COMPUTER CRIMINALS pdf

1: Computer Crime - criminal | www.enganchecubano.com

Convicted computer criminals are people who are caught and convicted of computer crimes such as breaking into computers or computer networks. Computer crime can be broadly defined as criminal activity involving information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or.

Share What is Computer Crime? Computer Crime is a type of crime that is classified as requiring, utilizing, and misuse of a computer or associated electronic networking system in order to commit illegal and unlawful acts. Computer crimes can range from the illegal use of the internet to the unlawful accessing of information stored in the computer terminal of another individual. Due to the expansiveness, as well as the relative modernity of the computer age, the legality surrounding cybercrime is not considered to be fully developed. New laws and legislation are in constant evolution with regard to Computer Crime. Computer Crime Offense Profile 1. Misdemeanor or Felony â€" varies upon case details 3. Varies upon the location of the crime, including the applicable country, nation, state, or province 4. Range of Punishment s: Fines, Probation, Internet Banning, or Incarceration â€" varies upon case details 5. Duration of Punishment s: Varies upon case details 6. Varies upon individual intent, criminal record, criminal history, and the time of the crime. However, cases involving child pornography, the corruption of a minor, or endangering the welfare of a minor through the usage of a computer can result in the mandatory registration in a sex offender database. Associated Offenses and Subgenres: The illegal possession of information, data, or records belonging to another individual or entity through the use of a computer. The purposeful engagement in the damaging, takeover, or hijacking of a computational system belonging to another individual or entity. The participation, disbursement, production, or sale of illegal sexual material of an explicit nature involving a minor. The unlawful disbursement of unsecured and fraudulent documentation with the intent to scam, trick, or steal. This includes phishing, spam, and malware. The unlawful possession of intellectual property belonging to another individual or entity through the use of a computer. This includes peer-to-peer sharing and illegal file-sharing. The unlawful use, possession, or distribution of intellectual property obtained through illegal means. The Arrest Process for Computer Crime Charges In the event that the prospect exists in which an individual is at risk for or has been arrested as a result of a Computer Crime charge, it is of the utmost importance that they are aware and mindful of the basic legality associated with the criminal justice system. Individuals who have been served documentation in the form of an arrest warrant displaying a Computer Crime, or have been arrested by law enforcement, are encouraged to cooperate with the arresting officers regardless of personal belief with regard to the charges. Individuals under arrest will be given the opportunity to consult with legal specialists subsequent to the arrest process. Resisting or fleeing from a Computer Crime arrest can result in harm, injury, and additional penalties. Upon arrest, an individual should be made aware of the following in order to prevent any further complication s: This includes fair, respectful, and ethical treatment devoid of undue violence and harm. Habeas Corpus with regard to a Computer Crime Charge Subsequent to an arrest resulting from a Computer Crime charge, the notion of habeas corpus entitles all individuals to the right to a trial in a court of law. In addition, each individual is granted the right to legal representation. Pertinent details regarding any Computer Crime allegation should be discussed with a defense attorney. The Presumption of Innocence In the event that an individual is arrested as a result of a Computer Crime charge, criminal law within the United States maintains the innocence of that individual unless they are found guilty within a court of law or they have admitted guilt on their own accord. Miranda Rights Upon the arrest for a Computer Crime charge, this is the standard arrest protocol that must be upheld by any and all arresting officers. Miranda Rights include the Fifth Amendment, which states that an individual retains the right to remain silent in order to avoid incriminating themselves. In addition, Miranda Rights also guarantee the following rights with regard to an arrest: The Preparation of Computer Crime Defense In the event that an individual has been arrested on a Computer Crime charge, they are encouraged to observe the behavioral protocol of the arrest process. Individuals are encouraged to consult with attorneys specializing in criminal law and, if possible, those who

focus on Cyber Crime legality. In the construction of a defense, the individual may be asked to provide the following:

COMPUTER CRIMINALS pdf

2: Top Five Computer Crimes & How to Protect From Them

The FBI is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists. The threat is incredibly seriousâ€"and growing. Cyber intrusions are becoming.

