Chapter 6

Computer Fraud and Abuse Techniques

Learning Objectives

After studying this chapter, you should be able to:

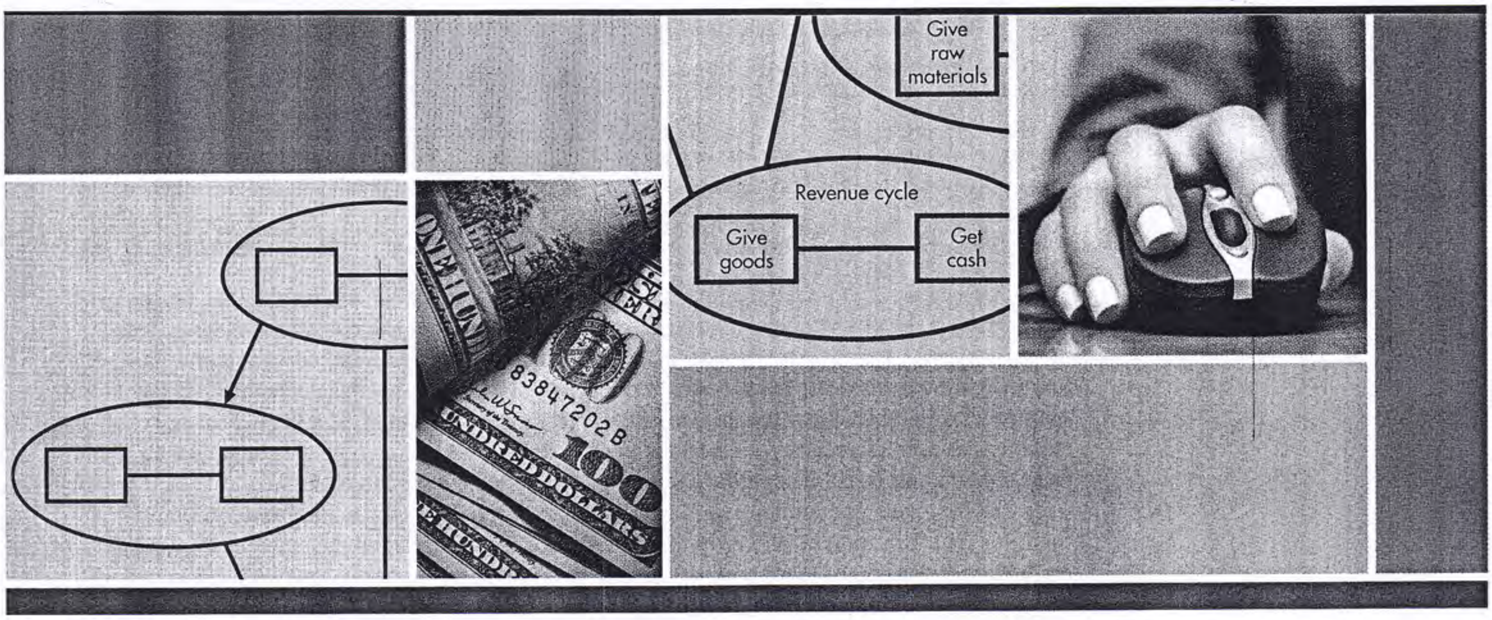
1. Compare and contrast computer attack and abuse tactics.
2. Explain how social engineering techniques are used to gain physical or logical access to computer resources.
3. Describe the different types of malware used to harm computers.

INTEGRATIVE CASE NORTHWEST INDUSTRIES

Northwest Industries wants to expand its service area and has been negotiating to buy Remodeling Products Centers (RPC), a competitor that operates in an area contiguous to Northwest. Jason Scott was part of a team sent to look over RPC's books before the deal was finalized. At the end of their first day, RPC's computer system crashed. The team decided to finish up what work they could and to let RPC's information technology (IT) people get the system up that night.

The next day, RPC's system was still down, so Jason tried to log into Northwest's computer system. It seemed to take forever to access, and then Jason found that system response was rather slow. His manager called the corporate office and found that there was something wrong with Northwest's system. It was assumed that the problem had something to do with communications with RPC's computers.

Jason's team was assigned to do a computer fraud and abuse evaluation of RPC's system while they waited. Since Jason had never participated in such a review, he was told to go back to the hotel where he could get on the Internet and spend the day researching the different ways computer systems could be attacked.



Introduction

Cyber criminals have devised an ever-increasing number of ways to commit computer fraud and abuse. This chapter discusses some of the more common techniques in three sections: computer attacks and abuse, social engineering, and malware. These classifications are not distinct; there is a lot of overlap among the categories. For example, social engineering methods are often used to launch computer attacks.

Computer Attacks and Abuse

All computers connected to the Internet, especially those with important trade secrets or valuable IT assets, are under constant attack from hackers, foreign governments, terrorist groups, disaffected employees, industrial spies, and competitors. These people attack computers looking for valuable data or to harm the computer system. Preventing attacks is a constant battle. On a busy day, large Web hosting farms suffer millions of attack attempts. This section describes some of the more common attack techniques.

Hacking is the unauthorized access, modification, or use of an electronic device or some element of a computer system. Most hackers break into systems using known flaws in operating systems or application programs, or as a result of poor access controls. One software-monitoring company estimates there are over 7,000 known flaws in software released in any given year. The following examples illustrate hacking attacks and the damage they cause:

- Russian hackers broke into Citibank's system and stole $10 million from customer accounts.
- Acxiom manages customer information for credit card issuers, banks, automotive manufacturers, and retailers. Daniel Baas, a systems administrator for a company doing business with Acxiom, exceeded his authorized access, downloaded an encrypted password file, and used a password-cracking program to access confidential identification information. The intrusion cost Acxiom over $5.8 million.
- During the Iraq war, Dutch hackers stole confidential information, including troop movements and weapons information, from 34 military sites. Their offer to sell the information to Iraq was declined, probably because Iraq feared it was a setup.
- A 17-year-old hacker, nicknamed Shadow Hawk, hacked the Bell Laboratories national network, destroyed files valued at $174,000, and copied 52 proprietary software programs worth $1.2 million. He published confidential information—such as telephone numbers, passwords, and instructions on how to breach AT&T's computer security

system—on underground bulletin boards. He was sentenced to nine months in prison and fined $10,000. Like Shadow Hawk, many hackers are young, some as young as 12 and 13.

- A hacker penetrated a software supplier's computer and used its "open pipe" to a bank customer to install a powerful Trojan horse in the bank's computer.

A ***botnet***, short for robot network, is a network of powerful and dangerous hijacked computers. ***Hijacking*** is gaining control of a computer to carry out illicit activities without the user's knowledge. ***Bot herders*** install software that responds to the hacker's electronic instructions onto unwitting PCs. Bot software is delivered in a variety of ways, including Trojans, e-mails, instant messages, Tweets, or an infected Web site. Bot herders use the combined power of the hijacked computers, called ***zombies***, to mount a variety of Internet attacks. Worldwide, there are over 2,000 botnets containing over 10 million computers (10% of online computers), many of them for rent. Bot toolkits and easy-to-use software are available on the Internet showing hackers how to create their own botnets; hacking is now almost as simple as picking and choosing features and clicking on a checkbox. The Mariposa botnet, containing almost 13 million computers in 190 countries, was created by three men without any advanced hacker skills.

Botnets are used to perform a ***denial-of-service (DoS) attack***, which is designed to make a resource unavailable to its users. In an e-mail attack, so many e-mails (thousands per second) are received, often from randomly generated false addresses, that the Internet service provider's e-mail server is overloaded and shuts down. Another attack involves sending so many Web page requests that the Web server crashes. An estimated 5,000 denial-of-service attacks occur per week. The Web sites of online merchants, banks, governmental agencies, and news agencies are frequent victims. The following examples illustrate denial-of-service attacks and the damage they cause:

- A DoS attack shut down 3,000 Web sites for 40 hours on one of the busiest shopping weekends of the year.
- CloudNine, an Internet service provider, went out of business after DoS attacks prevented its subscribers and their customers from communicating.
- An estimated 1 in 12 e-mails carried the MyDoom virus at its peak. The virus turned its host into a zombie that attacked Microsoft. Other companies, such as Amazon, Yahoo, CNN, and eBay, have all suffered similar DoS attacks.

