of law enforcement and the legal system understand computer crime is a realistic, permanent crime category, addressing it will become easier. Additionally, MSPCCU highlights the need for more training, both for street-level officers, as well as prosecutors. Sgt. Smolek suggests regionalized law enforcement training, and urges groups such as the Maryland Police Training Commission to offer their services to regional law enforcement agencies. Finally, MSPCCU states the need to evaluate and address the existing model for dealing

with computer crime and fraud. In regards to this element, Sgt. Smolek believes the internet itself can be more fully utilized as a resource, such as interviewing witnesses in real-time by camera – similar to the existing bail review by camera – as a way to reduce the need to transport witnesses into the jurisdiction from across the country (Sgt. R. Smolek, personal communication, 11/19/2004).

Coming from a local perspective, Sgt. Renninger feels MCCCUC effectively deals with the computer crime and fraud cases that are referred to them by the National White Collar Crime Center. He does not believe his agency requires anything further to be more effective in addressing the computer crime and fraud the deal with, namely online auction fraud and hate emails (Sgt. G. Renninger, personal communication, 11/18/2004).

The elements highlighted as necessary for more effective handling of computer crime and computer fraud by the NW3C mirror those of the State Police. The required elements include more extensive funding and training for computer crime and computer fraud, as well as better awareness and managerial support of these issues (B. Crane, personal communication, 11/28/04).

Peter Feeny would like to have an additional prosecutor in the Computer Crime unit. Also, he would like to see more correspondence and dedication of resources with county and state police agencies. Finally, there needs to be more manpower to fight computer crime (P. Feeny, personal communication, 12/1/2004).

Are existing statutes broad enough to cover all forms of criminal activity committed with the use/aid of a computer? Why or why not?

MSPCCU's Sgt. Smolek believes the existing statutes are not comprehensive enough to cover all of computer crime and computer fraud. Because our existing legal

code is based on English law and has slowly evolved over time as necessary, it is not currently able to fully address computer crime. MSPCCU suggests all legislation be examined to evaluate how it addresses computer crime and fraud. An illustrative example provided by Sgt. Smolek relates to current Maryland harassment laws. Currently, the victim telling the offender to stop is a required element to move forward; but this becomes difficult in a digital medium where the offender may be unreachable or may be using a different method to harass the victim, such as posting fraudulent online profiles of the victim (Sgt. R. Smolek, personal communication, 11/19/2004).

Alternatively, Sgt. Renninger of MCCCUC feels the existing laws and statutes adequately cover all forms of computer crime (Sgt. G. Renninger, personal communication, 11/18/2004). The NW3C representative also finds that the existing legal infrastructure to be adequate in dealing with these forms of crime (B. Crane, personal communication, 11/28/04).

Peter Feeny believes that the existing Maryland state statutes are broad enough to cover all forms of criminal activity committed with the use of/aid of a computer. He thinks jurisdictional issues need to be addressed (P. Feeny, personal communication, 12/1/2004).

What liaisons do you have with other agencies?

The MSPCCU currently has liaisons with the Maryland Police agencies, as well as the FBI child pornography initiative, Innocent Images. Many of these liaisons are in place to ensure there is not conflict of cases occurring. Additionally, MSPCCU maintains liaisons with a variety of online entities, such as various Internet Service

Providers, America Online, and PayPal's fraud department (Sgt. R. Smolek, personal communication, 11/19/2004).

The MCCCUC maintains liaisons with the NW3C, which is the agency responsible for referring computer crime and fraud cases to them, as well as the Federal Trade Commission (Sgt. G. Renninger, personal communication, 11/18/2004).

The liaisons maintained by the NW3C range from the local level to federal agencies. The NW3C has working partnerships with local, state, and federal agencies, including the FBI, Secret Service, the Internal Revenue Service, and the Department of Homeland Security (B. Crane, personal communication, 11/28/04). This wide range of alliances is specifically due to their training and support roles.

The members of the Computer Crime Unit are the liaisons to other agencies (P. Feeny, personal communication, 12/1/2004).

Within the USSS, Special Agent LeFever is hopeful the Electronic Crimes Special Agent Program will provide a wealth of liaisons in the future. Currently, both local agencies and professional organizations are the main source of liaisons for this agency (C. LeFever, personal communication, 12/6/2004).

Does your agency refer computer crime/computer fraud investigation or complaints to other agencies?

MSPCCU periodically refers specific cases to other agencies. Crimes with an international element may be referred out, as well as crimes against children, which can be referred to Customs. Crimes against children are generally referred out to the appropriate task force, of which forty-five exist. Sgt. Smolek notes that Maryland

currently lacks the advancement of jurisdiction needed to advance cases to other jurisdictions (Sgt. R. Smolek, personal communication, 11/19/2004).

MCCCU refers its computer crime and fraud information back to the NW3C where it is compiled into a central database. This database is a repository for all computer-related crime complaints (Sgt. G. Renninger, personal communication, 11/18/2004).

The Maryland States Attorneys office also refers computer crime cases to other agencies. Child pornography cases are referred to the U.S. Attorney's office. Online auction fraud cases are referred to other law enforcement agencies (P. Feeny, personal communication, 12/1/2004).

USSS refers cases to other agencies when they see the need for the specialized expertise of another agency. If another agency has preexisting resources or information that would be beneficial to handling the case, or if the case is outside the area of focus of the USSS, the investigation may be forwarded to that agency. For example, cases regarding child pornography are often forwarded to another agency (C. LeFever, personal communication, 12/6/2004).

How successful has your agency been in addressing computer crime/computer fraud thus far?

Sgt. Smolek considers the MSPCCU to be very successful in dealing with computer crime and fraud suspects that are in state. In regards to this, he notes anyone can be successful in addressing in-state computer crime cases. However, he admits MSPCCU is less successful in addressing the overall volume of cases. Because of the sheer amount of cases, MSPCCU is often forced to triage cases and prioritize them,

addressing first the cases where then can accomplish the most for their effort (Sgt. R. Smolek, personal communication, 11/19/2004).

Sgt. Renninger also believes the MCCCUC has been highly successful in addressing the computer crimes that have been referred by the NW3C. He notes one stipulation of the need for victims to be willing to cooperate in order for the agency to be fully successful (Sgt. G. Renninger, personal communication, 11/18/2004).

Peter Feeny said that his office has a 100 percent conviction rate. Every case indicted always leads to a finding of guilt (P. Feeny, personal communication, 12/1/2004).

Despite not providing a clear case load or clearance rate, Special Agent Chris LeFever feels the USSS is successful in handling computer crimes they address, considering the amount of time and effort given to other demands, such as an array of protective services and the recent Presidential campaign (C. LeFever, personal communication, 12/6/2004).

What do you see as the major areas of attention regarding computer crime/computer fraud in the future?

MSPCCUC believes the focus regarding computer crime and fraud in the future should be three-fold. Legislation should be given the tools to allow for the successful investigation of computer crime, law enforcement agencies should be provided with adequate computer crime training, and an emphasis should be placed on the education of consumers regarding these sorts of crimes (Sgt. R. Smolek, personal communication, 11/19/2004).

More specifically, MCCCUC believes phishing – the misrepresentation of legitimate businesses to fraudulently acquire personal information – will be a major area of attention within computer crime types in the future (Sgt. G. Renninger, personal communication, 11/18/2004).

Correspondingly, the NW3C also feels the vast majority of Internet-based criminal activities will be the major area of focus in the future (B. Crane, personal communication, 11/28/04). Interestingly, the example given for these activities by the NW3C Computer Crimes Section Manager was phishing, the same crime noted by MCCCUC.

Peter Feeny sees jurisdictional issues and technology issues as the major areas of attention regarding computer crime (P. Feeny, personal communication, 12/1/2004).

Special Agent LeFever thinks the increase in home computers and personal electronics being used to counterfeit currency is becoming a larger issue. Additionally, he sees a significant change in the number of fraud schemes that utilize email resources rather than the telephone (C. LeFever, personal communication, 12/6/2004).

Do you have any contacts that you believe would be able to provide helpful information regarding this study?

Sgt. Smolek is eager to offer his services for future efforts related to addressing computer crime, and also suggests examining other states' computer crime units, such as those in New York City, Pennsylvania, and Delaware (Sgt. R. Smolek, personal communication, 11/19/2004).

Sgt. Renninger suggests contacting the National White Collar Crime Center for more information (Sgt. G. Renninger, personal communication, 11/18/2004).

Mr. Crane believes the statistical information on computer crime and computer fraud complaints available from the Internet Fraud Complaint Center would be useful (B. Crane, personal communication, 11/28/04).

Peter Feeny says that the FBI should be contacted (P. Feeny, personal communication, 12/1/2004).

Conclusions

As a result of the literature review and discussion with representatives in the field, a number of conclusions regarding the future of law enforcement's efforts towards computer crime and computer fraud can be drawn. By synthesizing and creating some recommendations from this information, the efforts of law enforcement will be better prepared to address this crime type. We make the following recommendations, and each is discussed below:

- Uniform definition
- Statistical records
- Jurisdictional issues
- Training and available resources
- Crime reporting
- Legal review
- Further research

The creation of a uniform definition for both computer crime, as well as computer fraud, is the most immediate need for addressing this form of crime. As can be seen in both the literature and the intensive interviews, the definitions currently in place are varied and limited. Without a standard way to define these forms of crime, agencies cannot be sure they are consistently addressing the same topics. Additionally, the lack of clear and consistent definitions compromises the ability to track the nature and extent of computer crime and fraud.

Statistical data and a recording system are required to determine the change in trends of this form of crime, as well as to grasp a greater understanding of its

characteristics. Through the use of standardized practices and understandings regarding computer crime and computer fraud, statistics can be collected to gain insight into computer-related crimes. This will allow law enforcement to be able to better understand the issues they are confronting, and better apply the resources available to them. Once it is assured that agencies have a uniform understanding of computer crime and fraud, even the simple addition of a question concerning the use of a computer to crime reports can generate a wealth of information.

Another issue frequently seen involves jurisdictional issues inherent to computer crime investigations. Law enforcement agencies dealing with computer crime are hampered by jurisdictional limitations. Computer crime investigations essentially require agencies to cooperate with representatives from other regions to complete their work. Realizing these issues exist, a review and reevaluation of the ability of agencies to operate outside of their jurisdiction – such as in the execution of out of state subpoenas – would help law enforcement to more easily conduct these forms of investigation. In the event that no changes can be made to the jurisdictional limitations currently in place, and as a general good practice, law enforcement needs to continue to encourage interagency collaboration in addressing these issues.

Training and resources available to law enforcement must also be improved. It is recommended that comprehensive computer crime investigation and electronic crime scene training be a requirement for all law enforcement agencies. This will allow officers to be prepared to handle issues and complaints regarding computer crime and fraud, will provide all law enforcement to better understand the issues they are facing, and will ensure these investigations are handled in a standardized way. While some areas have a

geographical advantage in available training resources, other agencies need to provide additional resources to ensure this training is offered. Overall, there needs to be consistent managerial support for officers addressing these forms of crime.

Furthermore, a consistent finding is the low level of victim reporting and sporadic community awareness and reporting outlets. The efforts currently in place should be continued, and there should be a focus on computer crime and fraud awareness for both law enforcement and organizations in the future. Despite the best efforts of investigators, much of the responsibility lies in victims being able to identify their victimization, and knowing to whom and how to report the incident.

In regards to the laws and statutes currently in place, there are mixed reactions to their adequacy in addressing computer crime and computer fraud. An examination of the legal infrastructure should be conducted to see which laws currently in place can be adapted to handle these forms of crime, as well as what areas are not covered by existing legislation. This should allow lawmakers, law enforcement, and prosecutors to have a better understanding of the options available to them.

In general, continued research and publications should be created that specifically address computer crime and fraud issues. These efforts will allow the subject to be more fully researched, and will keep those involved in its prevention, investigation and prosecution abreast of emerging trends, as well as noteworthy cases, relevant legislation, and significant efforts being undertaken. This work will also help validate this crime type, and will encourage its research and efforts taken to address it. Moreover, a resource of relevant contacts should be created, maintained, and distributed. This resource should include area contacts with specialized knowledge of specific areas of computer crime and

fraud, as well as computer crime contacts for different jurisdictions. This could be an invaluable source of information for investigators in the future.

Computer crime and computer fraud are increasingly becoming a major crime threat. However, as can be seen in past research and through discussions of current law enforcement representatives, the efforts to mediate this threat are varied and faced with challenges. These topics should be a major focus of law enforcement in the future, matching the resources in place today with specific suggested improvements and adaptations. Law enforcement agencies can take advantage of the opportunity to expand their efforts to address computer crime and computer fraud in order to keep pace with this emerging crime category.

Appendix A

Preventing Internet Crime

The following prevention tips were created by the Internet Crime Complaint Center. The subsequent tips are listed in their original text and can be found at the following web site: http://www1.ifccfbi.gov/strategy/2003_IC3Report.pdf on pages 17-20.