Every year billions of dollars are made in a number of different cyber crimes , and the victims are usually people like you and me. The people writing the software found it amusing to write a program that exploited security flaws just to see how far it could spread. Today the incentive for making such software is generally more sinister and the reason it makes the list of the top five computer crimes. In some cases a piece of malware will pretend to be a legitimate piece of software, and will ask you for money to remove it: Not all malware tries to extract money from you directly, however. Many simply embed themselves into your computer in order to make use of it. Black-hat hackers may intend to launch an attack against a government or institution, and will use a network of compromised machines to do so. This sort of network is referred to as a botnet , and is a key tool of the trade for a number of Internet crimes. Macs, Windows and Linux PCs all need it. You really have no excuse. So grab one of these ten and start protecting your computer! Read More is a great place to start. Just as important as any software, however, is common sense. Identity Theft Identity theft easily makes the list of the top five computer crimes. In America alone there are almost 9 million victims of identity theft every year. The concept is simple: This could range from a black-hat hacker stealing your online banking account login and password to getting access to your social security number and using it to pretend to be you. Such people can make themselves a lot of money with your personal information, and screw you over in the process. The same goes for using your credit card or Paypal account to pay for something. The most important thing is to never share any personal information â€" such as your bank account number, your social security number or any information a fraudster could use to steal your identity â€" in an email, instant message or any other form of unencrypted communication. None of these communication channels were designed to be secure, and as such are not the proper way to share such information. This is a common ploy used by fakers. Nigerian princes do not ask strangers online to accept a money transfer. The Federal Trade Commission of the United States has a lot of good information about identity theft applicable to all countries; check it out. Cyberstalking People leave a lot of information about themselves online. Such information can leave you vulnerable to cyberstalking, a term that essentially refers to using the Internet to stalk someone in the traditional sense. Cyber stalking is essentially using the Internet to repeatedly harrass another person. This harassment could be sexual in nature, or it could have other motivations including anger or outright hostility. When you are online, only type things you would actually say to someone face to face. Think about how what you say might be interpreted without the context of body language and voice. Install and use parental control software on all computers. Know what sites your children frequent and monitor their online activity. Foster communication with your children so they understand the potential dangers they may be exposed to online. Good advice, all of it. The site also recommends a number of tools for achieving these goals, so check it out. Named for the amazing Monty Python sketch about a processed meat product , spam is illegal in many countries. So how does it spread? As such, one thing you can do to help stop the spread of spam is to ensure your computer is protected from such malware. This email service seems to have a spam problem licked, and it is the only service I personally use. Know another spam-free service? Share it in the comments below. There are a few other things you can do to slow spam from getting to your inbox, however. Can you think of any others beyond this list of the top five computer crimes? What are some other strategies for protecting yourself? If so please share in the comments below; a little knowledge can help us all a lot.

COMPUTER CRIMINALS pdf

3: Computer crime | Define Computer crime at www.enganchecubano.com

Cybercrime, or computer-oriented crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

Crime is an ever present problem, and with the proliferation of computer and computer technologies, crime using computers has become widespread. Computer crime, or cybercrime, is defined as any criminal activity in which computers, or a computer network, is the method or source of a crime. This encompasses a wide variety of crimes, from hacking into databases and stealing sensitive information to using computers to set up illegal activities. Since computers are so widespread, cybercrime has the ability to affect almost anyone today. Society and computer crime Society is becoming more integrated with computers, which means more personal information is online. Because of its ease, more business is also being conducted online. This attracts a growing number of criminals who can more easily get away with cybercrime than traditional crimes. Also, since it is harder to catch cyber criminals, they might feel a sense of protection. This leads to them committing cybercrime more frequently. Most people may have been affected by cybercrime in some way. For example, identity theft, a very damaging crime, is still on the rise, mostly through computers. This is the problem which society is confronting today. Types of computer crime Hacking Currently defined as to gain illegal or unautorized access to a file, computer or network. Identity Theft Various crimes in which a criminal or large group uses the identity of an unknowing, innocent person. E-mail fishing for personal and financial information disguised as legitimate business e-mail. Credit Card Fraud A wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. Forgery The process of making, adapting, or imitating objects, statistics, or documents, with the intent to deceive. New technologies are used to create fake checks, passports, visas, birth certificates with little skill or investments. Scams A confidence game or other fraudulent scheme,especially for making a quick profit,to cheat or swindle. Some sellers do not sell items or send inferior products. Common method is to buy a stock low, send out email urging others to buy and then, sell when the price goes up. Hacking Originally, the word, Hacking, was not used as defined above. Hacking was clever piece of code constructed by hackers who were smart and creative programmers. In s to s, the definition of hacking changed as many people started using computers and abused computer terminologies. By s, hacking behavior included spreading viruses, pranks, thefts, and phone phreaking. The difference between hackers and other criminals is the purpose of crime. Hackers commonly try to benefit not only themselves but also other computer users. Therefore, they have some ethics for their action. They believe sharing computer programs is important in development of new softwares. Openness will help people to access anything they need and use it for their personal demand. Decentralization will prevent authority from abusing information and controlling people. Those ethics will slowly change as the demand for computer changes. Identity Theft Today, threats of identify theft come in many forms. It is important that you learn how to recognize fraudulent activity to protect yourself from identity theft. Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes. For identity thieves, this information is as good as gold. Skilled identity thieves may use a variety of methods such as Old-Fashion Stealing, Skimming, Phishing, or Dumpster Diving to get hold of your information. To prevent any such identity theft is to monitor you personal accounts, bank statements and check your credit report on a regular basis. If you check your credit report regularly, you may be able to limit the damage caused by identity theft. Filing a police report, checking your credit reports, notifying creditors, and disputing any unauthorized transactions are some of the steps you must take immediately to restore your good name. Scams As of today there are so many ways to get lured to online scams. People who scam others are often referred as scammers, cheaters and swindlers. Online scams are everywhere they can be fake auctions and promotions. When people read great deals online they believe what they see but in reality it is a game of deceit. The frauds can also happen with health care, credit card, vacation and lottery. The internet changed the way we operate from research, leisure and work. Every day people are cheated by these frauds.