Spamming is e-mailing or texting an unsolicited message to many people at the same time, often in an attempt to sell something. An estimated 250 billion e-mails are sent every day (2.8 million per second); 80% are spam and viruses. The Federal Trade Commission estimates that 80% of spam is sent from botnets. Spams are annoying and costly, and 10% to 15% offer products or services that are fraudulent. In retaliation, some spammers are spammed in return with thousands of messages, causing their e-mail service to fail. Such retaliation affects innocent users and can result in the closure of an e-mail account. Spammers scan the Internet for addresses posted online, hack into company databases, and steal or buy mailing lists. An AOL employee stole the names and e-mail addresses of 92 million people and sold them to spammers.

Spammers also stage ***dictionary attacks*** (also called *direct harvesting attacks*). Spammers use special software to guess addresses at a company and send blank e-mail messages. Messages not returned usually have valid e-mail addresses and are added to spammer e-mail lists. Dictionary attacks are a major burden to corporate e-mail systems and Internet service providers. Some companies receive more dictionary attack e-mail than valid e-mail messages. One day 74% of the e-mail messages that Lewis University received were for nonexistent addresses. Companies use e-mail filtering software to detect dictionary attacks; unfortunately, spammers continue to find ways around the rules used in e-mail filtering software.

A blog (short for We*b log*) is a Web site containing online journals or commentary. Hackers create ***splogs*** (combination of *sp*am and b*log*) with links to Web sites they own to increase their Google PageRank, which is how often a Web page is referenced by other Web pages. Since Web sites with high PageRanks appear first in search results pages, splogs are created to artificially inflate paid-ad impressions from visitors, to sell links, or to get new sites indexed. Splogs are annoying, waste valuable disk space and bandwidth, and pollute search engine results.

Spoofing is making an electronic communication look as if someone else sent it to gain the trust of the recipient. Spoofing can take various forms, including the following:

- *E-mail spoofing* is making an e-mail appear as though it originated from a different source. Many spam and phishing attacks use special software to create random sender addresses. A former Oracle employee was charged with breaking into the company's computer network, falsifying evidence, and committing perjury for forging an e-mail message to support her charge that she was fired for ending a relationship with the company CEO. Using cell phone records, Oracle lawyers proved that the supervisor who had supposedly fired her and written the e-mail was out of town when the e-mail was written and could not have sent it. The employee was found guilty of forging the e-mail message and faced up to six years in jail.
- *Caller ID spoofing* is displaying an incorrect number (any number the attacker chooses) on a caller ID display to hide the caller's identity.
- *IP address spoofing* is creating Internet Protocol (IP) packets with a forged source IP address to conceal the identity of the sender or to impersonate another computer system. IP spoofing is most frequently used in denial-of-service attacks.
- *Address Resolution Protocol (ARP) spoofing* is sending fake ARP messages to an Ethernet LAN. ARP is a networking protocol for determining a network host's hardware address when only its IP or network address is known. ARP is critical for local area networking as well as for routing internet traffic across gateways (routers). ARP spoofing allows an attacker to associate his *MAC address* (*M*edia *A*ccess *C*ontrol address, a hardware address that uniquely identifies each node on a network) with the IP address of another node. Any traffic meant for the intended IP address is mistakenly sent to the attacker instead. The attacker can sniff the traffic and forward it to its intended target, modify the data before forwarding it (called a man-in-the-middle attack), or launch a denial of service attack.
- *SMS spoofing* is using the short message service (SMS) to change the name or number a text message appears to come from. In Australia, a woman got a call asking why she had sent the caller multiple adult message texts every day for the past few months. Neither she nor her mobile company could explain the texts, as her account showed that they were not coming from her phone. When she realized there was no way of blocking the messages, she changed her mobile number to avoid any further embarrassment by association.
- *Web-page spoofing*, also called phishing, is discussed later in the chapter.
- *DNS spoofing* is sniffing the ID of a Domain Name System (the "phone book" of the Internet that converts a domain, or Web site name, to an IP address) request and replying before the real DNS server can.

A ***zero-day attack*** (or *zero-hour attack*) is an attack between the time a new software vulnerability is discovered and the time a software developer releases a ***patch*** that fixes the problem. When hackers detect a new vulnerability, they "release it into the wild" by posting it on underground hacker sites. Word spreads quickly, and the attacks begin. It takes companies time to discover the attacks, study them, develop an antidote, release the patch to fix the problem, install the patch on user systems, and update antivirus software. One way software developers minimize the vulnerability window is to monitor known hacker sites so they know about the vulnerability when the hacker community does.

Vulnerability windows last anywhere from hours to forever if users do not patch their system. A national retailing firm employee used the server that clears credit card transactions to download music from an infected Web site. The music contained Trojan horse software that allowed Russian hackers to take advantage of an unpatched, known vulnerability to install software that collected and sent credit card data to 16 different computers in Russia every hour for four months until it was detected.

Cybercrooks take advantage of Microsoft's security update cycle by timing new attacks right before or just after "Patch Tuesday"—the second Tuesday of each month, when the software maker releases its fixes. The term "zero-day Wednesday" describes this strategy.

Cross-site scripting (XSS) is a vulnerability in dynamic Web pages that allows an attacker to bypass a browser's security mechanisms and instruct the victim's browser to execute code thinking it came from the desired Web site. Most attacks use executable JavaScript, although HTML, Flash, or other codes the browser can execute are also used. XSS flaws are the most prevalent flaws in Web applications today and occur anywhere a Web application uses input from a user in the output it generates without validating or encoding it. The likelihood that a site contains XSS vulnerabilities is extremely high. Finding these flaws is not difficult for attackers; there are many free tools available that help hackers find them, create the malicious code, and inject it into a target site. Many prominent sites have had XSS attacks, including Google, Yahoo, Facebook, MySpace, and MediaWiki. In fact, MediaWiki has had to fix over 30 XSS weaknesses to protect Wikipedia.

An example of how XSS works follows. Luana hosts a Web site that Christy frequently uses to store all her financial data. To use the Web site, Christy logs on using her username and password. While searching for vulnerable Web sites, Miles finds that Luana's Web site has an XSS vulnerability. Miles creates a URL to exploit it and sends it to Christy in an e-mail that motivates Christy to click on it while logged into Luana's Web site. The XSS vulnerability is exploited when the malicious script embedded in Miles's URL executes in Christy's browser, as if it came directly from Luana's server. The script sends Christy's session cookie to Miles, who hijacks Christy's session. Miles can now do anything Christy can do. Miles can also send the victim's cookie to another server, inject forms that steal Christy's confidential data, disclose her files, or install a Trojan horse program on her computer. Miles can also use XSS to send a malicious script to her husband Jeremy's computer. Jeremy's browser has no way of knowing that the script should not be trusted; it thinks it came from a trusted source and executes the script.

Miles could also execute XSS by posting a message with the malicious code to a social network. When Brian reads the message, Miles's XSS will steal his cookie, allowing Miles to hijack Brian's session and impersonate him.

Attempting to filter out malicious scripts is unlikely to succeed, as attackers encode the malicious script in hundreds of ways so it looks less suspicious to the user. The best way to protect against XSS is HTML sanitization, which is a process of validating input and only allowing users to input predetermined characters. Companies also try to identify and remove XSS flaws from a Web application. To find flaws, companies review their code, searching for all the locations where input from an HTTP request could enter the HTML output.

A ***buffer overflow attack*** happens when the amount of data entered into a program is greater than the amount of the memory (the input buffer) set aside to receive it. The input overflow usually overwrites the next computer instruction, causing the system to crash. Hackers exploit this buffer overflow by carefully crafting the input so that the overflow contains code that tells the computer what to do next. This code could open a back door into the system, provide the attacker with full control of the system, access confidential data, destroy or harm system components, slow system operations, and carry out any number of other inappropriate acts. Buffer overflow exploits can occur with any form of input, including mail servers, databases, Web servers, and ftps. Many exploits have been written to cause buffer overflows. The Code Red worm used a buffer overflow to exploit a hole in Microsoft's Internet Information Services.