Internet Auction Fraud

- Understand as much as possible about how Internet auction works, what your obligations are as a buyer, and what the seller's obligations are before you bid.
- Find out what actions the website takes if a problem occurs and consider insuring the transaction and shipment.
- Learn as much as possible about the seller, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where the seller/business is located.
- Examine the feedback on the seller, and use common sense. If the seller has a history of negative feedback, then do not deal with that particular seller.
- Determine what method of payment the seller is asking for and where he/she is asking to send payment. Use caution when the mailing address is a post office box number.
- Be aware of the difference in laws governing auctions between the U.S. and other countries. If a problem occurs with the auction transaction that has the seller in one country and a buyer in another, it might result in a dubious outcome leaving you empty handed.
- Be sure to ask the seller about when delivery can be expected and warranty/exchange information for merchandise that you might want to return.
- To avoid unexpected costs, find out if shipping and delivery are included in the auction price or are additional.
- Finally, avoid giving out your social security or driver's license number to the seller, as the sellers have no need for this information.

If you are victimized you should take the following steps.

- File a complaint with the online auction company. In order to be considered for eBay's Fraud Protection Program, you should submit an online Fraud Complaint at <http://crs.ebay.com/aw-cgi/ebayisapi.dll?crsstartpage> 30 days after the listing end-date.
- File a complaint with the Internet Crime Complaint Center (<http://www.ic3.gov>)
- Contact law enforcement officials at the local and state level
- Also contact law-enforcement officials in the perpetrator's town and state
- File a complaint with the shipper USPS
- File a complaint with the National Fraud Information Center (<http://www.fraud.org/info/contactnfic.htm>)
- File a complaint with the Better Business Bureau (<http://www.bbb.org>)

Non-Delivery of Merchandise

- Make sure you are purchasing merchandise from a reputable source. As with auction fraud, check the reputation of the seller whenever possible, including the Better Business Bureau.
- Try to obtain a physical address rather than merely a post office box and a phone number. Also call the seller to see if the number is correct and working.
- Send them e-mail to see if they have an active e-mail address. Be cautious of sellers who use free e-mail services where a credit card wasn't required to open the account.
- Investigate other web sites regarding this person/company
- Do not judge a person/company by their fancy web site; thoroughly check the person/company out.
- Be cautious when responding to special offers (especially through unsolicited e-mail).
- Be cautious when dealing with individuals/companies from outside your own country. Remember the laws of different countries might pose issues if a problem arises with your transaction.
- Inquire about returns and warranties on all items.
- The safest way to purchase items via the Internet is by credit card because you can often dispute the charges if something is wrong. Also, consider utilizing an escrow or alternate payment service.
- Make sure the web site is secure when you electronically send your credit card numbers.

Credit Card Fraud

- Don't give out your credit card number(s) online unless the site is both secure and reputable. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. The icon is not a guarantee of a secure site, but may provide you some assurance.
- Before using the site, check out the security software it uses; make sure your information will be protected.
- Make sure you are purchasing merchandise from a reputable/legitimate source. Once again investigate the person or company before purchasing products.
- Try to obtain a physical address rather than merely a post office box and a phone number, call the seller to see if the number is correct and working.
- Send them e-mail to see if they have an active e-mail address and be wary of sellers who use free e-mail service where a credit card wasn't required to open the account.
- Do not purchase from sellers who won't provide you with this type of information.
- Check with the Better Business Bureau to see if there have been any complaints against the seller before.
- Check out other web sites regarding this person/company
- Be cautious when responding to special offers (especially through unsolicited e-mail).

- Be cautious when dealing with individuals/companies from outside your own country.
- If you are going to purchase an item via the Internet, use a credit card since you can often dispute the charges if something does go wrong.
- Make sure the transaction is secure when you electronically send your credit card somewhere.
- You should keep a list of all your credit cards and account information along with the card issuer's contact information. If anything looks suspicious or you lose your credit card(s) contact the card issuer immediately.

Investment Fraud

- Don't invest in anything based on appearances. Just because an individual or company has a flashy web site doesn't mean it is legitimate. Web sites can be created in just a few days. After a short period of taking money, a site can vanish without a trace.
- Don't invest in anything you are not absolutely sure about. Do your homework on the investment to ensure that it is legitimate.
- Thoroughly investigate the individual or company to ensure that they are legitimate.
- Check out other web sites regarding this person/company.
- Be cautious when responding to special investment offers (especially through unsolicited e-mail) by fast talking telemarketers. Know whom you are dealing with!
- Inquire about all the terms and conditions dealing with the investors and the investment.
- Rule of thumb: If it sounds too good to be true, it probably is.

Nigerian Letter Scam/419 Scam

- Be skeptical of individuals representing themselves as Nigerian or other foreign government officials asking for your help in placing large sums of money in overseas bank accounts.
- Do you believe the promise of large sums of money for your cooperation.
- Do not give out any personal information regarding your savings, checking, credit, or other financial accounts.
- If you are solicited, do not respond and quickly notify the appropriate authorities.

Cyberstalking

- Use a gender-neutral name/e-mail address.
- Use a free e-mail account such as Hotmail or Yahoo! For newsgroup/ mailing lists, chat rooms, IMs, e-mails from strangers, message boards, filling out forms and other online activities.
- Don't give your primary e-mail address to anyone you do not know or trust.
- Instruct children to never give out their real name, age, address, or phone number over the net without your permission.

- Don't provide your credit card number or other information as proof of age to access or subscribe to a website you're not familiar with.
- Lurk on newsgroups, mailing lists and chat rooms before "speaking" or posting messages.
- When you do participate online, be careful-only type what you would say to someone's face.
- Don't be so trusting online-don't reveal personal things about yourself until you really and truly know the other person.
- Your first instinct may be to defend yourself-don't-this is how most online harassment situations begin.
- If it looks too good to be true-it is.

Phishing

The following prevention tips were created by the Anti-Phishing Working Group. The subsequent tips are listed in their original text and can be found at the following web site: <http://www.antiphishing.org>.

- Be suspicious of any email with urgent requests for personal financial information
 - unless the email is digitally signed, you can't be sure it wasn't forged or 'spoofed'
 - phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately
 - they typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc.
 - phisher emails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are
- Don't use the links in an email to get to any web page, if you suspect the message might not be authentic
 - instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser
- Avoid filling out forms in email messages that ask for personal financial information
 - you should only communicate information such as credit card numbers or account information via a secure website or the telephone
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser
 - to make sure you're on a secure Web server, check the beginning of the Web address in your browser's address bar – it should be "https://" rather than just "http://"
- Consider installing a Web browser tool bar to help protect you from known phishing fraud websites

- EarthLink ScamBlocker is part of a free browser toolbar that alerts you before you visit a page that's on Earthlink's list of known fraudulent phisher Web sites.
 - Its free to all Internet users – download at <http://www.earthlink.net/earthlinktoolbar>
- Regularly log into your online accounts
 - don't leave it for as long as a month before you check each account
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate
 - if anything is suspicious, contact your bank and all card issuers
- Ensure that your browser is up to date and security patches applied
 - in particular, people who use the Microsoft Internet Explorer browser should immediately go to the Microsoft Security home page – <http://www.microsoft.com/security/> -- to download a special patch relating to certain phishing schemes
- Always report “phishing” or “spoofed” e-mails to the following groups:
 - forward the email to reportphishing@antiphishing.com
 - forward the email to the Federal Trade Commission at spam@uce.gov
 - forward the email to the “abuse” email address at the company that is being spoofed (e.g. “spoof@ebay.com”)
 - when forwarding spoofed messages, always include the entire original email with its original header information intact
 - notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov/

How to Report Computer Crime

The subsequent was created by the Computer Crime and Intellectual Property Section and can be found in its entirety at the following web site www.cybercrime.gov/reporting.htm.

<i>Type of Crime</i>	<i>Appropriate Federal Investigative Law Enforcement Agencies</i>
Computer Intrusion (i.e. hacking)	<ul style="list-style-type: none">• FBI local office• U.S. Secret Service• Internet Fraud Complaint Center
Password Trafficking	<ul style="list-style-type: none">• FBI local office• U.S. Secret Service• Internet Fraud Complaint Center
Copyright (software, movie, sound recording) piracy	<ul style="list-style-type: none">• FBI local office• If imported, U.S. Customs and Border Patrol Protection local office• Internet Fraud Complaint Center
Theft of trade secrets	<ul style="list-style-type: none">• FBI local office
Trademark counterfeiting	<ul style="list-style-type: none">• FBI local office• If imported, U.S. Customs and Border Patrol Protection local office• Internet Fraud Complaint Center
Counterfeiting of currency	<ul style="list-style-type: none">• FBI local office• U.S. Secret Service• Internet Fraud Complaint Center
Child Pornography or Exploitation	<ul style="list-style-type: none">• FBI local office• If imported, U.S. Customs and Border Patrol Protection local office• Internet Fraud Complaint Center
Child Exploitation and Internet Fraud matters that have a mail nexus	<ul style="list-style-type: none">• U.S. Postal Inspection Service• Internet Fraud Complaint Center
Internet Fraud and Spam	<ul style="list-style-type: none">• FBI local office• U.S. Secret Service• Federal Trade Commission• Securities and Exchange Commission• Internet Fraud Complaint Center
Internet Harassment	<ul style="list-style-type: none">• FBI local office

Internet bomb threats	<ul style="list-style-type: none"> • FBI local office • ATF local office
Trafficking in explosive or incendiary devices or firearms over the Internet	<ul style="list-style-type: none"> • FBI local office • ATF local office
Phishing	<ul style="list-style-type: none"> • FBI local office • Anti-Phishing Working Group at www.antiphishing.org

Appendix B
State Computer Crime Statutes

State	Computer Crime Laws
Arizona	<ul style="list-style-type: none"> • Computer tampering • Interception of wire, electronic and oral communications; installations of pen register or trap and trace device • Divulging communication service information • Possession of interception devices • Stored oral, wire and electronic communications; agency access; backup preservation; delayed notice; records preservation request • Cyberstalking
California	<ul style="list-style-type: none"> • Unauthorized access to computers • Cyberfraud • Cyberstalking
Connecticut	<ul style="list-style-type: none"> • Unauthorized access to a computer system • Interruption of computer services • Misuse of computer system information • Destruction of computer equipment • Cyberstalking
Florida	<ul style="list-style-type: none"> • Offenses against intellectual property • Offenses against computer equipment or supplies • Offenses against computer users • Cyberstalking • Using the Internet in dealing stolen property
Iowa	<ul style="list-style-type: none"> • Unauthorized access • Computer damage • Computer theft • Cyberstalking
Maryland	<ul style="list-style-type: none"> • False entry in public record; altering, defacing, destroying, removing or concealing public record; accessing public record • Credit Card Fraud • Unauthorized access to computers • Cyberstalking
Massachusetts	<ul style="list-style-type: none"> • Larceny • Fraudulent obtaining of commercial computer service • Stolen trade secrets; buying or selling • Unauthorized accessing of computer systems • Cyberstalking

New York	<ul style="list-style-type: none"> • Unauthorized use of a computer • Computer Trespass • Computer tampering • Unlawful duplication of computer related material • Criminal possession of computer related material • Cyberstalking
Texas	<ul style="list-style-type: none"> • Breach of Computer Security • Cyberstalking • Assistance by Attorney General
Virginia	<ul style="list-style-type: none"> • Computer fraud • Transmission of unsolicited bulk electronic mail • Computer trespass • Computer invasion of privacy • Theft of computer services • Personal trespass by computer • Computer as instrument of forgery • Cyberstalking

Arizona State Laws:

13-2316. Computer tampering; venue; forfeiture; classification

A. A person who acts without authority or who exceeds authorization of use commits computer tampering by:

1. Accessing, altering, damaging or destroying any computer, computer system or network, or any part of a computer, computer system or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or to control property or services by means of false or fraudulent pretenses, representations or promises.
2. Knowingly altering, damaging, deleting or destroying computer programs or data.
3. Knowingly introducing a computer contaminant into any computer, computer system or network.
4. Recklessly disrupting or causing the disruption of computer, computer system or network services or denying or causing the denial of computer or network services to any authorized user of a computer, computer system or network.
5. Recklessly using a computer, computer system or network to engage in a scheme or course of conduct that is directed at another person and that seriously alarms, torments, threatens or terrorizes the person. For the purposes of this paragraph, the conduct must both:
 - a. Cause a reasonable person to suffer substantial emotional distress.
 - b. Serve no legitimate purpose.
6. Preventing a computer user from exiting a site, computer system or network-connected location in order to compel the user's computer to continue communicating with, connecting to or displaying the content of the service, site or system.
7. Knowingly obtaining any information that is required by law to be kept confidential or any records that are not public records by accessing any computer, computer system or network that is operated by this state, a political subdivision of this state or a medical institution.
8. Knowingly accessing any computer, computer system or network or any computer software, program or data that is contained in a computer, computer system or network.

B. In addition to section 13-109, a prosecution for a violation of this section may be tried in any of the following counties:

1. The county in which the victimized computer, computer system or network is located.

2. The county in which the computer, computer system or network that was used in the commission of the offense is located or in which any books, records, documents, property, financial instruments, computer software, data, access devices or instruments of the offense were used.
3. The county in which any authorized user was denied service or in which an authorized user's service was interrupted.
4. The county in which critical infrastructure resources were tampered with or affected.