COMPUTER CRIMINALS pdf

People get scammed by fake photos, damaged goods, misleading information, and false advertising. People are tricked into providing their private information like social security numbers, address, phone numbers and credit card information. Forgery Digital forgery has become a big problem with the boom of the internet. Many businesses need proof of identity to perform a service, and with identity fraud being a larger goal for criminals this proof is difficult to accept as truthful. A social security number, credit card number, or bank account number are not strong enough proof to show who someone is anymore. Many companies ask for copies of a social security card, birth certificate, or a monthly bill with your name and address on it for further verification. Even going to these lengths is not enough. Digital forgery is taken one step further with software to recreate and manipulate these private documents and proceed with the scam intended. Unfortunately these scams are being made even more accessible to even the least educated of internet criminals. It is to the point where a thief can obtain your credit card information and recreate your birth certificate for less than it costs to fill up his gas tank. This is frightening because you will never even know if it is happening to you. Everyone must be aware that there are always cyber-criminals on the loose, and no information is sacred on the internet. A Gift Of Fire. Is there a Hacker Ethic for 90s Hackers? Heroes of the Computer Revolution, page ix. Gangs Get Into Identity Theft. Retrieved 20 November , Website: Computer Crime Research Center. United States Department of Justice. This is just supportive source for your writing. You can use them as refference. Identity theft is not only done by hackers like we all assume. The Department of Consumer Affairs has been investigating a former employee that has been sending social security numbers on State payroll to a personal email account. Identity theft is popular among the gangs such as the Armenian Power gang, Long Beach chapter of the Crips, and the prison-based Mexican Mafia. Computers, guns and paperwork for fabricating identities were found in several property searches in March The ring leaders have been found guilty and some men could face up to 90 charges. The charges faced consist of computer intrusion, conspiracy, identity theft and fraud. There was a diverse nationality amongst the computer criminals which were Estonian, Ukrainian, Belarusian, and Chinese. During the operation, police confiscated various computers. Police officers suspected that the boy was the ringleader of an international cyber crime network. His network had access to 1. The hackers from the cyber crime network used computers to crash industry computers, steal credit card information and manipulate stock trades. In the end, the boy was released with no charges. These internet criminals typically live outside of the United States. They victimize Indiana banks, residents and businesses. Cyber crime is a growing worry in the United States. The task force will crack cases of criminals who take advantages of children, steal trade secrets and Internet fraud. They have investigated one hundred and forty cases and reacquired about ninety-eight thousand dollars. Her job was to provide payroll processing services. Her clients include companies both inside and outside of California. She had adjusted Green Waste payroll records and overpaid her husband, an employee at Green Waste. She was charged with fraud in connection with a protected computer. He is relatively well-known in the hacker community. The male hacker is only sixteen years old. The government had successfully proven that he committed crimes from to He will be serving time for eleven months in a juvenile detention facility. He used various online screen names to get close to his minor female victims. He would pose as a long lost friend, relative or acquaintances and gain their trust. The girls would learn his identity after a series of personal information. If the victims did not do as told, he would threaten them that he would expose all their secrets and personal information such as past sexual experiences and sexual fantasies. Some of the victims obeyed to his threats and some did not. A set trial date is still not fixed.

4: cybercrime | Definition, Statistics, & Examples | www.enganchecubano.com

Kevin Mitnick was a genius kid hacker. By the time of his arrest in , he was considered perhaps the most-wanted computer criminal in the United States, according to the New York Times.. He.

The unsolicited sending of bulk email for commercial purposes spam is unlawful in some jurisdictions. Phishing is mostly propagated via email. Phishing emails may contain links to other websites that are affected by malware. Obscene or offensive content[edit] The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be illegal. The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs. One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography , which is illegal in most jurisdictions in the world. Online harassment[edit] Various aspects needed to be considered when understanding harassment online. The examples and perspective in this section may not represent a worldwide view of the subject. You may improve this article , discuss the issue on the talk page , or create a new article , as appropriate. March See also: Cyberbullying , Online predator , Cyberstalking , and Internet troll Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties. Harassment on the internet also includes revenge porn. There are instances where committing a crime using a computer can lead to an enhanced sentence. For example, in the case of United States v. Neil Scott Kramer , Kramer was served an enhanced sentence according to the U. Although Kramer tried to argue this point, U. Sentencing Guidelines Manual states that the term computer "means an electronic, magnetic, optical, electrochemically , or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. Michigan , Arizona , and Virginia and South Carolina [19] have also passed laws banning harassment by electronic means. Although freedom of speech is protected by law in most democratic societies in the US this is done by the First Amendment , it does not include all types of speech. Some drug traffickers use encrypted messaging tools to communicate with drug mules. The dark web site Silk Road was a major online marketplace for drugs before it was shut down by law enforcement then reopened under new management, and then shut down by law enforcement again. After Silk Road 2. The original motivation of the hackers was to watch Star Trek reruns in Germany; which was something which Newscorp did not have the copyright to allow. In February , an individual going by the alias of MafiaBoy began a series denial-of-service attacks against high-profile websites, including Yahoo! About 50 computers at Stanford University , and also computers at the University of California at Santa Barbara, were amongst the zombie computers sending pings in DDoS attacks. On 3 August , Canadian federal prosecutors charged MafiaBoy with 54 counts of illegal access to computers, plus a total of ten counts of mischief to data for his attacks. Initially, much of its activity was legitimate. But apparently, the founders soon discovered that it was more profitable to host illegitimate activities and started hiring its services to criminals. It specialized in and in some cases monopolized personal identity theft for resale. It is the originator of MPack and an alleged operator of the now defunct Storm botnet. On 2 March , Spanish investigators arrested 3[clarification needed] in infection of over 13 million computers around the world. The "botnet" of infected computers included PCs inside more than half of the Fortune companies and more than 40 major banks, according to investigators. In August the international investigation Operation Delego , operating under the aegis of the Department of Homeland Security , shut down the international pedophile ring Dreamboard. The website had approximately members and may have distributed up to terabytes of child pornography roughly equivalent to 16, DVDs. To date this is the single largest U. Potentially compromising 70 million customers and 8. Other banks thought to be compromised: Bank of America , J. The Dow Jones later restored its session gains. In May , 74 countries logged a ransomware cybercrime, called " WannaCry " [33] Illicit access to camera sensors, microphone