In an ***SQL injection (insertion)*** attack, malicious code in the form of an SQL query is inserted into input so it can be passed to and executed by an application program. The idea is to convince the application to run SQL code that it was not intended to execute by exploiting a database vulnerability. It is one of several vulnerabilities that can occur when one programming language is embedded inside another. A successful SQL injection can read sensitive data from the database; modify, disclose, destroy, or limit the availability of the data; allow the attacker to become a database administrator; spoof identity; and issue operating system commands. An SQL injection attack can have a significant impact that is limited only by the attacker's skill and imagination and system controls.

Albert Gonzalez used SQL injection techniques to create a back door on corporate systems. He then used packet sniffing and ARP spoofing attacks to steal data on more than 170 million credit cards. His $200 million fraud was the largest such fraud in history. He was sentenced to 20 years in prison, the harshest computer crime sentence in American history. Like most fraud perpetrators, he spent his ill-gotten gains on a Miami condominium, an expensive car, Rolex watches, and a Tiffany ring for his girlfriend. He threw himself a $75,000 birthday party and stayed in lavish hotels and resorts. He even complained about having to count $340,000 by hand after his currency-counting machine broke.

As shown in Figure 6-1, a ***man-in-the-middle (MITM) attack*** places a hacker between a client and a host and intercepts network traffic between them. An MITM attack is often called a

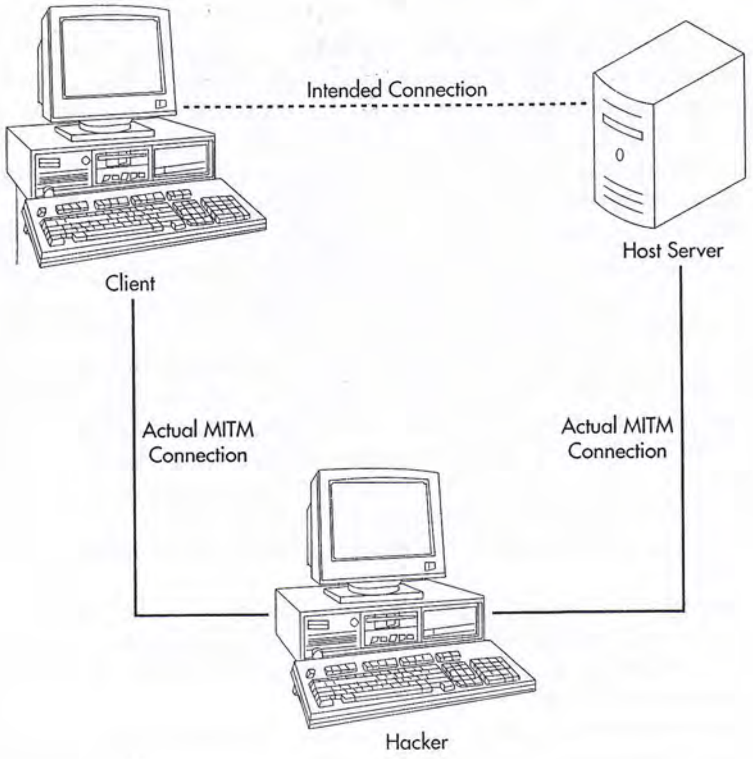


FIGURE 6-1
A Man-in-the Middle Cyber Attack

session hijacking attack. MITM attacks are used to attack public-key encryption systems where sensitive and valuable information is passed back and forth. For example, Linda sniffs and eavesdrops on a network communication and finds David sending his public key to Teressa so that they can communicate securely. Linda substitutes her forged public key for David's key and steps in the middle of their communications. If Linda can successfully impersonate both David and Teressa by intercepting and relaying the messages to each other, they believe they are communicating securely. Once an MITM presence is established, the hacker can read and modify client messages, mislead the two parties, manipulate transactions, and steal confidential data. To prevent MITM attacks, most cryptographic protocols authenticate each communication endpoint. Many of the spoofing techniques discussed in the chapter are used in MITM attacks.

Masquerading or ***impersonation*** is pretending to be an authorized user to access a system. This is possible when the perpetrator knows the user's ID number and password or uses her computer after she has logged in (while the user is in a meeting or at lunch).

Piggybacking has several meanings:

1. The clandestine use of a neighbor's Wi-Fi network; this can be prevented by enabling the security feature in the wireless network.
2. Tapping into a telecommunications line and electronically latching onto a legitimate user before the user enters a secure system; the legitimate user unknowingly carries the perpetrator into the system.
3. An unauthorized person following an authorized person through a secure door, bypassing physical security controls such as keypads, ID cards, or biometric identification scanners.

Password cracking is penetrating a system's defenses, stealing the file containing valid passwords, decrypting them, and using them to gain access to programs, files, and data. A police officer suspected his wife of an affair and believed the lovers communicated by e-mail. He asked a former police officer to break into his wife's password-protected corporate e-mail account and print her e-mails. The hacker used a wireless access point to penetrate the network and download her e-mail. It took three days to crack her password and confirm the husband's suspicions.

War dialing is programming a computer to dial thousands of phone lines searching for dial-up modem lines. Hackers hack into the PC attached to the modem and access the network to which it is connected. This approach got its name from the movie *War Games*. Much more problematic in today's world is ***war driving***, which is driving around looking for unprotected wireless networks. One enterprising group of researchers went ***war rocketing***. They used rockets to let loose wireless access points attached to parachutes that detected unsecured wireless networks in a 50-square-mile area.

Phreaking is attacking phone systems to obtain free phone line access or using phone lines to transmit viruses and to access, steal, and destroy data. One telephone company lost $4.5 million in three days when details on how to use its phone lines for free were published on the Internet. Phreakers also break into voice mail systems, as the New York Police Department learned. The hackers changed the voice mail greeting to say that officers were too busy drinking coffee and eating doughnuts to answer the phone and to call 119 (not 911) in case of an emergency. The owner of two small voice-over-IP (VoIP) phone companies hacked into a larger VoIP provider and routed over $1 million of calls through one of his systems. To keep the rerouting from being discovered, they broke into a New York firm's system, set up a server, and made it look like the calls came from many third parties. Other hackers have hijacked calls, rerouted them to their own call centers, and asked callers to identify themselves by divulging confidential information. To protect a system from phreakers, companies use a voice firewall that scans inbound and outbound voice traffic, terminates any suspicious activity, and provides real-time alerts.

Data diddling is changing data before, during, or after it is entered into the system in order to delete, alter, add, or incorrectly update key system data. A clerk for a Denver brokerage altered a transaction to record 1,700 shares of Loren Industries stock worth $2,500 as shares in Long Island Lighting worth more than $25,000.

Data leakage is the unauthorized copying of company data. Ten Social Security employees stole 11,000 Social Security numbers and other identifying information and sold them to identity theft fraudsters. Acxiom suffered a data loss when, over a year and a half, an individual used a company's ftp client to steal 8.2 GB of data. ***Podslurping*** is using a small device with storage capacity, such as an iPod or Flash drive, to download unauthorized data. Security expert Abe Usher created slurp.exe and copied all document files from his computer in 65 seconds. Usher now makes a version of his program for security audits that does not copy files but generates a report of the information that could have been stolen in a real attack.

The ***salami technique*** is used to embezzle money a "salami slice" at a time from many different accounts. A disgruntled employee programmed the company computer to increase all production costs by a fraction of a percent and place the excess in the account of a dummy vendor he controlled. Every few months, the fraudulent costs were raised another fraction of a percent. Because all expenses were rising together, no single account would call attention to the fraud. The perpetrator was caught when a teller failed to recognize the payee name on a check the perpetrator was trying to cash. The salami scheme was part of the plot line in several films, including *Superman III, Hackers*, and *Office Space*.

One salami technique has been given a name. In a ***round-down fraud***, all interest calculations are truncated at two decimal places and the excess decimals put into an account the perpetrator controls. No one is the wiser, since all the books balance. Over time, these fractions of a cent add up to a significant amount, especially when interest is calculated daily.