C. On conviction of a violation of this section, the court shall order that any computer system or instrument of communication that was owned or used exclusively by the defendant and that was used in the commission of the offense be forfeited and sold, destroyed or otherwise properly disposed.

D. A violation of subsection A, paragraph 6 of this section constitutes an unlawful practice under section 44-1522 and is in addition to all other causes of action, remedies and penalties that are available to this state. The attorney general may investigate and take appropriate action pursuant to title 44, chapter 10, article 7.

E. Computer tampering pursuant to subsection A, paragraph 1 of this section is a class 3 felony. Computer tampering pursuant to subsection A, paragraph 2, 3 or 4 of this section is a class 4 felony, unless the computer, computer system or network tampered with is a critical infrastructure resource, in which case it is a class 2 felony. Computer tampering pursuant to subsection A, paragraph 5 of this section is a class 5 felony. Computer tampering pursuant to subsection A, paragraph 7 or 8 of this section is a class 6 felony.

13-3005. Interception of wire, electronic and oral communications; installation of pen register or trap and trace device; classification; exceptions

A. Except as provided in this section and section 13-3012, a person is guilty of a class 5 felony who either:

1. Intentionally intercepts a wire or electronic communication to which he is not a party, or aids, authorizes, employs, procures or permits another to so do, without the consent of either a sender or receiver thereof.
2. Intentionally intercepts a conversation or discussion at which he is not present, or aids, authorizes, employs, procures or permits another to so do, without the consent of a party to such conversation or discussion.
3. Intentionally intercepts the deliberations of a jury or aids, authorizes, employs, procures or permits another to so do.

B. Except as provided in sections 13-3012 and 13-3017, a person who intentionally and without lawful authority installs or uses a pen register or trap and trace device on the telephone lines or communications facilities of another person which are utilized for wire or electronic communication is guilty of a class 6 felony.

13-3006. Divulging communication service information; classification; exception

A person is guilty of a class 6 felony who either:

1. Intentionally and without lawful authority obtains any knowledge of the contents of a wire or electronic communication by connivance with a communication service provider or its officer or employee.
2. Is a communications service provider, officer or employee of a communications service provider and intentionally divulges to anyone but the person for whom it was intended, except with the permission of the sender or the person for whom it was intended or in any case covered by the exemption in section 13-3012, the contents or the nature of a wire or electronic communication entrusted to the communications service provider for transmission or delivery.

13-3008. Possession of interception devices; classification

A. It is unlawful for a person to have in his possession or control any device, contrivance, machine or apparatus designed or primarily useful for the interception of wire, electronic or oral communications as defined in section 13-3001 with the intent to unlawfully use or employ or allow the device, contrivance, machine or apparatus to be used or employed for the interception, or having reason to know the device, contrivance, machine or apparatus is intended to be so used.

B. All property possessed or controlled by any person in violation of this section is subject to seizure and forfeiture pursuant to chapter 39 of this title.

C. A person who violates this section is guilty of a class 6 felony.

13-3009. Duty to report to law enforcement officers; classification

It shall be the duty of every communications service provider and its officers and employees to report any violation of sections 13-3005, 13-3006 and 13-3008 coming within their knowledge to the county attorney having jurisdiction and to the attorney general. Any intentional violation of this section is a class 3 misdemeanor.

13-3011. Disclosing confidential information relating to ex parte order; exceptions; classification

A. Except in any trial, hearing or other judicial proceeding, a person shall not knowingly disclose to another person any information concerning either:

1. The application for or the granting or denial of orders for the interception or installation of a pen register or trap and trace device or a request for the preservation of records or evidence pursuant to section 13-3016 or a subpoena issued pursuant to section 13-3018.

2. The identity of the person or persons whose communications are the subject of an ex parte order, subpoena or records preservation request granted pursuant to sections 13-3010, 13-3015, 13-3016, 13-3017 and 13-3018.

B. Subsection A of this section does not apply to the disclosure of information to the communication service provider whose facilities are involved or to an employee or other authorized agent of the county attorney, attorney general or law enforcement agency that applies for an order permitting interception or installation of a pen register or trap and trace device or who requests the preservation of records or evidence pursuant to section 13-3016 or a subpoena issued pursuant to section 13-3018.

C. Notwithstanding subsection A of this section, a peace officer or prosecuting attorney who obtains knowledge of the contents of a wire, electronic or oral communication as authorized by sections 13-3010, 13-3015, 13-3016, 13-3017 and 13-3018 or evidence derived from that knowledge may:

1. Disclose the contents of the communication to a peace officer or prosecuting attorney to the extent the disclosure is appropriate to the proper performance of the official duties of the peace officer or prosecuting attorney making or receiving the disclosure.
2. Use the contents of the communication to the extent that the use is appropriate to the proper performance of the official duties of the peace officer or prosecuting attorney.

D. A person who violates this section is guilty of a class 1 misdemeanor.

13-3016. Stored oral, wire and electronic communications; agency access; backup preservation; delayed notice; records preservation request; violation; classification

A. This section applies to oral, wire and electronic communications that are entrusted to a communication service provider or remote computing service solely for the purpose of transmission, storage or processing. Oral, wire and electronic communications that are in the possession of a person who is entitled to access the contents of such communications for any purpose other than transmission, storage or processing are ordinary business records that may be obtained by subpoena or court order.

B. An agency or political subdivision of this state may require the disclosure by a communication service provider or remote computing service of the contents of an oral, wire or electronic communication that has been in electronic storage for one hundred eighty days or less in one of the following ways:

1. Without prior notice to the subscriber or party, by obtaining a search warrant issued pursuant to chapter 38, article 8 of this title.
2. With prior notice to the subscriber or party, by serving a subpoena, except that notice may be delayed pursuant to subsection D of this section.

3. With prior notice to the subscriber or party, by obtaining a court order on an application and certification that contains specific and articulable facts showing that there are reasonable grounds to believe that the communication content sought is relevant to an ongoing criminal investigation, except that notice may be delayed pursuant to subsection D of this section.

C. An agency or political subdivision of this state may require the disclosure by a communication service provider or remote computing service of the contents of an oral, wire or electronic communication that has been in electronic storage for more than one hundred eighty days in one of the following ways:

1. Without notice to the subscriber or party, by obtaining a search warrant issued pursuant to chapter 38, article 8 of this title.
2. With prior notice to the subscriber or party, by serving a subpoena, except that notice may be delayed pursuant to subsection D of this section.
3. With prior notice to the subscriber or party, by obtaining a court order on an application and certification that contains specific and articulable facts showing that there are reasonable grounds to believe that the communication content sought is relevant to an ongoing criminal investigation, except that notice may be delayed pursuant to subsection D of this section.

D. Except as provided in subsection E of this section, the notice to the subscriber or party that is required by this section may be delayed for a period of not to exceed ninety days under any of the following circumstances:

1. If the applicant for a search warrant or court order pursuant to this section requests a delay of notification and the court finds that delay is necessary to protect the safety of any person or to prevent flight from prosecution, tampering with evidence, intimidation of witnesses or jeopardizing an investigation.
2. If the investigator or prosecuting attorney proceeding by subpoena executes a written certification that there is reason to believe that notice to the subscriber or party may result in danger to the safety of any person, flight from prosecution, tampering with evidence, intimidation of witnesses or jeopardizing an investigation. The agency shall retain a true copy of the certification with the subpoena.

E. If further delay of notification is necessary, extensions of up to ninety days each may be obtained by application to the court or certification pursuant to subsection D of this section.

F. Any agency acting pursuant to this section may apply for a court order directing the communication service provider or remote computing service not to notify any other person of the existence of the subpoena, court order or warrant for such period as the court deems appropriate. The court shall grant the application if it finds that there is reason to believe that notice may cause an adverse result described in subsection D of this

section. A person who violates an order issued pursuant to this subsection is guilty of a class 1 misdemeanor.

G. On the expiration of any period of delay under this section, the agency shall deliver to the subscriber or party a copy of the process used and notice including:

1. That information was requested from the service provider.
2. The date on which the information was requested.
3. That notification to the subscriber or party was delayed.
4. The identity of the court or agency ordering or certifying the delay.
5. The provision of this section by which delay was obtained.
6. That any challenge to the subpoena or order must be filed within fourteen days.

H. On the request of an agency or political subdivision of this state, a communication service provider or remote computing service shall take all necessary steps to preserve records, communication content and other evidence in its possession pending the issuance of a court order or other process. The communication service provider or remote computing service shall retain the preserved records, communication content and other evidence for ninety days. On the renewed request of an agency or political subdivision, the preservation period may be extended for an additional ninety days. Except as provided in section 13-3011, a person shall not notify the subscriber or party during the period of the preservation request

California State Laws:

CALIFORNIA CODES
PENAL CODE
PART 1. OF CRIMES AND PUNISHMENTS
TITLE 13. OF CRIMES AGAINST PROPERTY
CHAPTER 5. LARCENY [THEFT]

§ 502. Unauthorized access to computers, computer systems and computer data

(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of COMPUTER technology has resulted in a concomitant proliferation of COMPUTER CRIME and other forms of unauthorized access to COMPUTERS, COMPUTER systems, and COMPUTER data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

- (1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.
- (2) "Computer network" means any system which provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.
- (3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.
- (4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.
- (5) "Computer system" means a device or collection of devices, including support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contain

computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

- (6) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.
- (7) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.
- (8) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access.
- (9) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.
- (10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

- (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either
 - (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or
 - (B) wrongfully control or obtain money, property, or data.

- (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
- (3) Knowingly and without permission uses or causes to be used computer services.
- (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
- (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
- (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
- (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
- (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(d)

- (1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.
- (2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:
 - (A) For the first violation which does not result in injury, and where the value of the computer services used does not exceed four hundred dollars (\$400), by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.
 - (B) For any violation which results in a victim expenditure in an amount greater than five thousand dollars (\$5,000) or in an injury, or if the value of the computer services used exceeds four hundred dollars (\$400), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the state prison for 16 months, or two or

three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6), (7), or (8) of subdivision (c) is punishable as follows:

(A) For a first violation which does not result in injury, an infraction punishable by a fine not exceeding two hundred fifty dollars (\$250).

(B) For any violation which results in a victim expenditure in an amount not greater than five thousand dollars (\$5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation which results in a victim expenditure in an amount greater than five thousand dollars (\$5,000), by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(e)

(1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data may bring a civil action against any person convicted under this section for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees to a prevailing party.

(3) A community college, state university, or academic institution accredited in this state is required to include COMPUTER-RELATED CRIMES as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that effect.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) Any computer, computer system, computer network, or any software or data, owned by the defendant, which is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

(h)

(1) Subdivision (c) does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or data when acting within the scope of his or her lawful employment.

(2) Paragraph (3) of subdivision (c) does not apply to any employee who accesses or uses his or her employer's computer system, computer network, computer program, or data when acting outside the scope of his or her lawful employment, so long as the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or so long as the value of supplies and computer services, as defined in paragraph (4) of subdivision (b), which are used do not exceed an accumulated total of one hundred dollars (\$100).

(i) No activity exempted from prosecution under paragraph (2) of subdivision

(j) Which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

(k) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

(l) In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:

(1) The court shall consider prohibitions on access to and use of computers.

(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

California S.B. 757

Authorizes the investigation of illegal sales of tobacco products to minors by telephone, mail, or the Internet.

Chaptered by Secretary of State. Chapter No.376: OCTOBER 1, 2001;

California S.B. 412

Criminalizes the act of political cyberfraud with intent to mislead, deceive or defraud.

Defines political cyberfraud as an act concerning a political website. Provides these provisions do not apply to a domain registrar, registry or registration authority. Makes a violation punishable by a fine. Allows courts to transfer a domain name as part of the relief awarded

Connecticut State Laws:

GENERAL STATUTES OF CONNECTICUT

TITLE 53A. PENAL CODE

CHAPTER 952. PENAL CODE: OFFENSES

PART XXII. COMPUTER-RELATED OFFENSES

Conn. Gen. Stat. @ 53a-250 (1989)

Sec. 53a-250. Definitions.

For the purposes of this part and section 52-570b:

- (1) "Access" means to instruct, communicate with, store data in or retrieve data from a computer, computer system or computer network.
- (2) "Computer" means a programmable, electronic device capable of accepting and processing data.
- (3) "Computer network" means (A) a set of related devices connected to a computer by communications facilities, or (B) a complex of two or more computers, including related devices, connected by communications facilities.
- (4) "Computer program" means a set of instructions, statements or related data that, in actual or modified form, is capable of causing a computer or computer system to perform specified functions.
- (5) "Computer services" includes, but is not limited to, computer access, data processing and data storage.
- (6) "Computer software" means one or more computer programs, existing in any form, or any associated operational procedures, manuals or other documentation.
- (7) "Computer system" means a computer, its software, related equipment, communications facilities, if any, and includes computer networks.
- (8) "Data" means information of any kind in any form, including computer software.
- (9) "Person" means a natural person, corporation, trust, partnership, incorporated or unincorporated association and any other legal or governmental entity, including any state or municipal entity or public official.
- (10) "Private personal data" means data concerning a natural person which a reasonable person would want to keep private and which is protectable under law.
- (11) "Property" means anything of value, including data.

Sec. 53a-251. Computer crime.

(a) Defined. A person commits computer crime when he violates any of the provisions of this section.