sensors, phonebook contacts, all internet-enabled apps, and metadata of mobile telephones running Android and IOS were reportedly made accessible by Israeli spyware, found to be being in operation in at least 46 nation-states around the world. Journalists, Royalty and government officials were amongst the targets [34]. Combating computer crime[edit] You can help by adding to it. January Diffusion of cybercrime[edit] The broad diffusion of cybercriminal activities is an issue in computer crimes detection and prosecution. Blogs and communities have hugely contributed to information sharing: Furthermore, hacking is cheaper than ever: By comparison, a mail software-as-a-service is a scalable, inexpensive, bulk, and transactional e-mail-sending service for marketing purposes and could be easily set up for spam. Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigators in the form of a logfile. In most countries[citation needed] Internet Service Providers are required, by law, to keep their logfiles for a predetermined amount of time. For example; a European wide Data Retention Directive applicable to all EU member states states that all e-mail traffic should be retained for a minimum of 12 months. Methodology of cybercrime investigation There are many ways for cybercrime to take place, and investigations tend to start with an IP Address trace, however that is not necessarily a factual basis upon which detectives can solve a case. Different types of high-tech crime may also include elements of low-tech crime, and vice versa, making cybercrime investigators an indispensable part of modern law-enforcement. Methodology of cybercrime detective work is dynamic and is constantly improving, whether in closed police units, or in international cooperation framework. In developing countries, such as the Philippines , laws against cybercrime are weak or sometimes nonexistent. These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States , that has developed laws that allow for prosecution. While this proves difficult in some cases, agencies, such as the FBI , have used deception and subterfuge to catch criminals. For example, two Russian hackers had been evading the FBI for some time. They proceeded to lure the two Russian men into the United States by offering them work with this company. Upon completion of the interview, the suspects were arrested outside of the building. Clever tricks like this are sometimes a necessary part of catching cybercriminals when weak legislation makes it impossible otherwise. The executive order allows the United States to freeze assets of convicted cybercriminals and block their economic activity within the United States. This is some of the first solid legislation that combats cybercrime in this way. However, nuanced approaches have been developed that manage cyber offenders behavior without resorting to total computer or Internet bans. Cybercrime is becoming more of a threat to people across the world. Raising awareness about how information is being protected and the tactics criminals use to steal that information continues to grow in importance. Intelligence[edit] As cybercrime has proliferated, a professional ecosystem has evolved to support individuals and groups seeking to profit from cybercriminal activities. The ecosystem has become quite specialized, including malware developers, botnet operators, professional cybercrime groups, groups specializing in the sale of stolen content, and so forth. A few of the leading cybersecurity companies have the skills, resources and visibility to follow the activities of these individuals and group. Some of it is freely published, but consistent, on-going access typically requires subscribing to an adversary intelligence subscription service. Corporate sectors are considering crucial role of artificial intelligence cyber security.

COMPUTER CRIMINALS pdf

5: Computer Crime: How Techno-Criminals Operate

Similarly, many crimes involving computers are no different from crimes without computers: the computer is only a tool that a criminal uses to commit a crime. For example, Using a computer, a scanner, graphics software, and a high-quality color laser or ink jet printer for forgery or counterfeiting is the same crime as using an old-fashioned.