Economic espionage is the theft of information, trade secrets, and intellectual property. Losses are estimated to total $250 billion a year, with losses increasing by 323% during one five-year period. Almost 75% of losses are to an employee, former employee, contractor, or supplier. The FBI is investigating about 800 separate incidents of economic espionage at any point in time. Reuters Analytics allegedly broke into the computers of Bloomberg, a competitor, and stole code that helps financial institutions analyze stock market data. Toshiba paid $465 million to Lexar Media as compensation for trade secrets provided by a member of Lexar's board of directors.

Cyber-extortion is threatening to harm a company or a person if a specified amount of money is not paid. The owner of a credit card processor received an e-mail listing his clients as well as their credit card numbers. The e-mail told him to pay $50,000 in six payments, or the data would be sent to his clients. An investigation showed that his system had been successfully penetrated and that customer data had been copied. Not believing the attacker, the owner did nothing. The extortionists released the data, and he spent weeks trying to reassure his irate customers. His efforts were futile; his customers abandoned him, and within six months, he shut down his business. Diana DeGarmo, the runner-up from the third season of *American Idol*, was stalked by an obsessive fan who wanted to "become" Diana. The fan broke into Diana's MySpace account, stole her identity, and sent e-mails to her friends and fans. The fan phoned, e-mailed, and texted Diana more than a hundred times a day. When Diana finally asked her what she wanted, she replied that she wanted $1 million.

Cyber-bullying is using the Internet, cell phones, or other communication technologies to support deliberate, repeated, and hostile behavior that torments, threatens, harasses, humiliates, embarrasses, or otherwise harms another person. Cyber-bullying is especially prevalent among young people; research shows that almost half of all teens and preteens report some form of cyber-bullying. ***Sexting*** is exchanging explicit text messages and revealing pictures. One particularly degrading form of cyber-bullying is posting or sharing these pictures and messages with people who were never intended to see or read them. Anyone involved in transmitting nude pictures of someone under the age of 18 can be charged with dealing in child pornography. Legislation penalizing cyber-bullying has been passed in many states.

Internet terrorism is the act of disrupting electronic commerce and harming computers and communications. A Massachusetts man hired hackers to attack the WeaKnees.com Web site because WeaKnees turned down a business deal with him. The six-week-long attack used a botnet of 10,000 hijacked computers and caused $2 million in damage.

Internet misinformation is using the Internet to spread false or misleading information. McDonald's spent seven years fighting false accusations on Web sites. After 313 days of testimony and a cost of $16 million, McDonald's won and was awarded $94,000. A Web site mocked the verdict, called its campaign "unstoppable," and set up shop under a new name. Another form of Internet misinformation is pretending to be someone else and posting Web-based messages that damage the reputation of the impersonated person. Even subtler is entering bogus information in legitimate news stories. One young man broke into Yahoo's news pages and replaced the name of an arrested hacker with that of Bill Gates.

Perpetrators also send unsolicited ***e-mail threats***. Global Communications sent messages threatening legal action if an overdue amount was not paid within 24 hours. The court action could be avoided by calling an 809 area code (the Caribbean). Callers got a clever recording that responded to the caller's voice. The responses were designed to keep callers on the phone as long as possible because they were being billed at $25 per minute.

Internet auction fraud is using an Internet auction site to defraud another person. According to the FBI, 45% of the complaints they receive are about Internet auction fraud. Internet auction fraud can take several forms. For example, a seller can use a false identity or partner with someone to drive up the bid price. A person can enter a very high bid to win the auction and then cancel his bid, allowing his partner, who has the next highest, and much lower, bid to win. The seller can fail to deliver the merchandise, or the buyer can fail to make the agreed-upon payment. The seller can deliver an inferior product or a product other than the one sold. In a recent case, three art dealers were convicted of casting bids in over 1,100 of each other's eBay auctions to drive up the price of their merchandise over a five-year period. Many of the 120 defrauded consumers paid thousands of dollars more than they would have without the fake bids.

Internet pump-and-dump fraud is using the Internet to pump up the price of a stock and then selling it. Pump-and-dump fraudsters do three things. First, they buy a significant number of shares in small, low-priced, thinly traded penny stocks without driving up their price. Second, they use spam e-mails, texts, Tweets, and Internet postings to disseminate overly optimistic or false information about the company to create a buying frenzy that drives up the stock price. Third, they sell their shares to unsuspecting investors at inflated prices and pocket a handsome profit. Once they stop touting the stock, its price crumbles, and investors lose their money. In a recent fraud, fraudsters quietly acquired shares in 15 thinly traded public companies. They used sophisticated hacking and identity fraud techniques, such as installing keystroke-logging software on computers in hotel business centers and Internet cafes, to gain access to online brokerage accounts. The hackers sold the securities in those accounts, used the money to purchase large quantities of stock of the 15 companies to pump up the share prices of those companies, and sold their stock for a $732,941 profit. The pump-and-dump operation, which was perpetrated in a few hours, cost U.S. brokerage firms an estimated at $2 million.

Companies advertising online pay from a few cents to over $10 for each click on their ads. ***Click fraud*** is manipulating click numbers to inflate advertising bills. Examples include

(1) companies clicking on a competitor's ad to drive up their advertising costs, (2) Web page owners who get a commission to host a pay-per-click ad clicking to boost commissions, and (3) ad agencies inflating the number of clicks to make an ad campaign appear more effective. Most click fraudsters are cyber criminals who create Web sites with nothing on them but ads and use their botnets to repeatedly click on the ads. As many as 30% of all clicks are not legitimate. That is no small sum, given that total revenues from online advertising exceed $15 billion dollars a year.

Web cramming is offering a free Web site for a month, developing a worthless Web site, and charging the phone bill of the people who accept the offer for months, whether they want to continue using the Web site or not. Web cramming has been in the top ten of online scams for the past few years, and there are no signs that it is going away. Law enforcement has cracked down on this for the past few years with no apparent permanent success.

Software piracy is the unauthorized copying or distribution of copyrighted software. Software piracy usually takes one of three forms: (1) selling a computer with pre-loaded illegal software, (2) installing a single-license copy on multiple machines, and (3) loading software on a network server and allowing unrestricted access to it in violation of the software license agreement.

It is estimated that for every legal software sale, between seven and eight illegal copies are made. Within days of being released, most new software is on the Internet and available free to those who want to download it illegally. An estimated 43% of software is pirated; in some countries, over 90% is pirated. The software industry estimates the economic losses due to software piracy exceed $50 billion a year.

The Business Software Alliance, which files lawsuits against software pirates, found 1,400 copies of unlicensed software at an adult vocational school in Los Angeles and claimed $5 million in damages. Individuals convicted of software piracy are subject to fines of up to $250,000 and jail terms of up to five years. However, they are often given more creative punishments. A Puget Sound student was required to write a 20-page paper on the evils of software piracy and copyright infringement and perform 50 hours of community service wiring schools for Internet usage. Failure to comply would subject him to a $10,000 fine and a copyright infringement lawsuit.

Social Engineering

Social engineering refers to techniques or psychological tricks used to get people to comply with the perpetrator's wishes in order to gain physical or logical access to a building, computer, server, or network—usually to get the information needed to access a system for the purpose of obtaining confidential data. Often, the perpetrator has a conversation with someone to trick, lie to, or otherwise deceive the victim. Often the perpetrator has information, knowledge, authority, or confidence that makes it appear that he belongs or knows what he is doing.

Establishing the following policies and procedures—and training people to follow them—can help minimize social engineering:

1. Never let people follow you into a restricted building.
2. Never log in for someone else on a computer, especially if you have administrative access.
3. Never give sensitive information over the phone or through e-mail.
4. Never share passwords or user IDs.
5. Be cautious of anyone you do not know who is trying to gain access through you.

The remainder of this section discusses various social engineering issues and techniques.