(b) Unauthorized access to a computer system.

- (1) A person is guilty of the computer crime of unauthorized access to a computer system when, knowing that he is not authorized to do so, he accesses or causes to be accessed any computer system without authorization.
- (2) It shall be an affirmative defense to a prosecution for unauthorized access to a computer system that: (A) The person reasonably believed that the owner of the computer system, or a person empowered to license access thereto, had authorized him to access; (B) the person reasonably believed that the owner of the computer system, or a person empowered to license access thereto, would have authorized him to access without payment of any consideration; or (C) the person reasonably could not have known that his access was unauthorized.

(c) Theft of computer services. A person is guilty of the computer crime of theft of computer services when he accesses or causes to be accessed or otherwise uses or causes to be used a computer system with the intent to obtain unauthorized computer services.

(d) Interruption of computer services. A person is guilty of the computer crime of interruption of computer services when he, without authorization, intentionally or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user of a computer system.

(e) Misuse of computer system information. A person is guilty of the computer crime of misuse of computer system information when: (1) As a result of his accessing or causing to be accessed a computer system, he intentionally makes or causes to be made an unauthorized display, use, disclosure or copy, in any form, of data residing in, communicated by or produced by a computer system; or (2) he intentionally or recklessly and without authorization (A) alters, deletes, tampers with, damages, destroys or takes data intended for use by a computer system, whether residing within or external to a computer system, or (B) intercepts or adds data to data residing within a computer system; or (3) he knowingly receives or retains data obtained in violation of subdivision (1) or (2) of this subsection; or (4) he uses or discloses any data he knows or believes was obtained in violation of subdivision (1) or (2) of this subsection.

(f) Destruction of computer equipment. A person is guilty of the computer crime of destruction of computer equipment when he, without authorization, intentionally or recklessly tampers with, takes, transfers, conceals, alters, damages or destroys any equipment used in a computer system or intentionally or recklessly causes any of the foregoing to occur.

Sec. 53a-252. Computer crime in the first degree: Class B felony.

(a) A person is guilty of computer crime in the first degree when he commits computer crime as defined in section 53a-251 and the damage to or the value of the property or computer services exceeds ten thousand dollars.

(b) Computer crime in the first degree is a class B felony.

Sec. 53a-253. Computer crime in the second degree: Class C felony.

(a) A person is guilty of computer crime in the second degree when he commits computer crime as defined in section 53a-251 and the damage to or the value of the property or computer services exceeds five thousand dollars.

(b) Computer crime in the second degree is a class C felony.

Sec. 53a-254. Computer crime in the third degree: Class D felony.

(a) A person is guilty of computer crime in the third degree when he commits computer crime as defined in section 53a-251 and (1) the damage to or the value of the property or computer services exceeds one thousand dollars or (2) he recklessly engages in conduct which creates a risk of serious physical injury to another person.

(b) Computer crime in the third degree is a class D felony.

Sec. 53a-255. Computer crime in the fourth degree: Class A misdemeanor.

(a) A person is guilty of computer crime in the fourth degree when he commits computer crime as defined in section 53a-251 and the damage to or the value of the property or computer services exceeds five hundred dollars.

(b) Computer crime in the fourth degree is a class A misdemeanor.

Sec. 53a-256. Computer crime in the fifth degree: Class B misdemeanor.

(a) A person is guilty of computer crime in the fifth degree when he commits computer crime as defined in section 53a-251 and the damage to or the value of the property or computer services, if any, is five hundred dollars or less.

(b) Computer crime in the fifth degree is a class B misdemeanor.

Sec. 53a-257. Alternative fine based on defendant's gain.

If a person has gained money, property or services or other consideration through the commission of any offense under section 53a-251, upon conviction thereof the court, in lieu of imposing a fine, may sentence the defendant to pay an amount, fixed by the court, not to exceed double the amount of the defendant's gain from the commission of such offense. In such case the court shall make a finding as to the amount of the

defendant's gain from the offense and, if the record does not contain sufficient evidence to support such a finding, the court may conduct a hearing upon the issue. For the purpose of this section, "gain" means the amount of money or the value of property or computer services or other consideration derived.

Sec. 53a-258. Determination of degree of crime.

Amounts included in violations of section 53a-251 committed pursuant to one scheme or course of conduct, whether from the same person or several persons, may be aggregated in determining the degree of the crime.

Sec. 53a-259. Value of property or computer services.

(a) For the purposes of this part and section 52-570b, the value of property or computer services shall be: (1) The market value of the property or computer services at the time of the violation; or (2) if the property or computer services are unrecoverable, damaged or destroyed as a result of a violation of section 53a-251, the cost of reproducing or replacing the property or computer services at the time of the violation.

(b) When the value of the property or computer services or damage thereto cannot be satisfactorily ascertained, the value shall be deemed to be two hundred fifty dollars.

(c) Notwithstanding the provisions of this section, the value of private personal data shall be deemed to be one thousand five hundred dollars.

Sec. 53a-260. Location of offense.

(a) In any prosecution for a violation of section 53a-251, the offense shall be deemed to have been committed in the town in which the act occurred or in which the computer system or part thereof involved in the violation was located.

(b) In any prosecution for a violation of section 53a-251 based upon more than one act in violation thereof, the offense shall be deemed to have been committed in any of the towns in which any of the acts occurred or in which a computer system or part thereof involved in a violation was located.

Sec. 53a-261. Jurisdiction.

If any act performed in furtherance of the offenses set out in section 53a-251 occurs in this state or if any computer system or part thereof accessed in violation of section 53a-251 is located in this state, the offense shall be deemed to have occurred in this state.

Sec. 52-570b. Action for computer-related offenses.

(a) Any aggrieved person who has reason to believe that any other person has been engaged, is engaged or is about to engage in an alleged violation of any provision of section 53a-251 may bring an action against such person and may apply to the superior court for: (1) An order temporarily or permanently restraining and enjoining the

commencement or continuance of such act or acts; (2) an order directing restitution; or (3) an order directing the appointment of a receiver. Subject to making due provisions for the rights of innocent persons, a receiver shall have the power to sue for, collect, receive and take into his possession any property which belongs to the person who is alleged to have violated any provision of section 53a-251 and which may have been derived by, been used in or aided in any manner such alleged violation. Such property shall include goods and chattels, rights and credits, moneys and effects, books, records, documents, papers, choses in action, bills, notes and property of every description including all computer system equipment and data, and including property with which such property has been commingled if it cannot be identified in kind because of such commingling. The receiver shall also have the power to sell, convey and assign all of the foregoing and hold and dispose of the proceeds thereof under the direction of the court. Any person who has suffered damages as a result of an alleged violation of any provision of section 53a-251, and submits proof to the satisfaction of the court that he has in fact been damaged, may participate with general creditors in the distribution of the assets to the extent he has sustained out-of-pocket losses. The court shall have jurisdiction of all questions arising in such proceedings and may make such orders and judgments therein as may be required.

(b) The court may award the relief applied for or such other relief as it may deem appropriate in equity.

(c) Independent of or in conjunction with an action under subsection (a) of this section, any person who suffers any injury to person, business or property may bring an action for damages against a person who is alleged to have violated any provision of section 53a-251. The aggrieved person shall recover actual damages and damages for unjust enrichment not taken into account in computing damages for actual loss, and treble damages where there has been a showing of willful and malicious conduct.

(d) Proof of pecuniary loss is not required to establish actual damages in connection with an alleged violation of subsection (e) of section 53a-251 arising from misuse of private personal data.

(e) In any civil action brought under this section, the court shall award to any aggrieved person who prevails, reasonable costs and reasonable attorney's fees.

(f) The filing of a criminal action against a person is not a prerequisite to the bringing of a civil action under this section against such person.

(g) A civil action may be brought under this section against the state or any political subdivision thereof and the defense of governmental immunity shall not be available in any such action. The rights and liability of the state or any political subdivision thereof in each such action shall be coextensive with and shall equal the rights and liability of private persons in like circumstances.

(h) No civil action under this section may be brought but within three years from the date the alleged violation of section 53a-251 is discovered or should have been discovered by the exercise of reasonable diligence.

Florida State Laws:

FLORIDA

TITLE XLVI CRIMES

CHAPTER 815 COMPUTER-RELATED CRIMES

815.01 Short title.

The provisions of this act shall be known and may be cited as the "Florida Computer Crimes Act."

815.02 Legislative intent.

The Legislature finds and declares that:

- (1) Computer-related crime is a growing problem in government as well as in the private sector.
- (2) Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime.
- (3) The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great.
- (4) While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.

815.03 Definitions.

As used in this chapter, unless the context clearly indicates otherwise:

- (1) "Intellectual property" means data, including programs.
- (2) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data.
- (3) "Computer" means an internally programmed, automatic device that performs data processing.
- (4) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

- (5) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, or computer software.
- (6) "Computer network" means a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities.
- (7) "Computer system services" means providing a computer system or computer network to perform useful work.
- (8) "Property" means anything of value as defined in n1 s. 812.011 and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine-readable or human-readable form, and any other tangible or intangible item of value.
- (9) "Financial instrument" means any check, draft, money order, certificate of deposit letter of credit, bill of exchange, credit card, or marketable security.
- (10) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

815.04 Offenses against intellectual property; public records exemption.

- (1) Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.
- (2) Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.
- (3) (a) Data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 which resides or exists internal or external to a computer, computer system, or computer network which is held by an agency as defined in chapter 119 is confidential and exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This exemption is subject to the Open Government Sunset Review Act in accordance with s. 119.14.
(b) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.
- (4) (a) Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.
(b) If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

815.05 Offenses against computer equipment or supplies.

- (1) (a) Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits an offense against computer equipment or supplies.
(b) 1. Except as provided in this paragraph, an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.
2. If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.
- (2) (a) Whoever willfully, knowingly, and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization destroys, injures, or damages any computer, computer system, or computer network commits an offense against computer equipment or supplies.
(b) 1. Except as provided in this paragraph, an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.
2. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is greater than \$ 200 but less than \$ 1,000, then the offender is guilty of a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.
3. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is \$ 1,000 or greater, or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service, then the offender is guilty of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

815.06 Offenses against computer users.

- (1) Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users.
- (2) (a) Except as provided in this subsection, an offense against computer users is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.
(b) If the offense is committed for the purposes of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty

of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

815.07 This chapter not exclusive.

The provisions of this chapter shall not be construed to preclude the applicability of any other provision of the criminal law of this state which presently applies or may in the future apply to any transaction which violates this chapter, unless such provision is inconsistent with the terms of this chapter.

Florida S.B. 1282

Provides criminal penalties for using the Internet in dealing in stolen property

Iowa State Laws:

TITLE XXXV CRIMINAL LAW CHAPTER 716A COMPUTER CRIME Iowa Code @ 716A.1 (1989)

716A.1 Definitions

As used in this chapter, unless the context otherwise requires:

1. "Access" means to instruct, communicate with, store data in, or retrieve data from a computer, computer system, or computer network.
2. "Computer" means an electronic device which performs logical, arithmetical, and memory functions by manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, computer software, and communication facilities which are connected or related to the computer in a computer system or computer network.
3. "Computer system" means related, connected or unconnected, computers or peripheral equipment.
4. "Computer network" means a set of related, remotely connected devices and communication facilities including two or more computers with capability to transmit data among them through communication facilities.
5. "Computer program" means an ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.
6. "Computer software" means a set of computer programs, procedures, or associated documentation used in the operation of a computer.
7. "Data" means a representation of information, knowledge, facts, concepts or instructions that has been prepared or is being prepared in a formalized manner and has been processed, or is intended to be processed in a computer. Data may be in any form including, but not limited to, printouts, magnetic storage media, punched cards and as stored in the memory of a computer.
8. "Property" means anything of value as defined in section 702.14, including but not limited to computers and computer data, information, software, and programs.
9. "Services" means the use of a computer, computer system, or computer network and includes, but is not limited to, computer time, data processing, and storage functions.
10. "Loss of property" means the greatest of the following:
 - a. The retail value of the property involved.
 - b. The reasonable replacement or repair cost, whichever is less.
11. "Loss of services" means the reasonable value of the damage created by the unavailability or lack of utility of the property or services involved until repair or replacement can be effected.

716A.2 Unauthorized access

A person who knowingly and without authorization accesses a computer, computer system, or computer network commits a simple misdemeanor.

716A.3 Computer damage defined

A person commits computer damage when the person knowingly and without authorization damages or destroys a computer, computer system, computer network, computer software, computer program, or any other property as defined in section 716A.1, subsection 8, or knowingly and without authorization and with the intent to injure or defraud alters any computer, computer system, computer network, computer software, computer program, or any other property as defined in section 716A.1, subsection 8.

716A.4 Computer damage in the first degree

Computer damage is computer damage in the first degree when the damage results in a loss of property or services of more than five thousand dollars. Computer damage in the first degree is a class "C" felony.

716A.5 Computer damage in the second degree

Computer damage is computer damage in the second degree when the damage results in a loss of property or services of more than five hundred dollars but not more than five thousand dollars. Computer damage in the second degree is a class "D" felony.

716A.6 Computer damage in the third degree

Computer damage is computer damage in the third degree when the damage results in a loss of property or services of more than one hundred dollars but not more than five hundred dollars. Computer damage in the third degree is an aggravated misdemeanor.