See Article History Alternative Title: Cybercrime, especially through the Internet , has grown in importance as the computer has become central to commerce, entertainment, and government. Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another. Defining cybercrime New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer , but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Cybercrime, especially involving the Internet, represents an extension of existing criminal behaviour alongside some novel illegal activities. Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity. An important aspect of cybercrime is its nonlocal character: This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. For example, if a person accesses child pornography located on a computer in a country that does not ban child pornography, is that individual committing a crime in a nation where such materials are illegal? Where exactly does cybercrime take place? Cyberspace is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified. In the Council of Europe , together with government representatives from the United States, Canada, and Japan, drafted a preliminary international treaty covering computer crime. Work on the treaty proceeded nevertheless, and on November 23, , the Council of Europe Convention on Cybercrime was signed by 30 states. The convention came into effect in Additional protocols , covering terrorist activities and racist and xenophobic cybercrimes, were proposed in and came into effect in Types of cybercrime Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual. Also at this end of the spectrum is the growing crime of identity theft. Midway along the spectrum lie transaction-based crimes such as fraud , trafficking in child pornography , digital piracy , money laundering , and counterfeiting. These are specific crimes with specific victims, but the criminal hides in the relative anonymity provided by the Internet. Another part of this type of crime involves individuals within corporations or government bureaucracies deliberately altering data for either profit or political objectives. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These range from spam , hacking, and denial of service attacks against specific sites to acts of cyberterrorismâ€”that is, the use of the Internet to cause public disturbances and even death. Since the September 11 attacks of , public awareness of the threat of cyberterrorism has grown dramatically. Page 1 of 6.

COMPUTER CRIMINALS pdf

6: Computer Criminals | Is There a Security Problem in Computing? | InformIT

Computer Crime. Computer crime describes a very broad category of offenses. Some of them are the same as non-computer offenses, such as larceny or fraud, except that a computer or the Internet is used in the commission of the crime.

By contrast, the sheriff dressed well, stood proud and tall, was known and respected by everyone in town, and struck fear in the hearts of most criminals. To be sure, some computer criminals are mean and sinister types. But many more wear business suits, have university degrees, and appear to be pillars of their communities. Some are high school or university students. Others are middle-aged business executives. Some are mentally deranged, overtly hostile, or extremely committed to a cause, and they attack computers as a symbol. Others are ordinary people tempted by personal profit, revenge, challenge, advancement, or job security. No single profile captures the characteristics of a "typical" computer criminal, and many who fit the profile are not criminals at all. Whatever their characteristics and motivations, computer criminals have access to enormous amounts of hardware, software, and data; they have the potential to cripple much of effective business and government throughout the world. In a sense, then, the purpose of computer security is to prevent these criminals from doing damage. For the purposes of studying computer security, we say computer crime is any crime involving a computer or aided by the use of one. Although this definition is admittedly broad, it allows us to consider ways to protect ourselves, our businesses, and our communities against those who use computers maliciously. Federal Bureau of Investigation regularly reports uniform crime statistics. The data do not separate computer crime from crime of other sorts. Moreover, many companies do not report computer crime at all, perhaps because they fear damage to their reputation, they are ashamed to have allowed their systems to be compromised, or they have agreed not to prosecute if the criminal will "go away. One approach to prevention or moderation is to understand who commits these crimes and why. Many studies have attempted to determine the characteristics of computer criminals. By studying those who have already used computers to commit crimes, we may be able in the future to spot likely criminals and prevent the crimes from occurring. In this section, we examine some of these characteristics. Amateurs Amateurs have committed most of the computer crimes reported to date. Most embezzlers are not career criminals but rather are normal people who observe a weakness in a security system that allows them to access cash or other valuables. In the same sense, most computer criminals are ordinary computer professionals or users who, while doing their jobs, discover they have access to something valuable. When no one objects, the amateur may start using the computer at work to write letters, maintain soccer league team standings, or do accounting. Alternatively, amateurs may become disgruntled over some negative work situation such as a reprimand or denial of promotion and vow to "get even" with management by wreaking havoc on a computing installation. Crackers or Malicious Hackers System crackers, 2 often high school or university students, attempt to access computing facilities for which they have not been authorized. The perception is that nobody is hurt or even endangered by a little stolen machine time. Crackers enjoy the simple challenge of trying to log in, just to see whether it can be done. Most crackers can do their harm without confronting anybody, not even making a sound. In the absence of explicit warnings not to trespass in a system, crackers infer that access is permitted. An underground network of hackers helps pass along secrets of success; as with a jigsaw puzzle, a few isolated pieces joined together may produce a large effect. Others attack for curiosity, personal gain, or self-satisfaction. And still others enjoy causing chaos, loss, or harm. There is no common profile or motivation for these attackers. Career Criminals By contrast, the career computer criminal understands the targets of computer crime. Criminals seldom change fields from arson, murder, or auto theft to computing; more often, criminals begin as computer professionals who engage in computer crime, finding the prospects and payoff good. There is some evidence that organized crime and international groups are engaging in computer crime. Recent attacks have shown that organized crime and professional criminals have discovered just how lucrative computer crime can be. Mike Danseglio, a security project manager with Microsoft, said, "In , the attackers want to pay the rent. They want to assimilate your computers and use them to make money" [NAR06a]. Ken