Identity theft is assuming someone's identity, usually for economic gain, by illegally obtaining and using confidential information, such as a Social Security number or a bank account or credit card number. Identity thieves empty bank accounts, apply for credit cards, run up large debts, and take out mortgages and loans. By carefully covering his tracks and having all bills sent to an address he controls, the identity thief can prolong the scheme because the victim will not know what is happening until considerable damage has been caused. Victims can usually prove they are not responsible for the debts or missing funds, but it takes significant time to clean up credit records and restore reputations.

A convicted felon incurred $100,000 of credit card debt, took out a home loan, purchased homes and consumer goods, and filed for bankruptcy in the victim's name. He phoned and mocked his victim because the victim could not do anything, because identity theft was not a crime at the time. The victim spent four years and $15,000 to restore his credit and reputation. The identity thief served a brief sentence for lying while buying a gun and did not have to make restitution. This and similar cases resulted in Congress making identity theft a federal offense in 1998.

Pretexting is using an invented scenario (the pretext) to increase the likelihood that a victim will divulge information or do something. The pretext is more than a just simple lie; it usually involves creating legitimacy in the target's mind that makes impersonation possible. Pretexters conduct a security survey and lull the victim into disclosing confidential information by asking 10 innocent questions before asking the confidential ones. They call help desks and claim to be an employee who has forgotten a password. They call users and say they are testing the system and need a password. They pose as buyers, prospective employees, or salespeople to get plant tours and obtain information that may help them break into the system. They use voice-changing devices to make a male voice sound like a female voice or use spoofing devices to make it appear they are phoning from the intended victim's phone.

The chairwoman of Hewlett-Packard was forced to resign after H-P hired a private investigator to catch H-P directors who had leaked confidential information to reporters. The private investigator pretended to be someone he was not to get private phone records and other confidential information of directors and journalists. As a result, Congress passed a bill making the use of pretexting to obtain a person's phone records illegal.

A hacker tricked a T-Mobile employee into disclosing the information needed to hack into Paris Hilton's phone by answering the question "What is your favorite pet's name?" Tinkerbell, the name of her dog, was well known. The hacker accessed her phone and posted the contents of her address book, notes, and some very embarrassing photos on the Internet.

Posing is creating a seemingly legitimate business (often selling new and exciting products), collecting personal information while making a sale, and never delivering the product. Fraudsters also create Internet job listing sites to collect confidential information.

Phishing is sending an electronic message pretending to be a legitimate company, usually a financial institution, and requesting information or verification of information and often warning of some dire consequence if it is not provided. The recipient is asked to respond to the bogus request or visit a Web page and submit data. The message usually contains a link to a Web page that appears legitimate. The Web page has company logos, familiar graphics, phone numbers, and Internet links that appear to be those of the victimized company. It also has a form requesting everything from a home address to an ATM card's PIN. Phishers are becoming more sophisticated. Early phishing scams sent messages to everyone. Targeted versions of phishing, called spear phishing, have emerged that target known customers of a specific company.

In the early days, each phishing e-mail resulted in tens of thousands of calls to bank call centers, disrupted business, and cost hundreds of thousands of dollars to handle the deluge of calls. An estimated 2 million Americans have been fooled by phishing scams, with yearly losses exceeding $3.2 billion.

It is easy to launch a phishing attack because hackers sell kits that lead people through the process. Some phishing e-mails secretly install software that spies on or hijacks the user's computer. The software captures log-on names or takes pictures of the user's screen when he logs into his financial institution.

The IRS has set up a Web site and an e-mail address (phishing@irs.gov) where people can forward suspicious e-mails that purport to be from the IRS. In a recent IRS phishing attack, e-mail recipients were told that they were due a refund and were directed to a Website that looked just like the IRS Web site and contained forms that looked just like IRS forms. To claim the refund, the taxpayer had to enter confidential information that facilitated identity theft.

Voice phishing, or ***vishing***, is like phishing except that the victim enters confidential data by phone. Perpetrators use Voice over Internet Protocol (VoIP) to spoof the legitimate phone number (caller ID shows they are calling their financial institution) and to detect the telephone keystrokes.

To avoid being phished or vished, be highly skeptical of any message that suggests you are the target of illegal activity. Ignore e-mails that request confidential information, and do not call a number given in an unsolicited message. If you are concerned, call the institution using a number you know is valid to ensure that account information has not been tampered with.

Carding refers to activities performed on stolen credit cards, including making a small online purchase to determine whether the card is still valid and buying and selling stolen credit card numbers. Scores of underground Web sites facilitate carding, with some rating the reliability of sellers the same way eBay does. Cyber-criminal gangs run many of the carding sites.

Pharming is redirecting Web site traffic to a spoofed Web site. If you could change XYZ Company's number in the phone book to your phone number, people using the phone book to call XYZ Company would reach you instead. Similarly, each Web site has a unique IP (Internet) address (four groupings of numbers separated by three periods). There is a Domain Name System (think phone book) that converts a domain (Web site) name to an IP address. Pharmers change the IP address in the Domain Name System (DNS) to an IP address they control. Compromised DNS servers are referred to as "poisoned."

Malware can also be used to change a computer's host file (internal DNS) or an Internet service provider's IP addresses. Because most PCs are not as well controlled, they are better targets for pharming than Internet servers. Once these files are poisoned, all subsequent requests to visit that Web site are directed to the spoofed site.

Pharming is a very popular social engineering tool for two reasons. First, it is difficult to detect because the user's browser shows the correct Web site. Antivirus and spyware removal software are currently ineffective protections against pharming. Instead, complicated anti-pharming techniques are required. Second is the ability to target many people at a time through domain spoofing rather than one at a time with phishing e-mails.

A recent pharming attack targeted 65 financial firms, including PayPal, eBay, Discover Card, and American Express. The sophisticated and multi-pronged attack involved thousands of computers, multiple IP addresses in multiple countries, and a flood of fraudulent spam. The two-and-a-half-day pharming attack was so successful, resilient, and hard to correct that it was evident that a professional team planned it. The first e-mail spam contained bogus news that the Australia Prime Minister was struggling for his life after a heart attack. The e-mail contained a link to a newspaper story from *The Australian*. The second e-mail lure had a link to news of a cricket match in Australia. When people clicked on the links, they were redirected to one of five malicious Web sites that infected their computers with pharming malware.

An ***evil twin*** is a wireless network with the same name (called *Service Set Identifier*, or *SSID*) as a legitimate wireless access point. The hacker produces a wireless signal that is stronger than the legitimate signal or disrupts or disables the legitimate access point by disconnecting it, directing a denial-of-service against it, or creating radio frequency interference around it. Users are unaware that they connect to the evil twin. The perpetrator monitors the traffic looking for confidential information. Hackers also use evil twins to unleash a wide variety of malware and to install software to attack other computers. After a small coffee shop advertised free wireless Internet, there was an increase in identity thefts. The police discovered that a man living next to the coffee shop had set up an evil twin and was stealing confidential information.

Typosquatting, or ***URL hijacking***, is setting up similarly named Web sites so that users making typographical errors when entering a Web site name are sent to an invalid site. For example, typing goggle.com instead of google.com might lead to a cyber-squatter site that:

- Tricks the user into thinking she is at the real site because of a copied or a similar logo, Web site layout, or content. These sites often contain advertising that appeals to the person looking for the real domain name. The typosquatter might also be a competitor.
- Is very different from what was wanted. One typosquatter sent people looking for a children's site to a pornographic Web site.
- Distributes malware such as viruses, spyware, and adware.

To stop typosquatting, companies send a cease-and-desist letter to the offender, purchase the Web site address, or file a lawsuit. Google won a case against a Russian typosquatter who registered domain names such as googkle.com and gooigle.com. The lawsuit was decided on three criteria: The domain names were obvious misspellings of google.com, the Russian had no independent claims or interest in the names, and he used the Web sites to infect computers with malware. Google was given possession of the domain names.

To prevent typosquatting, a company (1) tries to obtain all the Web names similar to theirs to redirect people to the correct site, or (2) uses software to scan the Internet and find domains that appear to be typosquatting. Parents can use the same software to restrict access to sites that squat on typos of children's Web sites.