716A.7 Computer damage in the fourth degree

Computer damage is computer damage in the fourth degree when the damage results in a loss of property or services of more than fifty dollars but not more than one hundred dollars. Computer damage in the fourth degree is a serious misdemeanor.

716A.8 Computer damage in the fifth degree

Computer damage is computer damage in the fifth degree when the damage results in a loss of property or services of not more than fifty dollars. Computer damage in the fifth degree is a simple misdemeanor.

716A.9 Computer theft defined

A person commits computer theft when the person knowingly and without authorization accesses or causes to be accessed a computer, computer system, or computer network, or any part thereof, for the purpose of obtaining services, information or property or knowingly and without authorization and with the intent to permanently deprive the owner of possession, takes, transfers, conceals or retains possession of a computer, computer system, or computer network or any computer software or program, or data contained in a computer, computer system, or computer network.

716A.10 Computer theft in the first degree

Computer theft is computer theft in the first degree when the theft involves or results in a loss of services or property of more than five thousand dollars. Computer theft in the first degree is a class "C" felony.

716A.11 Computer theft in the second degree

Computer theft is computer theft in the second degree when the theft involves or results in a loss of services or property of more than five hundred dollars but not more than five thousand dollars. Computer theft in the second degree is a class "D" felony.

716A.12 Computer theft in the third degree

Computer theft is computer theft in the third degree when the theft involves or results in a loss of services or property of more than one hundred dollars but not more than five hundred dollars. Computer theft in the third degree is an aggravated misdemeanor.

716A.13 Computer theft in the fourth degree

Computer theft is computer theft in the fourth degree when the theft involves or results in a loss of services or property of more than fifty dollars but not more than one hundred dollars. Computer theft in the fourth degree is a serious misdemeanor.

716A.14 Computer theft in the fifth degree

Computer theft is computer theft in the fifth degree when the theft involves or results in a loss of services or property of not more than fifty dollars. Computer theft in the fifth degree is a simple misdemeanor.

716A.15 Chapter not exclusive

This chapter does not preclude the applicability of any other provision of the law of this state which is not inconsistent with this chapter and which applies or may apply to an act or transaction in violation of this chapter.

716A.16 Printouts admissible as evidence

In a prosecution under this chapter, computer printouts shall be admitted as evidence of any computer software, program, or data contained in or taken from a computer, notwithstanding an applicable rule of evidence to the contrary.

Maryland State Laws:

Maryland Ann. Code Art. 27

45A. False entry in public record; altering, defacing, destroying, removing or concealing public record; accessing public records

- (a) For the purposes of this section, the following words have the meanings indicated.
 - (1) "Public record" includes all official books, papers, or records whether kept on a manual or automated basis, which are created, received, or used by the State or any agency thereof, a bicounty or a multicounty agency, any county, municipality, or other political subdivision.
 - (2) "Access" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of equipment including, but not limited to, computers and other data processing equipment or resources connected therewith.
- (b) It is unlawful for a person to do or attempt to do the following:
 - (1) Wilfully make a false entry in any public records;
 - (2) Except under proper authority, wilfully alter, deface, destroy, remove, or conceal any public record; or
 - (3) Except under proper authority, wilfully and intentionally access public records.
- (c) Any person who violates this section is guilty of a misdemeanor and may be imprisoned up to 3 years or fined up to \$1,000, or both.

146. Unauthorized access to computers prohibited

- (a) Definitions. -- In this section the following words have the meanings indicated.
 - (1) (i) "Computer" means an electronic, magnetic, optical, organic, or other data processing device or system that performs logical, arithmetic, memory, or storage functions.
 - (ii) "Computer" includes any property, data storage facility, or communications facility that is directly related to or operated in conjunction with that device or system.
 - (iii) "Computer" does not include an automated typewriter or typesetter, or a portable calculator.
- (2) "Computer control language" means any ordered statements that direct a computer to perform specific functions.
- (3) "Computer data base" means a representation of information, knowledge, facts, concepts, or instructions that:
 - (i) Are being prepared or have been prepared in a formalized manner or are or have been produced by a computer, computer system, or computer network; and
 - (ii) Are intended for use in a computer, computer system, or computer network.

- (4) "Computer network" means the interconnection of 1 or more computers through:
 - (i) The use of satellite, microwave, line, or other communication media; and
 - (ii) Terminals or a complex consisting of 2 or more interconnected computers whether or not the interconnection is continuously maintained.
- (5) "Computer program" means an ordered set of instructions or statements that may interact with related data that, when executed in a computer system, causes the computer to perform specified functions.
- (6) "Computer services" includes, but is not limited to, computer time, data processing, and storage functions.
- (7) "Computer software" means computer programs, instructions, procedures, or associated documentation that is concerned with the operation of a computer system.
- (8) "Computer system" means 1 or more connected or unconnected computers, peripheral devices, software, data, or programs.
- (9) "Access" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of equipment including, but not limited to, computers and other data processing equipment or resources connected therewith.

(b) Other applicable Code provisions. -- This section does not preclude the applicability of any other provision of this Code.

(c) Illegal access. --

- (1) A person may not intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services.
- (2) A person may not intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services to
 - (i) Cause the malfunction or interrupt the operation of a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services; or
 - (ii) Alter, damage, or destroy data or a computer program stored, maintained, or produced by a computer, computer network, computer system, computer services, computer data base, or any part of these systems or services.
- (3) A person may not intentionally, willfully, and without authorization:
 - (i) Identify or attempt to identify any valid access codes; or
 - (ii) Distribute or publicize any valid access codes to any unauthorized person.

(d) Penalty. --

- (1) Any person who violates any provision of subsection (c) (1) of this section is guilty of a misdemeanor and on conviction is subject to a fine not exceeding \$1,000 or imprisonment not exceeding 3 years or both.
- (2) (i) Any person who violates any provision of subsection (c) (2) or (c) (3) of this section where the aggregate amount of the loss is less than \$10,000 is guilty of a misdemeanor and on conviction is subject to a fine not exceeding \$5,000 or imprisonment not exceeding 5 years or both.
(ii) Any person who violates any provision of subsection (c) (2) or (c) (3) of this section where the aggregate amount of the loss is \$10,000 or greater is guilty of a felony and on conviction is subject to a fine not exceeding \$10,000 or imprisonment not exceeding 10 years or both.

(e) Scope of offenses; jurisdiction. --

- (1) When illegal access to a computer, computer network, computer control language, computer system, computer services, computer software, computer data base, or any part of these systems or services is committed in violation of this section pursuant to 1 scheme or continuing course of conduct, the conduct may be considered as 1 offense.
- (2) A court of competent jurisdiction in this State may try a person who allegedly violates any provision of subsection (c) of this section in any county in this State where:
 - (i) The person performs the act; or
 - (ii) The accessed computer is located.

Massachusetts State Laws:

SECTION 1. Chapter 266 of the General Laws is hereby amended by inserting after section 37D the following section:-

Section 37E. (a) For purposes of this section, the following words shall have the following meanings:-

"Harass", willfully and maliciously engage in an act directed at a specific person or persons, which act seriously alarms or annoys such person or persons and would cause a reasonable person to suffer substantial emotional distress.

"Personal identifying information", any name or number that may be used, alone or in conjunction with any other information, to assume the identity of an individual, including any name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, credit card number or computer password identification.

"Pose", to falsely represent oneself, directly or indirectly, as another person or persons.

"Victim", any person who has suffered financial loss or any entity that provided money, credit, goods, services or anything of value and has suffered financial loss as a direct result of the commission or attempted commission of a violation of this section.

(b) Whoever, with intent to defraud, poses as another person without the express authorization of that person and uses such person's personal identifying information to obtain or to attempt to obtain money, credit, goods, services, anything of value, any identification card or other evidence of such person's identity, or to harass another shall be guilty of identity fraud and shall be punished by a fine of not more than \$5,000 or imprisonment in a house of correction for not more than two and one-half years, or by both such fine and imprisonment.

(c) Whoever, with intent to defraud, obtains personal identifying information about another person without the express authorization of such person, with the intent to pose as such person or who obtains personal identifying information about a person without the express authorization of such person in order to assist another to pose as such person in order to obtain money, credit, goods, services, anything of value, any identification card or other evidence of such person's identity, or to harass another shall be guilty of the crime of identity fraud and shall be punished by a fine of not more than \$5,000 or imprisonment in a house of correction for not more than two and one-half years, or by both such fine and imprisonment.

(d) A person found guilty of violating any provisions of this section shall, in addition to any other punishment, be ordered to make restitution for financial loss sustained by a victim as a result of such violation. Financial loss may include any costs incurred by such

victim in correcting the credit history of such victim or any costs incurred in connection with any civil or administrative proceeding to satisfy any debt or other obligation of such victim, including lost wages and attorney's fees.

Chapter 266: Section 30 Larceny; general provisions and penalties

Section 30. (1) Whoever steals, or with intent to defraud obtains by a false pretence, or whoever unlawfully, and with intent to steal or embezzle, converts, or secretes with intent to convert, the property of another as defined in this section, whether such property is or is not in his possession at the time of such conversion or secreting, shall be guilty of larceny, and shall, if the property stolen is a firearm, as defined in section one hundred and twenty-one of chapter one hundred and forty, or, if the value of the property stolen exceeds two hundred and fifty dollars, be punished by imprisonment in the state prison for not more than five years, or by a fine of not more than twenty-five thousand dollars and imprisonment in jail for not more than two years; or, if the value of the property stolen, other than a firearm as so defined, does not exceed two hundred and fifty dollars, shall be punished by imprisonment in jail for not more than one year or by a fine of not more than three hundred dollars; or, if the property was stolen from the conveyance of a common carrier or of a person carrying on an express business, shall be punished for the first offence by imprisonment for not less than six months nor more than two and one half years, or by a fine of not less than fifty nor more than six hundred dollars, or both, and for a subsequent offence, by imprisonment for not less than eighteen months nor more than two and one half years, or by a fine of not less than one hundred and fifty nor more than six hundred dollars, or both.

(2) The term "property", as used in the section, shall include money, personal chattels, a bank note, bond, promissory note, bill of exchange or other bill, order or certificate, a book of accounts for or concerning money or goods due or to become due or to be delivered, a deed or writing containing a conveyance of land, any valuable contract in force, a receipt, release or defeasance, a writ, process, certificate of title or duplicate certificate issued under chapter one hundred and eighty-five, a public record, anything which is of the realty or is annexed thereto, a security deposit received pursuant to section fifteen B of chapter one hundred and eighty-six, electronically processed or stored data, either tangible or intangible, data while in transit, telecommunications services, and any domesticated animal, including dogs, or a beast or bird which is ordinarily kept in confinement.

(3) The stealing of real property may be a larceny from one or more tenants, sole, joint or in common, in fee, for life or years, at will or sufferance, mortgagors or mortgagees, in possession of the same, or who may have an action of tort against the offender for trespass upon the property, but not from one having only the use or custody thereof. The larceny may be from a wife in possession, if she is authorized by law to hold such property as if sole, otherwise her occupation may be the possession of the husband. If such property which was of a person deceased is stolen, it may be a larceny from any one or more heirs, devisees, reversioners, remaindermen or others, who have a right upon such deceased to take possession, but not having entered, as it would be after entry. The

larceny may be from a person whose name is unknown, if it would be such if the property stolen were personal, and may be committed by those who have only the use or custody of the property, but not by a person against whom no action of tort could be maintained for acts like those constituting the larceny.

(4) Whoever steals, or with intent to defraud obtains by a false pretense, or whoever unlawfully, and with intent to steal or embezzle, converts, secretes, unlawfully takes, carries away, conceals or copies with intent to convert any trade secret of another, regardless of value, whether such trade secret is or is not in his possession at the time of such conversion or secreting, shall be guilty of larceny, and shall be punished by imprisonment in the state prison for not more than five years, or by a fine of not more than twenty-five thousand dollars and imprisonment in jail for not more than two years. The term "trade secret" as used in this paragraph means and includes anything tangible or intangible or electronically kept or stored, which constitutes, represents, evidences or records a secret scientific, technical, merchandising, production or management information, design, process, procedure, formula, invention or improvement.

(5) Whoever steals or with intent to defraud obtains by a false pretense, or whoever unlawfully, and with intent to steal or embezzle, converts, or secretes with intent to convert, the property of another, sixty years of age or older, or of a person with a disability as defined in section thirteen K of chapter two hundred and sixty-five, whether such property is or is not in his possession at the time of such conversion or secreting, shall be guilty of larceny, and shall, if the value of the property exceeds two hundred and fifty dollars, be punished by imprisonment in the state prison for not more than ten years or in the house of correction for not more than two and one-half years, or by a fine of not more than fifty thousand dollars or by both such fine and imprisonment; or if the value of the property does not exceed two hundred and fifty dollars, shall be punished by imprisonment in the house of correction for not more than two and one-half years or by a fine of not more than one thousand dollars or by both such fine and imprisonment. The court may order, regardless of the value of the property, restitution to be paid to the victim commensurate with the value of the property.

Section 33A. Fraudulent Obtaining of Commercial Computer Service; Penalty.