Dunham, Director of the Rapid Response Team for Verisign says he is "convinced that groups of well-organized mobsters have taken control of a global billion-dollar crime network powered by skillful hackers" [NAR06b]. Snow [SNO05] observes that a hacker wants a score, bragging rights. Organized crime wants a resource; they want to stay and extract profit from the system over time. These different objectives lead to different approaches: The hacker can use a quick-and-dirty attack, whereas the professional attacker wants a neat, robust, and undetected method. As mentioned earlier, some companies are reticent to prosecute computer criminals. In fact, after having discovered a computer crime, the companies are often thankful if the criminal quietly resigns. In other cases, the company is understandably more concerned about protecting its assets and so it closes down an attacked system rather than gathering evidence that could lead to identification and conviction of the criminal. The criminal is then free to continue the same illegal pattern with another company. Terrorists The link between computers and terrorism is quite evident. We see terrorists using computers in three ways: We cannot accurately measure the amount of computer-based terrorism because our definitions and measurement tools are rather weak. Still, there is evidence that all three of these activities are increasing.

COMPUTER CRIMINALS pdf

7: Computer and Internet Crime Laws | www.enganchecubano.com

Computer crime, or cybercrime, is defined as any criminal activity in which computers, or a computer network, is the method or source of a crime. This encompasses a wide variety of crimes, from hacking into databases and stealing sensitive information to using computers to set up illegal activities.

Computer and internet crimes run the gamut from identity theft to computer fraud and computer hacking. States and the federal government have laws that criminalize various types of behavior involving computers, computer systems, and the internet, and each has its own requirements and potential penalties. State computer crime laws differ widely, and when a person uses a computer to commit a crime, that crime may be covered under several different state or federal laws. Unlawful use or access. Access for fraudulent purposes. Other states have laws that punish using a computer to accomplish a fraudulent act. Some states, for example, make it a crime to use a computer, computer software, or computer network to fraudulently obtain goods or services of any kind. Some states provide additional penalties in cases where the data theft resulted in damage, while less severe penalties apply for thefts which did result in data being damaged, altered, or destroyed. All 50 states, as well as the federal government, have laws which prohibit keeping pornographic images of children. There are also laws which prohibit transmitting harmful materials to children. Internet Crime While computer crimes cover a wide range of activity, internet crime laws punish activity that specifically involves the internet in some way. These laws apply to emails and websites, as well as using the internet to commit identity theft or other forms of fraud. Like computer crimes, both individual states and the federal government have laws that apply to internet crime. Luring or soliciting children. Nearly all states have laws that make it a crime to use the internet to solicit, lure, or entice a child to engage in a sexual act. These laws apply when a person aged 18 or older uses the internet to communicate with a child. The age limit of a child for the purposes of these laws is usually Harassment, stalking, and bullying. Various states have enacted laws which criminalize using the internet to stalk , harass , or make criminal threats against someone. Recently, some states have enacted cyber bullying laws which criminalizes harassment aimed specifically towards minors. Other laws and new laws. There are any number of federal and state crimes that may also apply in computer and internet criminal cases. Federal wire fraud , for example, can apply to any case where a person uses a computer or electronic communications device to fraudulently deprive someone else of property. As computers and the internet continue to change and proliferate, legislatures regularly introduce new criminal laws which apply to internet and computer use. Penalties Because there are numerous different types of computer and internet crimes, there are also a wide range of potential penalties. Some computer crimes have minor penalties associated with them, while more serious crimes can impose significant fines and lengthy prison sentences. Fines for a conviction of various computer and internet crimes range widely. A person convicted of certain internet or computer crimes may also face a jail or prison sentence. The most serious crimes, such as possessing child pornography, can result in a prison sentence of 20 years or more. Probation sentences for computer crimes are also possible as either individual penalties or in addition to jail or fines. Probation terms can differ widely, but typically last at least one year and require the person on probation to not commit more crimes, maintain employment, report to a probation officer, and pay all court costs and fines. Talk to an Attorney Being accused of a computer or internet crime is very serious. Computer and internet crimes can be very complicated, involving numerous laws, evidentiary issues, and extensive government investigations. Your best defense against those powers is to find a qualified, experienced criminal defense attorney in your area. You need an attorney who has knowledge of the local courts, police, and prosecutors, and who can help you at every stage of your case.

8: What is a Computer Crime? (with pictures)

Computer Crime. The use of a computer to take or alter data, or to gain unlawful use of computers or services. Because of the versatility of the computer, drawing lines between criminal and noncriminal behavior regarding its use can be difficult.