Tabnapping is secretly changing an already open browser tab. Tabnapping begins when a victim is tricked into opening an e-mail link or visiting an infected Web site. The site uses JavaScript to identify a frequently visited site and secretly change the label and contents of the open, but inactive, browser tab. When the victim clicks on the altered tab, it shows that the site has been timed out. When the victim logs back in, the user ID and password are captured and forwarded to the identity thief.

Scavenging, or *dumpster diving*, is gaining access to confidential information by searching documents and records. Some identity thieves search garbage cans, communal trash bins, and city dumps to find information. Oracle Corporation was embarrassed a few years ago when investigators it hired were caught going through the trash of companies that supported its rival, Microsoft. The investigators had paid building janitors $1,200 for the trash. In another instance, Jerry Schneider discovered Pacific Telephone computer operating guides in a trash bin on his way home from high school. Over time, his scavenging activities resulted in a technical library that allowed him to steal $1 million worth of electronic equipment.

In *shoulder surfing*, as its name suggests, perpetrators look over a person's shoulders in a public place to get information such as ATM PIN numbers or user IDs and passwords. Fraudsters also surf from a distance using binoculars or cameras. In South America, a man hid a video camera in some bushes and pointed it at a company president's computer, which was visible through a first-floor window. A significant business acquisition almost fell through because of the information on the videotape. Shoulder surfers can be foiled by blocking the surfer's view of the input device.

In *Lebanese looping*, the perpetrator inserts a sleeve into an ATM that prevents the ATM from ejecting the card. When it is obvious that the card is trapped, the perpetrator approaches the victim and pretends to help, tricking the person into entering her PIN again. Once the victim gives up, the thief removes the card and uses the card and PIN to withdraw as much money as the ATM allows. Lebanese looping is common in any country with a large number of ATMs.

Skimming is double-swiping a credit card in a legitimate terminal or covertly swiping a credit card in a small, hidden, handheld card reader that records credit card data for later use. Commonly committed in retail outlets such as restaurants and carried out by employees with a legitimate reason to possess the victim's cards, skimming losses exceed $1 billion per year. A part-time employee at a gas station skimmed the cards of 80 customers, including the owner, who was a relative, and stole over $200,000.

Chipping is posing as a service engineer and planting a small chip that records transaction data in a legitimate credit card reader. The chip is later removed to access the data recorded on it.

Eavesdropping is listening to private communications or tapping into data transmissions. The equipment needed to set up a wiretap on an unprotected communications line is readily available at local electronics stores. One alleged wiretapping fraud involved Mark Koenig, a 28-year-old telecommunications consultant, and four associates. Federal agents say they pulled crucial data about Bank of America customers from telephone lines and used it to make 5,500 fake ATM cards. Koenig and his friends allegedly intended to use the cards over a long weekend to withdraw money from banks across the country. Authorities were tipped off, and they were apprehended before they could use the cards.

Malware

This section describes ***malware***, which is any software that can be used to do harm. A recent study shows that malware is spread using several simultaneous approaches, including file sharing (used in 72% of attacks), shared access to files (42%), e-mail attachments (25%), and remote access vulnerabilities (24%).

Spyware software secretly monitors and collects personal information about users and sends it to someone else. The information is gathered by logging keystrokes, monitoring Web sites visited, and scanning documents on the computer's hard drive. Spyware can also hijack a browser, replacing a computer's home page with a page the spyware creator wants you to visit. Unless the spyware is removed, resetting a browser home page lasts only until the computer is rebooted. Spyware can also hijack search requests, returning results chosen by the spyware rather than the results desired. Spyware infections, of which users are usually unaware, come from the following:

- Downloads such as file-sharing programs, system utilities, games, wallpaper, screensavers, music, and videos.
- Web sites that secretly download spyware. This is called *drive-by downloading*.
- A hacker using security holes in Web browsers and other software.
- Malware masquerading as anti-spyware security software.
- A worm or virus.
- Public wireless networks. At Kinko's in Manhattan, an employee gathered the data needed to open bank accounts and apply for credit cards in the names of the people using Kinko's wireless network.

Spyware is especially problematic for companies with employees who telecommute or remotely access the network. Spyware on these computers record the user's network interactions, copy corporate data, and introduce spyware to the entire organization. A main source of spyware is adult-oriented sites. The computers of people who visit those sites are infected, and when they log onto their corporate systems those infections are passed to their employer's internal network.

Adware is spyware that pops banner ads on a monitor, collects information about the user's Web-surfing and spending habits, and forwards it to the adware creator. Adware companies charge for each computer showing its ads. They increase the number of computers with adware by paying shareware developers to bundle the adware with their software. This allows shareware developers to make money without charging for their software. One company that engages in digital media content sharing offers users a $30 version or a free version. The license agreement for the free software discloses the adware (hence making it "legal" spyware), but most users do not read the agreement and are not aware it is installed. Reputable adware companies claim sensitive or identifying data are not collected. However, there is no way for users to effectively control or limit the data collected and transmitted.

A recent AOL study found that 80% of inspected computers were infected with spyware, each machine containing on average 93 spyware or adware components. Another study estimated that 90% of computers connected to the Internet had spyware, with 90% of the owners unaware of the infection. The best protection against spyware and adware is a good antispyware software package that neutralizes or eliminates it and prevents its installation. One downside is that after the spyware or adware is erased, the free software that was its host may not work. Use multiple anti-spyware programs; unlike antivirus software and firewalls, they won't conflict.

Some malware developers intentionally make their software difficult to uninstall. Malware companies sometimes battle each other over whose software will infect a computer. Some of them have developed ***torpedo software*** that destroys competing malware, resulting in "malware warfare" between competing developers.

Scareware is software that is often malicious and of little or no benefit that is sold using scare tactics. The most common scare tactic is a dire warning that most computers are infected with viruses, spyware, and other catastrophic problems. Some scareware even warns that a user's job, career, or marriage is at risk. The scareware creators offer a solution—a free computer scan using their fake antivirus software. Accepting the free scan does several things. First, it does not perform a scan. Second, it claims to find dozens of problems and again warns of dire consequences if the computer is not cleaned up. Third, it often introduces into the consumer's computer the very problems that scared the consumer into trying the software. Fourth, it encourages the consumer to buy the fake antivirus software to clean the computer and keep it clean.

Scareware is marketed using spam e-mail and pop-up windows or banners on Web sites, some of which look as though they were placed by big-name corporations. To deceive consumers, the software looks and feels like legitimate security software, the e-mails look like they come from legitimate security software companies, and the pop-ups look like they come from the user's operating system. Scareware scammers also create Web pages about celebrity news and other hot topics that appear at the top of Google search results; clicking on any of the many links on the Web page launches the scareware. Scammers also steal Facebook and Twitter account logons, send messages carrying a tainted Web link to the victim's contacts, and rely on the high trust common to social networks to trick users into launching scareware.

There are tens of thousands of different scareware packages, with the number rising almost 600% in one recent six-month period. In another growth comparison, Microsoft reported that its free Malicious Software Removal Tool cleaned scareware off 7.8 million PCs in one six-month period compared to 5.3 million in the prior six months.

Scareware can be spotted several ways, First, the scare tactics are a big giveaway; legitimate companies will not try to scare you into using their products. A second giveaway is bad English; most scareware comes from countries where English is not the creator's first language.

The Federal Trade Commission sued the perpetrators of a massive scareware scheme that offered fake computer scans that falsely claimed to detect viruses, spyware, system errors, and illegal pornography. They tricked over a million people into spending $1.9 million to buy fake computer security products, including DriveCleaner, XP Antivirus, WinAntivirus, ErrorSafe, and WinFixer.

Like scareware, ***ransomware*** comes in the form of fake antivirus software. When activated, well-written ransomware locks you out of all your programs and data by encrypting them. That means you can't run your installed security programs and, if it disables your USB ports and DVD drives, you can't load new security programs to combat it. It directs Internet Explorer to the perpetrator's Web site, where the victim is informed that a monetary payment made directly to a bank must be made to have the software removed. Since payments can be traced, ransomware is not as common as other malware. Most ransomware is delivered via a spam e-mail that motivates the recipient to open an infected file. It can also be delivered by Web sites. Keeping Windows updated is crucial to blocking these downloads.