Whoever, with intent to defraud, obtains, or attempts to obtain, or aids or abets another in obtaining, any commercial computer service by any false representation, false statement, unauthorized charging to the account of another, by installing or tampering with any facilities or equipment or by any other means, shall be punished by imprisonment in the house of correction for not more than two and one-half years or by a fine of not more than three thousand dollars, or both. As used in this section, the words "commercial computer service" mean the use of computers, computer systems, computer programs or computer networks, or the access to or copying of the data, where such use, access or copying is offered by the proprietor or operator of the computer, system, program, network or data to others on a subscription or other basis for monetary consideration.

Chapter 266: Section 60A Stolen trade secrets; buying or selling

Section 60A. Whoever buys, receives, conceals, stores, barter, sells or disposes of any trade secret, or pledges or accepts as security for a loan any trade secret, regardless of value, knowing the same to have been stolen, unlawfully converted, or taken, shall be punished by imprisonment for not more than five years or by a fine of not more than five hundred dollars and imprisonment in jail for not more than two years. The term "trade secret" as used in this section shall have the same meaning as is set forth in section thirty.

Section 79K. Admissibility of Duplicate of Computer Data File or Program File.

A duplicate of a computer data file or program file is admissible in evidence as the original itself unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original. For purposes of this section, if data stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, shall be an original. A "duplicate of a computer data file or program file" shall mean a file produced by the same impression as the original, or from the same matrix, or by mechanical or electronic recording, in the normal way such a duplicate is produced on a computer, or by other equivalent techniques that accurately reproduce the original.

Section 120F. Unauthorized Accessing of Computer Systems; Penalty; Password Requirement as Notice.

Whoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access, shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both. The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.

New York State Laws:

New York Penal Law, Computer Crime, Section 156.00. This act became effective in 1986.

Section 156.00 Offenses involving computers; definitions of terms

The following definitions are applicable to this chapter except where different meanings are expressly specified:

1. "Computer" means a device or group of devices which, by manipulation of electronic, magnetic, optical or electrochemical impulses, pursuant to a computer program, can automatically perform arithmetic, logical, storage or retrieval operations with or on computer data, and includes any connected or directly related device, equipment or facility which enables such computer to store, retrieve or communicate to or from a person, another computer or another device the results of computer operations, computer programs or computer data.
2. "Computer program" is property and means an ordered set of data representing coded instructions or statements that, when executed by computer, cause the computer to process data or direct the computer to perform one or more computer operations or both and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of the computer.
3. "Computer data" is property and means a representation of information, knowledge, facts, concepts or instructions which are being processed, or have been processed in a computer and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of the computer.
4. "Computer service" means any and all services provided by or through the facilities of any computer communications system allowing the input, output, examination, or transfer, of computer data or computer programs from one computer to another.
5. "Computer material" is property and means any computer data or computer program which:
 - a. contains records of the medical history or medical treatment of an identified or readily identifiable individual or individuals. This term shall not apply to the gaining access to or duplication solely of the medical history or medical treatment records of a person by that person or by another specifically authorized by the person who records are gained access to or duplicated; or
 - b. contains records maintained by the state or any political subdivision thereof or any governmental instrumentality within the state which contains any information concerning a person, as defined in subdivision seven of section 10.00 of this chapter, which because of

- name, number, symbol, mark or other identifier, can be used to identify the person and which is otherwise prohibited by law from being disclosed. This term shall not apply to the gaining access to or duplication solely of records of a person by that person or by another specifically authorized by the person whose records are gained access to or duplicated; or
- c. is not and is not intended to be available to anyone other than the person or person rightfully in possession thereof or selected person having access thereto with his or their consent and which accords or may accord such rightful possessors an advantage over competitors an advantage over competitors or other person who do not have knowledge or the benefit thereof.
6. "Uses a computer or computer service without authorization" means the use of a computer or computer service without the permission of, or in excess of the permission of, the owner or lessor or someone licensed or privileged by the owner or lessor after notice to that effect to the user of the computer or computer service has been given by:
- a. giving actual notice in writing or orally to the user; or
 - b. prominently posting written notice adjacent to the computer being utilized by the user; or
 - c. a notice that is displayed on, printed out on or announced by the computer being utilized by the user. Proof that the computer is programmed to automatically display, print or announce such notice or a notice prohibiting copying, reproduction or duplication shall be presumptive evidence that such notice was displayed.

7. "Felony" as used in this article means any felony defined in the laws of this state or any offense defined in the laws of any other jurisdiction for which a sentence to imprisonment in excess of one year is authorized in this state.

Section 156.05. Unauthorized use of a computer

A person is guilty of unauthorized use of a computer when he knowingly uses or causes to be used a computer or computer service without authorization and the computer utilized is equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of said computer or computer system.

Unauthorized use of a computer is a class A misdemeanor.

Section 156.10. Computer trespass

A person is guilty of computer trespass when he knowingly uses or caused to be used a computer or computer service without authorization and:

- 1. he does so with an intent to commit or attempt to commit or further the commission of any felony; or

2. he thereby knowingly gains access to computer material.

Computer trespass is a class E felony.

Section 156.20. Computer tampering in the second degree

A person is guilty of computer tampering in the second degree when he uses or causes to be used a computer or computer service and having no right to do so he intentionally alters in any manner or destroys computer data or a computer program of another person.

Computer tampering in the second degree is a class A misdemeanor.

Section. 156.25. Computer tampering in the first degree

A person is guilty of computer tampering in the first degree when he commits the crime of computer tampering in the second degree and:

1. he does so with an intent to commit or attempt to commit or further the commission of any felony; or
2. he has been previously convicted of any crime under this article or subdivision ten of section 165.15 of this chapter; or
3. he intentionally alters in any manner or destroys computer material; or
4. he intentionally alters in any manner or destroys computer data or a computer program in an amount exceeding one thousand dollars.

Computer tampering in the first degree is a class E felony.

Section 156.30. Unlawful duplication of computer related material

A person is guilty of unlawful duplication of computer related material when having no right to do so, he copies, reproduces or duplicates in any manner:

1. any computer data or computer program and thereby intentionally and wrongfully deprives or appropriates from an owner thereof an economic value or benefit in excess of two thousand five hundred dollars; or
2. any computer data or computer program with an intent to commit or attempt to commit or further the commission of any felony.

Unlawful duplication of computer related material is a class E felony.

Section 156.35 Criminal possession of computer related material

A person is guilty of criminal possession of computer related material when having no right to do so, he knowingly possesses, in any form, any copy, reproduction or duplicate of any computer data or computer program which was copied, reproduced or duplicated in violation of section 156.30 of this article, with intent to benefit himself or a person other than an owner thereof.

Criminal possession of computer related material is a class E felony.

Section 156.50 Offenses involving computers; defenses

In any prosecution:

1. under section 156.05 or 156.10 of this article, it shall be a defense that the defendant had reasonable grounds to believe that he had authorization to use the computer;
2. under section 156.20 or 156.25 of this article it shall be a defense that the defendant had reasonable grounds to believe that he had the right to alter in any manner or destroy the computer data or the computer program;
3. under section 156.30 of this article it shall be a defense that the defendant had reasonable grounds to believe that he had the right to copy, reproduce or duplicate in any manner the computer data or the computer program.

Texas State Laws:**TPC Title 7 Chapter 33.01 Computer Crimes**

In this chapter:

Definitions.

- (1) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer system, or computer network.
- (2) "Communications common carrier" means a person who owns or operates a telephone system in this state that includes equipment or facilities for the conveyance, transmission, or reception of communications and who receives compensation from persons who use that system.
- (3) "Computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.
- (4) "Computer network" means the interconnection of two or more computers or computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers.
- (5) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data or perform specific functions.
- (6) "Computer security system" means the design, procedures, or other measures that the person responsible for the operation and use of a computer employs to restrict the use of the computer to particular persons or uses or that the owner or licensee of data stored or maintained by a computer in which the owner or licensee is entitled to store or maintain the data employs to restrict access to the data.
- (7) "Computer services" means the product of the use of a computer, the information stored in the computer, or the personnel supporting the computer, including computer time, data processing, and storage functions.
- (8) "Computer system" means any combination of a computer or computer network with the documentation, computer software, or physical facilities supporting the computer or computer network.
- (9) "Computer software" means a set of computer programs, procedures, and associated documentation related to the operation of a computer, computer system, or computer network.

(10) "Computer virus" means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

(11) "Data" means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, laser storage media, and punch cards, or may be stored internally in the memory of the computer.

(12) "Effective consent" includes consent by a person legally authorized to act for the owner. Consent is not effective if:

- (A) induced by deception, as defined by Section 31.01, or induced by coercion;
- (B) given by a person the actor knows is not legally authorized to act for the owner;
- (C) given by a person who by reason of youth, mental disease or defect, or intoxication is known by the actor to be unable to make reasonable property dispositions;
- (D) given solely to detect the commission of an offense; or
- (E) used for a purpose other than that for which the consent was given.

(13) "Electric utility" has the meaning assigned by Subsection (c), Section 3, Public Utility Regulatory Act (Article 1446c, Vernon's Texas Civil Statutes).

(14) "Harm" includes partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a computer virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.

(15) "Owner" means a person who:

- (A) has title to the property, possession of the property, whether lawful or not, or a greater right to possession of the property than the actor;
- (B) has the right to restrict access to the property; or
- (C) is the licensee of data or computer software.

(16) "Property" means:

- (A) tangible or intangible personal property including a computer, computer system, computer network, computer software, or data; or
- (B) the use of a computer, computer system, computer network, computer software, or data.

33.02. Breach of Computer Security

(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

(b) A person commits an offense if the person intentionally or knowingly gives a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the effective consent of the person employing the computer security system to restrict access to a computer, computer network, computer system, or data.

(c) An offense under this section is a Class A misdemeanor unless the actor's intent is to obtain a benefit or defraud or harm another, in which event the offense is:

- (1) a state jail felony if the value of the benefit or the amount of the loss or harm is less than \$20,000; or
- (2) a felony of the third degree if the value of the benefit or the amount of the loss or harm is \$20,000 or more.

(d) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

33.03. Defenses

It is an affirmative defense to prosecution under Section 33.02 that the actor was an officer, employee, or agent of a communications common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the communications common carrier or electric utility.

33.04. Assistance by Attorney General

The attorney general, if requested to do so by a prosecuting attorney, may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or of any other offense involving the use of a computer.

Virginia State Laws
Title 18.2 Chapter 5 Article 7.1

VIRGINIA CODE
TITLE 18.2. CRIMES AND OFFENSES GENERALLY
CHAPTER 5. CRIMES AGAINST PROPERTY
ARTICLE 7.1. COMPUTER CRIMES
SECTIONS 18.2-152.2, 152.3:1, 152.4, 152.12 & 152.16 (2003)
(including amendments by Acts 2003, ch. 987 & 1016, approved April 3, 2003)

§ 18.2-152.2. Definitions.

For purposes of this article:

"Computer" means an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term "computer" includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device.

"Computer data" means any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or computer network. "Computer data" may be in any form, whether readable only by a computer or only by a human or by either, including, but not limited to, computer printouts, magnetic storage media, punched cards, or stored internally in the memory of the computer.

"Computer network" means two or more computers connected by a network.

"Computer operation" means arithmetic, logical, monitoring, storage or retrieval functions and any combination thereof, and includes, but is not limited to, communication with, storage of data to, or retrieval of data from any device or human hand manipulation of electronic or magnetic impulses. A "computer operation" for a particular computer may also be any function for which that computer was generally designed.

"Computer program" means an ordered set of data representing coded instructions or statements that, when executed by a computer, causes the computer to perform one or more computer operations.

"Computer services" means computer time or services, including data processing services, Internet services, electronic mail services, electronic message services, or information or data stored in connection therewith.

"Computer software" means a set of computer programs, procedures and associated documentation concerned with computer data or with the operation of a computer, computer program, or computer network.

"Electronic mail service provider" means any person who (i) is an intermediary in sending or receiving electronic mail and (ii) provides to end-users of electronic mail services the ability to send or receive electronic mail.

"Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computerized representation thereof.

"Network" means any combination of digital transmission facilities and packet switches, routers, and similar equipment interconnected to enable the exchange of computer data.

"Owner" means an owner or lessee of a computer or a computer network or an owner, lessee, or licensee of computer data, computer programs, or computer software.

"Person" shall include any individual, partnership, association, corporation or joint venture.

"Property" shall include:

1. Real property;
2. Computers and computer networks;
3. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:
 - a. Tangible or intangible;
 - b. In a format readable by humans or by a computer;
 - c. In transit between computers or within a computer network or between any devices which comprise a computer; or
 - d. Located on any paper or in any device on which it is stored by a computer or by a human; and
4. Computer services.

A person "uses" a computer or computer network when he attempts to cause or causes:

1. A computer or computer network to perform or to stop performing computer operations;
2. The withholding or denial of the use of a computer, computer network, computer program, computer data or computer software to another user; or
3. A person to put false information into a computer.

A person is "without authority" when he has no right or permission of the owner to use a computer or he uses a computer or computer network in a manner exceeding such right or permission.

§ 18.2-152.3. Computer fraud.

Any person who uses a computer or computer network without authority and with the intent to:

1. Obtain property or services by false pretenses;
2. Embezzle or commit larceny; or
3. Convert the property of another is guilty of the crime of computer fraud.