Conclusion Introduction There are no precise, reliable statistics on the amount of computer crime and the economic loss to victims, partly because many of these crimes are apparently not detected by victims, many of these crimes are never reported to authorities, and partly because the losses are often difficult to calculate. Nevertheless, there is a consensus among both law enforcement personnel and computer scientists who specialize in security that both the number of computer crime incidents and the sophistication of computer criminals is increasing rapidly. Experts in computer security, who are not attorneys, speak of "information warfare". While such "information warfare" is just another name for computer crime, the word "warfare" does fairly denote the amount of damage inflicted on society. Two comments on word usage in this essay: However, to most users of English, the word "hacker" refers to computer criminals, and that is the usage that I have adopted in this essay. The legal problem of obscenity on the Internet is mostly the same as the legal problem of obscenity in books and magazines, except for some technical issues of personal jurisdiction on the Internet. Similarly, many crimes involving computers are no different from crimes without computers: Stealing a laptop computer with proprietary information stored on the hard disk inside the computer is the same crime as stealing a briefcase that contains papers with proprietary information. Using the Internet or online services to solicit sex is similar to other forms of solicitation of sex, and so is not a new crime. Using computers can be another way to commit either larceny or fraud. In contrast to merely using computer equipment as a tool to commit old crimes, this essay is concerned with computer crimes that are new ways to harm people. E-mails with bogus From: These acts might be punishable by existing criminal statutes that prohibit impersonation, forgery, deceit, or fraud. However, a judge might decide that the specific language in old statutes about writing or signature does not apply to e-mail. Similar issues arise in both: Unauthorized Use Unauthorized use of computers tends generally takes the following forms: The criminal reads or copies confidential or proprietary information, but data is neither deleted nor changed. For example, change a grade on a school transcript, add "money" to a checking account, etc. Unauthorized changing of data is generally a fraudulent act. Deleting entire files could be an act of vandalism or sabotage. Denying service to authorized users. On a modern time-sharing computer, any user takes some time and disk space, which is then not available to other users. During , computer programs and data were generally stored on cardboard cards with holes punched in them. If a vandal were to break into an office and either damage or steal the punch cards, the vandal could be adequately punished under traditional law of breaking and entering, vandalism, or theft. However, after about , it became common to enter programs and data from remote terminals a keyboard and monitor using a modem and a telephone line. The traditional laws were no longer adequate to punish criminals who used computer modems. Most unauthorized use of a computer is accomplished by a person in his home, who uses a modem to access a remote computer. In this way, the computer criminal is acting analogous to a burglar. The classic definition of a burglary is: Either the burglary statute needed to be made more general or new criminal statute s needed to be enacted for unauthorized access to a computer. Legislatures chose to enact totally new statutes. There are several basic ways to get these data: This sounds ridiculous, but many people will give out such valuable information to anyone who pretends to have a good reason. Not only should you refuse to provide such information, but please report such requests to the management of the online service or the local police, so they can be alert to an active criminal. In the s and early s, many of these computer voyeurs also used technology to make long-distance telephone calls for free, which technology also concealed their location when they were hacking into computers. Many of these voyeurs take a special thrill from hacking into military computers, bank computers, and telephone operating system computers, because the security is allegedly higher at these computers, so it is a greater technical challenge to hack into these machines. The criminals who change or delete data, or who deliberately gobble large amounts of computer resources, have a

more sinister motive and are capable of doing immense damage. In this regard, I would make an analogy to a homicide that occurs "accidentally" during the commission of a felony: In the s and early s, a common reaction was that hackers were a minor nuisance, like teenagers throwing rolls of toilet paper into trees. Altering files on that computer could have killed patients, which reminded everyone that hacking was a serious problem. This incident was cited by the U. Congress in the legislative history of a federal computer crime statute. Victims of such attacks include various U. Attacking the FBI website is like poking a lion with a stick. This is not the worst kind of computer crime. The proper owner of the site can always close the website temporarily, restore all of the files from backup media, improve the security at the site, and then re-open the site. The Internet is a medium for freely sharing information and opinions. These criminals often make the self-serving excuse for their actions that they only attack sites sponsored by bad corporations or bad people. However, this excuse makes these criminals into vigilantes who serve as legislature, judge, jury, and executioner: One example of punishment for the crime of defacing a website is the case of Dennis M. In February , he made "unauthorized intrusions" into computers at four different U. See the New Hampshire DoJ press release. Denial of Service DoS Attacks A denial of service attack occurs when an Internet server is flooded with a nearly continuous stream of bogus requests for webpages, thereby denying legitimate users an opportunity to download a page and also possibly crashing the webserver. The criminal first plants remote-control programs on dozens of computers that have broadband access to the Internet. When the criminal is ready to attack, he instructs the programs to begin pinging a specific target address. The computers containing the remote-control programs act as "zombies". The victim computer responds to each ping, but because the zombie computers gave false source addresses for their pings, the victim computer is unable to establish a connection with the zombie computers. Typically, after one or two hours, the criminal instructs his programs to stop pinging the victim. My essay , Tips for Avoiding Computer Crime, has specific suggestions for how you can use firewall software on your computer to prevent your computer from being used by criminals in DoS attacks on victims. The following is one case involving a famous series of DoS attacks: The Yahoo website was attacked at The websites of amazon. About fifty computers at Stanford University, and also computers at the University of California at Santa Barbara, were amongst the zombie computers sending pings in these DoS attacks. The attacks received the attention of President Clinton and the U. The FBI began to investigate. Because he was a juvenile, his name can not be publicly disclosed, so he was called by his Internet pseudonym Mafiaboy. CNN reported that Mafiaboy was granted bail, with the following conditions: He spent two weeks in jail. In December , Mafiaboy, now 16 y old, dropped out of school after being suspended from school six times since the beginning of that academic year, and failing all of his classes except physical education , and was employed at a menial job. He was again granted bail. On 18 Jan , Mafiaboy pleaded guilty to 5 counts of mischief to data and 51 counts of illegal access to computers. In issuing the sentence, Judge Gilles Ouellet commented: This is a grave matter. This attack weakened the entire electronic communications system. And the motivation was undeniable, this adolescent had a criminal intent. A virus is a program that "infects" an executable file. After infection, the executable file functions in a different way than before: There are two key features of a computer virus: Running the executable file may make new copies of the virus. A worm is a program that copies itself. Releasing such a worm into the Internet will slow the legitimate traffic on the Internet, as continuously increasing amounts of traffic are mere copies of the worm. A Trojan Horse is a deceptively labeled program that contains at least one function that is unknown to the user and that harms the user. A Trojan Horse does not replicate, which distinguishes it from viruses and worms. Other Trojan Horses are downloaded perhaps in an attachment in e-mail and installed by the user, who intends to acquire a benefit that is quite different from the undisclosed true purpose of the Trojan Horse. A logic bomb is a program that "detonates" when some event occurs. The detonated program might stop working e. A hoax is a warning about a nonexistent malicious program. I have a separate essay that describes how to recognize hoaxes, and how to respond to them. Some confusion about the distinction between a virus and a worm is caused by two distinctly different criteria: For most viruses or worms, these two different criteria give the same result. However, there have been a few malicious programs that might be considered a virus by some and a worm by others. Ultimately, the taxonomy matters only to computer scientists who are doing research