Key logging software records computer activity, such as a user's keystrokes, e-mails sent and received, Web sites visited, and chat session participation. Parents use the software to monitor their children's computer usage, and businesses use it to monitor employee activity. Law enforcement uses it to detect or prevent crime. A Drug Enforcement Administration agent persuaded a federal judge to authorize him to sneak into an Escondido, California, office believed to be a front for manufacturing the drug Ecstasy. Copying the contents of all hard drives and installing keystroke loggers successfully thwarted their plans to distribute Ecstasy.

Fraud perpetrators use key loggers to capture and send confidential information. Over 10,000 unique key logging software programs are available in underground chat rooms; most are free or very cheap. Computers are infected with key logging software when they visit corrupt Web sites or download free software. One enterprising student installed key logging software on his teacher's computer, recorded her typed exams answers, and decoded the keystrokes. He was caught trying to sell exam answers to other students.

A ***Trojan horse*** is a set of malicious computer instructions in an authorized and otherwise properly functioning program. Unlike viruses and worms, the code does not try to replicate itself. Some Trojan horses give the creator the power to control the victim's computer remotely. Most Trojan horse infections occur when a user runs an infected program received in an e-mail, visits a malicious Web site, or downloads software billed as helpful add-ons to popular software programs. In Israel, companies were sent business proposals on a disk that contained the Trojan. In another case, visitors to an adult site were told to download a special program to see the pictures. This program disconnected them from their Internet service providers and connected them to a service that billed them $2 a minute until they turned off their computers. Over 800,000 minutes were billed, with some phone bills as high as $3,000, before the scam was detected. The HotLan Trojan caused infected computers to sign up for Microsoft Hotmail and Google Gmail accounts and used them for spamming. Over 514,000 Hotmail accounts and 49,000 Gmail accounts were created in a single day. One type of Trojan horse relies on the curiosity of the victim. The attacker creates a malware-infected CD ROM or USB flash drive, gives it a legitimate looking and curiosity piquing label (company logo, accompanied by 4Q Evaluation and Salary Data), leaves it where it can be found (bathroom, desktop, hallway), and waits for a curious employee to try to read the file. The file installs the Trojan on the employee's computer, likely giving the attacker access to the company's internal computer network.

Time bombs and ***logic bombs*** are Trojan horses that lie idle until triggered by a specified date or time, by a change in the system, by a message sent to the system, or by an event that does not occur. Once triggered, the bomb goes off, destroying programs, data, or both. Disgruntled company insiders who want to get even with their company write many bombs. Anticipating that he would not receive a bonus or new contract, Roger Duronio planted a Trojan horse time bomb at USB PaineWebber. Several weeks after he left the firm, the trigger date of March 4 arrived. His 60 lines of malicious code attacked the company's 2,000 servers and deleted company files just as the stock market opened. The effects were catastrophic. Broker computers were out of commission for days or weeks, depending on how badly the machines were damaged and the existence of branch backup tapes. Some 20% of the computers had no backup tapes, and some servers were never fully restored. Over 400 employees and 200 IBM consultants worked feverishly, at a cost of $3.1 million, to restore the system. Duronio cashed out his IRA and sold UBS stock short, figuring to make a killing when the stock plunged. It never did, and he lost money on his short sale. Duronio was sentenced to eight years in prison.

There are legal uses of time and logic bombs, such as in trial versions of software. The software becomes unusable after a certain amount of time passes or after the software has been used a certain number of times.

A ***trap door***, or ***back door***, is a way into a system that bypasses normal authorization and authentication controls. Programmers create trap doors so they can modify programs during systems development and then remove them before the system is put into operation. The back door can also be created by a virus or worm or by a disgruntled programmer. Anyone who discovers a trap door can enter the program. Security consultants claim that back doors are frequently discovered in organizations. BackOrifice, Netbus, and SubSeven are tools intruders use to gain remote, back door access to systems with Windows software. Jonathan James, the first juvenile sent to prison for hacking, installed a back door into a Department of Defense server, accessed sensitive e-mails, and captured employee usernames and passwords.

Packet sniffers capture data from information packets as they travel over networks. Captured data are examined to find confidential or proprietary information. In Sweden, Dan Egerstad's packet sniffer looked for key words such as *government*, *military*, *war*, *passport*, and *visa*. He intercepted e-mails from embassies and governments, many with visa and passport data.

Steganography is writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects their existence. Steganography messages do not attract attention to themselves, whereas an encrypted message arouses suspicion. ***Steganography programs*** hide data files inside a host file, such as a large image or sound file. The software merges the two files by removing scattered bytes from the host file and replacing them with data from the hidden file. The steganography program password protects the merged file, and the only way to reassemble the hidden file is to key the password into the same steganography program. The host file can still be heard or viewed because human visual and auditory senses are not sensitive enough to pick up the slight decrease in image or sound quality that the hidden file causes. Company employees can merge confidential information with a seemingly harmless file and send it anywhere in the world, where the confidential information is reassembled.

Steganography is used by terrorists, as it is an effective way for a spy to transmit information and receive orders. Some experts believe steganography was one way terrorists communicated in planning the September 11 terrorist attack on the United States. A *USA Today* article alleged that Al-Qaeda operatives sent hundreds of messages hidden in digital photographs sold on eBay.

A ***rootkit*** conceals processes, files, network connections, memory addresses, systems utility programs, and system data from the operating system and other programs. Rootkits often modify the operating system or install themselves as drivers. A rootkit is used to hide the presence of trap doors, sniffers, and key loggers; conceal software that originates a denial-of-service or an e-mail spam attack; and access user names and log-in information. Unlike viruses and worms, rootkits do not spread to other systems. Rootkit software is readily available on the Internet. Several vendors sell programs that detect rootkits, and security vendors include rootkit detection in their antivirus products. When a rootkit is detected, it is better to reinstall the operating system from scratch rather than spend the time and effort to delete it from the system. In a famous instance of rootkit use, Sony music CDs secretly placed a copy-protection rootkit on Windows computers. The software inadvertently opened security holes that allowed viruses to break in. Sony had to recall all CDs that included the software.

Superzapping is the unauthorized use of special system programs to bypass regular system controls and perform illegal acts, all without leaving an audit trail. The technique derives its name from Superzap, a software utility developed by IBM to handle emergencies. The manager of computer operations at a bank was told to use a Superzap program to correct a problem affecting account balances caused by unanticipated problems in changing from one computer system to another. When he discovered he could use the program to make account changes without the usual controls, audits, or documentation, he moved $128,000 into the accounts of several friends. Because the Superzap program left no evidence of data file changes, he was not detected until a customer complained about a shortage in his account.

A computer ***virus*** is a segment of self-replicating, executable code that attaches itself to a file or program. During its replication phase, the virus spreads to other systems when the infected file or program is downloaded or opened by the recipient. Newer viruses can mutate each time they infect a computer, making them more difficult to detect and destroy. Many viruses lie dormant for extended periods without causing damage, except to propagate themselves. In one survey, 90% of respondents said their company was infected with a virus during the prior 12 months.

During the attack phase, triggered by some predefined event, viruses destroy or alter data or programs, take control of the computer, destroy the hard drive's file allocation table, delete or rename files or directories, reformat the hard drive, change the content of files, or keep users from booting the system or accessing data on the hard drive. A virus can intercept and change transmissions, display disruptive images or messages, or cause the screen image to change color or disappear. Many viruses automatically send e-mails, faxes, or text messages with the victim's name as the source. As the virus spreads, it takes up space, clogs communications, and hinders system performance. Computer virus symptoms include computers that will not start or execute; unexpected read or write operations; an inability to save files; long program load times; abnormally large file sizes; slow systems operation; incessant pop-ups; and unusual screen activity, error messages, or file names.

A bad virus attack shut down a bank with 200 servers and 10,000 desktop computers for four days. During the downtime, the bank was locked out of its system, and customer accounts could not be accessed. A firm that specializes in fixing virus attacks eventually restored the system. The Sobig virus, written by Russian hackers, infected an estimated 1 of every 17 e-mails several years ago. The virus took months to write and was released in ever-improving versions. A year later, the MyDoom virus infected 1 in 12 e-mails and did $4.75 billion in damages.