If the value of the property or services obtained is \$200 or more, the crime of computer fraud shall be punishable as a Class 5 felony. Where the value of the property or services obtained is less than \$200, the crime of computer fraud shall be punishable as a Class 1 misdemeanor.

(1984, c. 751; 1985, c. 322; 2003, cc. 987, 1016.)

§ 18.2-152.3:1. Transmission of unsolicited bulk electronic mail; penalty.

A. Any person who:

1. Uses a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers; or
2. Knowingly sells, gives, or otherwise distributes or possesses with the intent to sell, give, or distribute software that (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information is guilty of a Class 1 misdemeanor.

B. A person is guilty of a Class 6 felony if he commits a violation of subsection A and:

1. The volume of UBE transmitted exceeded 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period; or

2. The revenue generated from a specific UBE transmission exceeded \$1,000 or the total revenue generated from all UBE transmitted to any EMSP exceeded \$50,000.
- C. A person is guilty of a Class 6 felony if he knowingly hires, employs, uses, or permits any minor to assist in the transmission of UBE in violation of subdivision B 1 or subdivision B 2.

§ 18.2-152.4. Computer trespass; penalty.

- A. It shall be unlawful for any person to use a computer or computer network without authority and with the intent to:
2. Temporarily or permanently remove, halt, or otherwise disable any computer data, computer programs, or computer software from a computer or computer network;
 3. Cause a computer to malfunction, regardless of how long the malfunction persists;
 4. Alter or erase any computer data, computer programs, or computer software;
 5. Effect the creation or alteration of a financial instrument or of an electronic transfer of funds;
 6. Cause physical injury to the property of another;
 7. Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.
- B. Any person who violates this section shall be guilty of computer trespass, which offense shall be punishable as a Class 1 misdemeanor. If there is damage to the property of another valued at \$2,500 or more caused by such person's malicious act in violation of this section, the offense shall be punishable as a Class 6 felony.
- C. Nothing in this section shall be construed to interfere with or prohibit terms or conditions in a contract or license related to computers, computer data, computer networks, computer operations, computer programs, computer services, or computer software or to create any liability by reason of terms or conditions adopted by, or technical measures implemented by, a Virginia-based electronic mail service provider to prevent the transmission of unsolicited electronic mail in violation of this article. Nothing in this section shall be construed to prohibit the monitoring of computer usage of, the otherwise lawful copying of data of, or the denial of computer or Internet access to a minor by a parent or legal guardian of the minor.

§ 18.2-152.5. Computer invasion of privacy.

- A. A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any

employment, salary, credit or any other financial or personal information relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.

- B. The crime of computer invasion of privacy shall be punishable as a Class 1 misdemeanor.

(1984, c. 751; 1985, c. 398; 2001, c. 358.)

18.2-152.6. Theft of COMPUTER services.

Any person who willfully uses a COMPUTER or COMPUTER network, with intent to obtain COMPUTER services without authority, shall be guilty of the CRIME of theft of COMPUTER services, which shall be punishable as a Class 1 misdemeanor.

18.2-152.7. Personal trespass by COMPUTER.

- A. A person is guilty of the CRIME of personal trespass by COMPUTER when he uses a COMPUTER or COMPUTER network without authority and with the intent to cause physical injury to an individual.
- B. If committed maliciously, the CRIME of personal trespass by COMPUTER shall be punishable as a Class 3 felony. If such act be done unlawfully but not maliciously, the CRIME of personal trespass by COMPUTER shall be punishable as a Class 1 misdemeanor.

s 18.2-152.8. Property capable of embezzlement.

For purposes of s 18.2-111, personal property subject to embezzlement shall include:

1. COMPUTERS and COMPUTER networks;
2. Financial instruments, COMPUTER data, COMPUTER programs, COMPUTER software and all other personal property regardless of whether they are:
 - a. Tangible or intangible;
 - b. In a format readable by humans or by a COMPUTER;
 - c. In transit between COMPUTERS or within a COMPUTER network or between any devices which comprise a COMPUTER; or
 - d. Located on any paper or in any device on which it is stored by a COMPUTER or by a human; and
3. COMPUTER services.

(1984, c. 751.)

§ 18.2-152.12. Civil relief; damages.

- A. Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefore and recover for any damages sustained, and

the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.

- B. If the injury under this article arises from the transmission of unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider where the defendant has knowledge of the authority or policies of the EMSP or where the authority or policies of the EMSP are available on the electronic mail service provider's website, the injured person, other than an electronic mail service provider, may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover the lesser of \$10 for each and every unsolicited bulk electronic mail message transmitted in violation of this article, or \$25,000 per day. The injured person shall not have a cause of action against the electronic mail service provider that merely transmits the unsolicited bulk electronic mail over its computer network. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.
- C. If the injury under this article arises from the transmission of unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider where the defendant has knowledge of the authority or policies of the EMSP or where the authority or policies of the EMSP are available on the electronic mail service provider's website, an injured electronic mail service provider may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover \$1 for each and every intended recipient of an unsolicited bulk electronic mail message where the intended recipient is an end user of the EMSP or \$25,000 for each day an attempt is made to transmit an unsolicited bulk electronic mail message to an end user of the EMSP. In calculating the statutory damages under this provision, the court may adjust the amount awarded as necessary, but in doing so shall take into account the number of complaints to the EMSP generated by the defendant's messages, the defendant's degree of culpability, the defendant's prior history of such conduct, and the extent of economic gain resulting from the conduct. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.
- D. At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party and in such a way as to protect the privacy of nonparties who complain about violations of this section.
- E. The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

- F. A civil action under this section must be commenced before expiration of the time period prescribed in § 8.01-40.1. In actions alleging injury arising from the transmission of unsolicited bulk electronic mail, personal jurisdiction may be exercised pursuant to § 8.01-328.1.

s 18.2-152.14. COMPUTER as instrument of forgery.

The creation, alteration, or deletion of any COMPUTER data contained in any COMPUTER or COMPUTER network, which if done on a tangible document or instrument would constitute forgery under Article 1 (s 18.2-168 et seq.) of Chapter 6 of this Title, will also be deemed to be forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to any CRIME set forth in Article 1 (s 18.2-168 et seq.) of Chapter 6 of this Title if a creation, alteration, or deletion of COMPUTER data was involved in lieu of a tangible document or instrument. (1984, c. 751; 1985, c. 322.)

§ 18.2-152.16. Forfeitures for violation of this article.

All moneys and other income, including all proceeds earned but not yet received by a defendant from a third party as a result of the defendant's violations of this article, and all computer equipment, all computer software, and all personal property used in connection with any violation of this article known by the owner thereof to have been used in violation of this article, shall be subject to lawful seizure by a law-enforcement officer and forfeiture by the Commonwealth in accordance with the procedures set forth in Chapter 22.1 (§ 19.2-386.1 et seq.) of Title 19.2, applied mutatis mutandis.

18.2-186.3. Identity theft; penalty; restitution; victim assistance.

- B. It shall be unlawful for any person, without the authorization or permission of the person or persons who are the subjects of the identifying information, with the intent to defraud, for his own use or the use of a third person, to:
1. Obtain, record or access identifying information which is not available to the general public that would assist in accessing financial resources, obtaining identification documents, or obtaining benefits of such other person;
 2. Obtain goods or services through the use of identifying information of such other person;
 3. Obtain identification documents in such other person's name; or
 4. Obtain, record or access identifying information while impersonating a law-enforcement officer or an official of the government of the Commonwealth.
- B. It shall be unlawful for any person without the authorization or permission of the person who is the subject of the identifying information, with the intent to sell or distribute the information to another to:
1. Fraudulently obtain, record or access identifying information that is not available to the general public that would assist in accessing financial resources, obtaining identification documents, or obtaining benefits of such other person;

2. Obtain goods or services through the use of identifying information of such other person;
3. Obtain identification documents in such other person's name; or
4. Obtain, record or access identifying information while impersonating a law-enforcement officer or an official of the Commonwealth.

B1. It shall be unlawful for any person to use identification documents or identifying information of another person or of a false or fictitious person, whether that person is dead or alive, to avoid summons, arrest, prosecution or to impede a criminal investigation.

C. As used in this section, "identifying information" shall include but not be limited to: (i) name; (ii) date of birth; (iii) social security number; (iv) driver's license number; (v) bank account numbers; (vi) credit or debit card numbers; (vii) personal identification numbers (PIN); (viii) electronic identification codes; (ix) automated or electronic signatures; (x) biometric data; (xi) fingerprints; (xii) passwords; or (xiii) any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain goods or services.

D. Violations of this section shall be punishable as a Class 1 misdemeanor. Any violation resulting in financial loss of greater than \$200 shall be punishable as a Class 6 felony. Any second or subsequent conviction shall be punishable as a Class 6 felony. Any violation resulting in the arrest and detention of the person whose identification documents or identifying information were used to avoid summons, arrest, prosecution, or to impede a criminal investigation shall be punishable as a Class 6 felony. In any proceeding brought pursuant to this section, the crime shall be considered to have been committed in any locality where the person whose identifying information was appropriated resides, or in which any part of the offense took place, regardless of whether the defendant was ever actually in such locality.

E. Upon conviction, in addition to any other punishment, a person found guilty of this offense shall be ordered by the court to make restitution as the court deems appropriate to any person whose identifying information was appropriated or to the estate of such person. Such restitution may include the person's or his estate's actual expenses associated with correcting inaccuracies or errors in his credit report or other identifying information.

G. Upon the request of a person whose identifying information was appropriated, the Attorney General may provide assistance to the victim in obtaining information necessary to correct inaccuracies or errors in his credit report or other identifying information; however, no legal representation shall be afforded such person.

(2000, c. 349; 2001, c. 423; 2003, cc. 847, 914, 918; 2004, c. 450.)

Appendix C

Federal Computer Crime Statutes

The following sections are taken verbatim from the USA PATRIOT Act which was accessed through the following website

<http://www.epic.org/privacy/terrorism/hr3162.html>

Section 217 INTERCEPTION OF COMPUTER TRESPASSER COMMUNICATIONS.

Chapter 119 of title 18, United States Code, is amended--

(1) in section 2510--

(A) in paragraph (18), by striking `and' at the end;

(B) in paragraph (19), by striking the period and inserting a semicolon; and

(C) by inserting after paragraph (19) the following:

`(20) `protected computer' has the meaning set forth in section 1030; and

`(21) `computer trespasser'--

`(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

`(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.'; and

(2) in section 2511(2), by inserting at the end the following:

`(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

`(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

`(II) the person acting under color of law is lawfully engaged in an investigation;

`(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

`(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.'.

Section 220 NATIONWIDE SERVICE OF SEARCH WARRANTS FOR ELECTRONIC EVIDENCE.

a) IN GENERAL- Chapter 121 of title 18, United States Code, is amended--

(1) in section 2703, by striking `under the Federal Rules of Criminal Procedure' every place it appears and inserting `using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation'; and

(2) in section 2711--

(A) in paragraph (1), by striking `and';
(B) in paragraph (2), by striking the period and inserting `; and'; and
(C) by inserting at the end the following:
`(3) the term `court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.'

(b) CONFORMING AMENDMENT- Section 2703(d) of title 18, United States Code, is amended by striking `described in section 3127(2)(A)'.

SEC. 814. DETERRENCE AND PREVENTION OF CYBERTERRORISM.

(a) CLARIFICATION OF PROTECTION OF PROTECTED COMPUTERS- Section 1030(a)(5) of title 18, United States Code, is amended--

(1) by inserting `(i)' after `(A)';
(2) by redesignating subparagraphs (B) and (C) as clauses (ii) and (iii), respectively;
(3) by adding `and' at the end of clause (iii), as so redesignated; and
(4) by adding at the end the following:
`(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--
`(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;
`(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
`(iii) physical injury to any person;
`(iv) a threat to public health or safety; or
`(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;'

(b) PROTECTION FROM EXTORTION- Section 1030(a)(7) of title 18, United States Code, is amended by striking `, firm, association, educational institution, financial institution, government entity, or other legal entity,'.

(c) PENALTIES- Section 1030(c) of title 18, United States Code, is amended--

(1) in paragraph (2)--
(A) in subparagraph (A) --
(i) by inserting `except as provided in subparagraph (B),' before `a fine';
(ii) by striking `(a)(5)(C)' and inserting `(a)(5)(A)(iii)'; and
(iii) by striking `and' at the end;
(B) in subparagraph (B), by inserting `or an attempt to commit an offense punishable under this subparagraph,' after `subsection (a)(2),' in the matter preceding clause (i); and
(C) in subparagraph (C), by striking `and' at the end;

(2) in paragraph (3)--

(A) by striking `, (a)(5)(A), (a)(5)(B),' both places it appears; and

(B) by striking `(a)(5)(C)' and inserting `(a)(5)(A)(iii)'; and

(3) by adding at the end the following:

`(4)(A) a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

`(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

`(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.'