with these malicious programs. The first computer virus found "in the wild" was written in in a computer store in Lahore, Pakistan. In the s, computer viruses were generally spread by passing floppy disks from one user to another user. In the late s, computer viruses were generally spread via the Internet, either in e-mail e. The worm rapidly copied itself and effectively shut down the Internet. My long discussion of a few famous malicious programs is in a separate essay , emphasizes the nonexistent or weak punishment of the authors of these programs. There is a reported case under state law for inserting a logic bomb into custom software.

COMPUTER CRIMINALS pdf

9: Cybercrime - Wikipedia

Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files. Examples of computer crimes Below is a listing of the different types of computer crimes today. Clicking on any of the links below gives further information about each crime. Child pornography - Making or distributing child pornography. Cracking - Breaking or deciphering codes that are being used to protect data. Cyber terrorism - Hacking, threats, and blackmailing towards a business or person. Cyberbully or Cyberstalking - Harassing or stalking others online. Cybersquatting - Setting up a domain of another person or company with the sole intentions of selling it to them later at a premium price. Creating Malware - Writing, creating, or distributing malware e. Denial of Service attack - Overloading a system with so many requests it cannot serve normal requests. Espionage - Spying on a person or business. Fraud - Manipulating data, e. Harvesting - Collect account or other account related information on other people. Human trafficking - Participating in the illegal act of buying or selling other humans. Identity theft - Pretending to be someone you are not. Illegal sales - Buying or selling illicit goods online including drugs, guns, and psychotropic substances. Intellectual property theft - Stealing practical or conceptual information developed by another person or company. Phishing - Deceiving individuals to gain private or personal information about that person. Salami slicing - Stealing tiny amounts of money from each transaction. Scam - Tricking people into believing something that is not true. Slander - Posting libel or slander against another person or company. Software piracy - Copying, distributing, or using software that is copyrighted that you did not purchase. Spamming - Distributed unsolicited e-mail to dozens or hundreds of different addresses. Spoofing - Deceiving a system into thinking you are someone you really are not. Typosquatting - Setting up a domain that is a misspelling of another domain. Unauthorized access - Gaining access to systems you have no permission to access. Wiretapping - Connecting a device to a phone line to listen to conversations.

COMPUTER CRIMINALS pdf

Vol. 7. Greenes tu quoque John Cook The penguin book of classical myths Modern Sunday school and its present day task The emotional impact of subarachnoid haemorrhage Disability adjuster study guide The fantastic planet Identifying and treating risk patients in the wet finger environment Patterns in silicon Responses P. Jones, R. Melick The end of Marko Kraljevic Design Techniques for Modern Lace Audiences, and all that jazz, by R. A. Peterson. Kannada prabha epaper Memorias de un francotirador en stalingrado gratis Youve got to believe me Coaching actuaries exam p formula sheet Paul Baloche Our God Saves Ploughshares Spring 1999 Feminism : questions from the Indian context Fiendish a twisted fairytale by meka james The game ebook Bob Dole, legendary senator Legislative action to combat the world tobacco epidemic Third party insurance in Australia Firsts under the wire Hellenization revisited White girl problems Life centered career education Recent Transportation Literature for Planning Engineering Librarians (January 1991 (Public Administration Computer methods for engineering Good housekeeping caravan cooking Flowers on their bridles, hooves in the air Glen Hirshberg THE CHATTO BOOK OF LOVE POETRY 116 Dependent on the Kindness of Strangers Abnormal Psych with Client Snapshots W/CD Ethics and the conduct of business 5th edition Lawyers other reptiles The Gossamer Plain The Kingfisher encyclopedia of the future New Years babies