(d) DEFINITIONS- Section 1030(e) of title 18, United States Code is amended--

(1) in paragraph (2)(B), by inserting `, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States' before the semicolon;

(2) in paragraph (7), by striking `and' at the end;

(3) by striking paragraph (8) and inserting the following:

`(8) the term `damage' means any impairment to the integrity or availability of data, a program, a system, or information;';

(4) in paragraph (9), by striking the period at the end and inserting a semicolon; and

(5) by adding at the end the following:

`(10) the term `conviction' shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

`(11) the term `loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

`(12) the term `person' means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.'

(e) DAMAGES IN CIVIL ACTIONS- Section 1030(g) of title 18, United States Code is amended--

(1) by striking the second sentence and inserting the following: `A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages.'; and

(2) by adding at the end the following: `No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.'.

(f) AMENDMENT OF SENTENCING GUIDELINES RELATING TO CERTAIN COMPUTER FRAUD AND ABUSE- Pursuant to its authority under section 994(p) of title 28, United States Code, the United States Sentencing Commission shall amend the Federal sentencing guidelines to ensure that any individual convicted of a violation of section 1030 of title 18, United States Code, can be subjected to appropriate penalties, without regard to any mandatory minimum term of imprisonment.

SEC. 816. DEVELOPMENT AND SUPPORT OF CYBERSECURITY FORENSIC CAPABILITIES.

(a) IN GENERAL- The Attorney General shall establish such regional computer forensic laboratories as the Attorney General considers appropriate, and provide support to existing computer forensic laboratories, in order that all such computer forensic laboratories have the capability--

- (1) to provide forensic examinations with respect to seized or intercepted computer evidence relating to criminal activity (including cyberterrorism);
- (2) to provide training and education for Federal, State, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer-related crime (including cyberterrorism);
- (3) to assist Federal, State, and local law enforcement in enforcing Federal, State, and local criminal laws relating to computer-related crime;
- (4) to facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer-related crime with State and local law enforcement personnel and prosecutors, including the use of multijurisdictional task forces; and
- (5) to carry out such other activities as the Attorney General considers appropriate.

(b) AUTHORIZATION OF APPROPRIATIONS-

(1) AUTHORIZATION- There is hereby authorized to be appropriated in each fiscal year \$50,000,000 for purposes of carrying out this section.

(2) AVAILABILITY- Amounts appropriated pursuant to the authorization of appropriations in paragraph (1) shall remain available until expended.

Works Cited

- Anti-Phishing Working Group. Anti-Phishing Working Group.
<http://www.antiphishing.org> (accessed 28 November 2004).
- Arizona State Legislature. Title 13 Criminal Code.
<http://www.azleg.state.az.us/ArizonaRevisedStatutes.asp?Title=13> (accessed 15 October 2004).
- Associated Press. "Trial Reveals Spammer Techniques." 14 Nov. 2004.
<http://edition.cnn.com/2004/TECH/internet/11/14/inside.spamming.ap/>
(accessed 3 December 2004).
- Business Software Alliance. Play It Cyber Safe.
<http://www.playitcybersafe.com/cybercrime> (accessed 22 November 2004).
- Business Software Alliance. Teaching Cyber Ethics to America's Youth Should Begin @ Home Survey Says.
<http://www.bsa.org/usa/press/newsreleases/Teaching-Cyber-Ethics-to-Americas-Youth-Begin-at-Home-Survey-Says.cfm> (accessed 2 November 2004).
- CERT. Denial of Service Attacks.
http://www.cert.org/tech_tips/denial_of_service.html (accessed 22 November 2004).
- CNNMoney. More sites hacked in wake of Yahoo!
<http://money.cnn.com/2000/02/08/technology/yahoo/> (accessed 22 November 2004).
- Computer Crime Research Center. About Computer Crime Research Center.
<http://www.crime-research.org/about/> (accessed 23 November 2004).
- Computer Crimes and Intellectual Property Section. Computer Crimes Policy and Programs.
<http://www.cybercrime.gov/ccpolicy.html> (accessed 22 November 2004).
- Computer Science @ Virginia Tech. Virginia State Laws.
<http://courses.cs.vt.edu/~cs3604/lib.crime.virginia.law.full> (accessed 15 October 2004).
- Computer Security Institute. 2003 CSI/FBI Computer Crime and Security Survey.
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf (accessed 10 November 2003).

- Computer Security Institute. 2004 CSI/FBI Computer Crime and Security Survey.
http://i.cmpnet.com/gosci/db_area/pdfs/fbi/FBI2004.pdf (accessed 12 October 2004).
- Computer Security Policy and Research Institute. CSPRI - About Us - Mission.
<http://www.cpi.seas.gwu.edu/aboutus.html> (accessed 23 November 2004).
- Consumer Sentinel. "National and State Trends in Fraud and Identity Theft January - December 2003". Federal Trade Commission. 22 Jan 2004.
<http://www.consumer.gov/sentinel/trends.htm> (accessed 3 December 2004).
- Crane, Bill. Personal Interview. 27 November 2004.
- CyberAngels. CyberAngels.org - The Largest Online Internet Safety Program Since 1995.
<http://www.cyberangels.org/index.html> (accessed 23 November 2004).
- CyberAngels. Cyberangels Mission Statement.
<http://www.cyberangels.org/mission/index.html> (accessed 23 November 2004).
- Denning, DE. Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives.
<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> (accessed 22 November 2004).
- Department of Justice. Lanham, Maryland Man Pleads Guilty to Copyright Infringement for Operating a Pay-for-Access Website Offering Pirated Copies of Business Software (October 14, 2004).
<http://www.cybercrime.gov/singh2Plea.htm> (accessed 22 November 2004).
- Department of Justice. Lusby, Maryland Man Pleads Guilty to Sabotaging IRS Computers.
<http://www.usdoj.gov/criminal/cybercrime/carpenterPlea.htm> (accessed 22 November 2004).
- Department of Justice. Russian Man Sentenced for Hacking into Computers in the United States.
<http://www.cybercrime.gov/ivanovSent.htm> (accessed 22 November 2004).
- Federal Bureau of Investigation. Investigative Programs: Crimes Against Children.
<http://www.fbi.gov/hq/cid/cac/innocent.htm> (accessed 22 November 2004).
- Feeny, Peter. Personal interview. 1 December 2004.
- Goodman, M. "Making Computer Crime Count". FBI Law Enforcement Bulletin. August 2001:10-17.

- Gordon, LA, Loeb MP, Lucyshyn W, Richardson R. 2004 CSI/FBI Computer Crime and Security Survey. Computer Security Institute, 2004.
- Gordon, GR, Hosmer, CD, Siedsma, C, Rebovich D. Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime.
<http://www.ncjrs.org/pdffiles1/nij/grants/198421.pdf> (accessed 3 November 2004).
- Haantz, S. WCC Issue: Computer Crime: Computer as the Instrumentality of the Crime. National White Collar Crime Center. September 2002.
- Haugen, S, Selin RJ. "Identifying and Controlling Computer Crime and Employee Fraud." Industrial Management and Data Systems 99.8 (1999): 340.
- Internet crime Complaint Center. IC3 - Internet Crime Complaint Center.
<http://www.ic3.gov/> (accessed 28 November 2004).
- Internet Fraud Complaint Center. Internet Fraud Complaint Center.
<http://www.ifccfbi.gov/index.asp> (accessed 23 November 2004).
- Internet Fraud Complaint Center. IC3 2003 Internet Fraud Report.
http://www1.ifccfbi.gov/strategy/2003_IC3Report.pdf (accessed 12 October 2004).
- Koinange, Jeff. "Internet fleecing scams thrive in Nigeria" 11 Aug 2002.
<http://archives.cnn.com/2002/TECH/internet/08/11/nigeria.scam/index.html> (accessed 3 December 2004).
- Krebs, Brian. "Phishing Feeds Internet Black Markets". Washington Post 11/18/04
- Law Office of Davis McCown. California Computer Crime.
<http://www.davismccownlaw.com/articles/calcc.htm> (accessed 15 October 2004).
- Lee, Allen Lt. Personal interview. 19 November 2004.
- LeFever, Chris Special Agent. Personal interview. 6 December 2004.
- Maryland State Laws, obtained via the United States Secret Service "Forward Edge Computer Training on Seizing Electronic Evidence" compact disk
- Mass.gov. General Laws of Massachusetts.
<http://www.mass.gov/legis/laws/mgl/gl-266-toc.htm> (accessed 15 October 2004).
- Micci-Barreca, Daniele. "With Criminal Intent." Fraud International 22 (2004):30-4.

- Montgomery County Department of Police. MC Department of Police:
Divisions/District Stations - Computer Crimes.
<http://www.montgomerycountymd.gov/poltmpl.asp?url=/Content/POL/ask/computerCrimes.asp> (ACCESSED 18 November 2004).
- Motion Picture Association of America. Anti-Piracy.
<http://www.mpaa.org/anti-piracy/> (accessed 22 November 2004).
- National Conference of State Legislature. Computer Crime 2001 Enactments.
<http://www.ncsl.org/programs/lis/legislation/compcrime01.htm> (accessed 3 December 2004).
- National Fraud Information Center. Internet and Telemarketing Fraud: Advice, Trends, and More.
<http://www.fraud.org/> (accessed 23 November 2004).
- National Institute of Justice. JUSTNET - Justice Technology Information Network.
<http://www.nlectc.org/assistance/justnet.html> (accessed 22 November 2004).
- National Security Institute. California Codes.
<http://nsi.org/Library/Compsec/computerlaw/Californ.txt> (accessed 3 November 2004).
- National Security Institute. Code of Iowa 1989.
<http://nsi.org/Library/Compsec/computerlaw/Iowa.txt> (accessed 15 October 2004).
- National Security Institute. General Statutes of Connecticut.
<http://nsi.org/Library/Compsec/computerlaw/Connecti.txt> (accessed 15 October 2004).
- National White Collar Crime Center. NW3C (National White Collar Crime Center).
<http://www.nw3c.org/index.html> (accessed 28 November 2004).
- National White Collar Crime Center. IFCC 2002 Internet Fraud Report: January 1, 2002-December 31, 2002. http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdf (accessed 12 October 2004).
- National White Collar Crime Center. WCC Issue: Computer Crime: Computer as the Instrumentality of the Crime.
<http://www.nw3c.org/> (accessed 3 November 2004).
- National White Collar Crime Center and the Federal Bureau of Investigation. "IC3 2003 Internet Fraud Report". January 2004.
http://www1.ifccfbi.gov/strategy/2003_IC3Report.pdf (accessed 3 December 2004).

- PBS. Computer Crime Laws.
<http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html>
(accessed 3 November 2004).
- Rantala, RR. Cybercrime Against Business. Bureau of Justice Statistics. March 2004.
- Renninger, Gary. Personal interview. 18 November 2004.\
- Richardson, R. 2003 CSI/FBI Computer Crime and Security Survey. Computer Security Institute, 2003.
- Rushinek, A, Rushinek, SF. "Using Experts for Detecting and Litigating Computer Crime". Managerial Auditing Journal. 8.7(1993):19-22.
- Security Focus. Florida.
<http://downloads.securityfocus.com/library/florida.html> (accessed 15 October 2004).
- Simpson, Doug. "Feds Find Dangerous Cyberstalking Hard to Prevent". 12 June 2000.
<http://archives.cnn.com/2000/TECH/computing/06/12/cyberstalkers.idg/index.html> (accessed 3 December 2004).
- Smolek, Robert Sgt. Personal interview. 18 November 2004.
- Smolek, Robert Sgt. Personal interview. 19 November 2004.
- Tandukar, Amita. "Mapping Relationships." Fraud International 20 (2004): 58-60.
- Texas State Laws. Texas Statutes Penal Code.
www.capitol.state.tx.us/statutes/pe.toc.htm (access 15 October 2004).
- TextFiles.com. New York Penal Law.
http://www.textfiles.com/law/ny_lawsta.law (accessed 15 October 2004).
- The Gallup Organization. Crime Victimization about the Same as Last Year: One in 20 Households Experience Violent Crime.
<http://www.gallup.com/poll/content/print.aspx?i=9613> (accessed 18 October 2004).
- Thompson, David. "1997 Computer Crime and Security Survey". Information Management and Computer Security. 6.2 (1998): 78+.
- Department of Justice. Internet Fraud.
<http://www.internetfraud.usdoj.gov/> (accessed 12 October 2004).

- U.S. Department of Justice. National Institute of Justice Research Report. Electronic Crime Needs Assessment for State and Local Law Enforcement. National Institute of Justice, March 2001.
- United States. U.S. Sentencing Commission. Computer Fraud Working Group. September 1993. <http://www.ussc.gov/publicat.cmptfrd.pdf> (accessed 12 October 2004).
- United States. "Stalking and Domestic Violence Report to Congress" May 2001. Department of Justice. <http://www.ncjrs.org/pdffiles1/ojp/186157.pdf> (accessed 3 December 2004).
- Williams, WP. The National Cybercrime Training Partnership. <http://www.wjin.net/Pubs/3417.htm> (accessed 22 November 2004).
- Wood, C. Fighting Net Crime: Canada's Police are Only Starting to Catch Up with Hackers and Other Criminals Who Target Online Computer Users. Maclean's. Toronto: Jun 12, 2000. 113.24:38+.
- Working to Halt Online Abuse. List of Cyberstalking Laws. <http://www.haltabuse.org/resources/laws/index.shtml> (accessed 12 October 2004).