Every day, virus creators send an estimated 1 billion virus-infected e-mail messages. The creators are getting good at making them look authentic. One recent virus came in an e-mail that appeared to come from Microsoft—the Microsoft logo and copyright were included in the message window launched by the virus. The e-mail told the recipient to use the attached patch to fix a security flaw in either Microsoft Internet Explorer or Outlook. Instead, opening the attachment downloaded malicious software that installed a back door allowing the perpetrator to control the computer.

It is estimated that viruses and worms cost businesses over $20 billion a year. A computer system can be protected from viruses by following the guidelines listed in Focus 6-1.

A computer ***worm*** is a self-replicating computer program similar to a virus, with some exceptions:

1. A virus is a segment of code hidden in or attached to a host program or executable file, whereas a worm is a stand-alone program.
2. A virus requires a human to do something (run a program, open a file, etc.) to replicate itself, whereas a worm does not and actively seeks to send copies of itself to other network devices.
3. Worms harm networks (if only by consuming bandwidth), whereas viruses infect or corrupt files or data on a targeted computer.

Worms often reside in e-mail attachments and reproduce by mailing themselves to the recipient's mailing list, resulting in an electronic chain letter. Some recent worms have completely shut down e-mail systems. Worms are not confined to personal computers; thousands of worms infect cell phones each year by jumping from phone to phone over wireless networks.

A worm usually does not live very long, but it is quite destructive while alive. It takes little technical knowledge to create a worm or virus. Many Web sites provide applications that enable unsophisticated users to create worms. One application has been downloaded over 25,000 times.

More recently, MySpace had to go offline to disable a worm that added over 1 million friends to the hacker's site in less than a day. MySpace profiles were also infected by a worm after viewing a

FOCUS 6-1 Keeping Your Computers Virus-Free

Here are some practical suggestions for protecting computers from viruses:

- Install reputable and reliable antivirus software that scans for, identifies, and destroys viruses. Use only one antivirus program; multiple programs conflict with each other.
- Do not fall for ads touting free antivirus software; much of it is fake and contains malware. Some hackers create Web sites stuffed with content about breaking news so that the site appears on the first page of search results. Anyone clicking on the link is confronted with a pop-up with a link to fake antivirus software.
- Do not fall for pop-up notices that warn of horrible threats and offer a free scan of your computer. Although no scan actually takes place, the program reports dozens of dangerous infections and tells you to purchase and download their fake antivirus program to clean them up.
- Make sure that the latest versions of the antivirus programs are used. National City Bank in Cleveland, Ohio, installed some new laptops. The manufacturer and the bank checked the laptops for viruses but did not use the latest antivirus software. A virus spread from the laptop hard drives to 300 network servers and 12,000 workstations. It took the bank over two days to eradicate the virus from all bank systems.
- Scan all incoming e-mail for viruses at the server level as well as at users' desktops.
- Do not download anything from an e-mail that uses noticeably bad English, such as terrible grammar and misspelled words. Real companies hire people to produce quality writing. Many viruses come from overseas perpetrators whose first language is not English.
- All software should be certified as virus-free before you load it into the system. Be wary of software from unknown sources: They may be virus bait—especially if their prices or functionality sound too good to be true.
- Deal only with trusted software retailers.
- Some software suppliers use electronic techniques to make tampering evident. Ask whether the software you are purchasing has such protection.
- Check new software on an isolated machine with virus-detection software. Software direct from the publisher has been known to have viruses.
- Have two backups of all files. Data files should be backed up separately from programs to avoid contaminating backup data.
- If you use flash drives or CDs, do not put them in strange machines; they may become infected. Do not let others use those storage devices on your machine. Scan all new files with antiviral software before any data or programs are copied to your machine.

FOCUS 6-2 "Loafing" on the Job

Although the Internet offers many opportunities to businesses, it also poses a threat in providing employees with the means to "loaf" on the job. *Cyberloafing*, the use of the Internet in the workplace for non-work-related purposes, can result in reduced productivity, increased bandwidth use, and serious damage, such as virus attacks, legal liabilities, lawsuits, and unintentional disclosure of confidential information. Companies can face serious lawsuits if employees post damaging comments in online forums or distribute copyrighted or offensive materials using the company's network. Other examples of "loafing on the job" include replying to personal e-mails, surfing entertainment Web sites, and maintaining personal blogs.

In 2008, a study conducted by researchers at Multimedia University, Malaysia, found that some employees become involved in computer abuse because they are unaware that such behaviors are inappropriate. The study, which involved 393 employees in local companies, documented the lack of awareness among employees on a number of cyberloafing behaviors. More than 10% of the respondents believed the following behaviors were not wrong: online chatting with friends while working (11%); writing and sending personal e-mails at work (17%); using an office computer for personal work (15%); and surfing the Internet for leisure during office hours (13%).

Given these findings, training, policy implementation, and rehabilitation can be beneficial to companies that are interested in curbing such problems. Properly developed, implemented, and communicated policies on computer and Internet use have been proven to reduce cyberloafing in the workplace. Such policies can create awareness among employees about appropriate Internet use and can communicate the company's views on the issue. To reduce cyberloafing that has resulted from employees' dissatisfaction and boredom, companies can also benefit by creating the right work climates and addressing issues relevant to work conditions.

QuickTime video containing malicious software that replaced the links in the user's page with links to a phishing site. The devastating Conficker worm infected 25% of enterprise Window PCs.

Many viruses and worms exploit known software vulnerabilities than can be corrected with a software patch. Therefore, a good defense against them is making sure that all software patches are installed as soon as they are available.

Recent viruses and worms have attacked cell phones and personal electronic devices using text messages, Internet page downloads, and Bluetooth wireless technology. Flaws in Bluetooth applications open the system to attack. ***Bluesnarfing*** is stealing (snarfing) contact lists, images, and other data using Bluetooth. A reporter for TimesOnline accompanied Adam Laurie, a security expert, around London scanning for Bluetooth-compatible phones. Before a Bluetooth connection can be made, the person contacted must agree to accept the link. However, Laurie has written software to bypass this control and identified vulnerable handsets at an average rate of one per minute. He downloaded entire phonebooks, calendars, diary contents, and stored pictures. Phones up to 90 meters away were vulnerable.

Bluebugging is taking control of someone else's phone to make or listen to calls, send or read text messages, connect to the Internet, forward the victim's calls, and call numbers that charge fees. These attacks will become more popular as phones are used to pay for items purchased. When a hacker wants something, all he has to do is bluebug a nearby phone and make a purchase. To prevent these attacks, a bluetooth device can be set to make it hard for other devices to recognize it. Antivirus software for phones is being developed to deal with such problems.

In the future, many other devices—such as home security systems, home appliances, automobiles, and elevators—will be connected to the Internet and will be the target of viruses and worms.

Table 6-1 summarizes, in alphabetical order, the computer fraud and abuse techniques discussed in the chapter.

TABLE 6-1 Computer Fraud and Abuse Techniques

Technique	Description
Address Resolution Protocol (ARP) spoofing	Sending fake ARP messages to an Ethernet LAN. ARP is a computer networking protocol for determining a network host's hardware address when only its IP or network address is known.
Adware	Software that collects and forwards data to advertising companies or causes banner ads to pop up as the Internet is surfed.
Bluebugging	Taking control of a phone to make calls, send text messages, listen to calls, or read text messages.
Bluesnarfing	Stealing contact lists, images, and other data using Bluetooth.
Botnet, bot herders	A network of hijacked computers. Bot herders use the hijacked computers, called zombies, in a variety of Internet attacks.
Buffer overflow attack	Inputting so much data that the input buffer overflows. The overflow contains code that takes control of the computer.
Caller ID spoofing	Displaying an incorrect number on the recipient's caller ID display to hide the identity of the caller.
Carding	Verifying credit card validity; buying and selling stolen credit cards.
Chipping	Planting a chip that records transaction data in a legitimate credit card reader.
Cross-site scripting (XSS) attack	Exploits Web page security vulnerabilities to bypass browser security mechanisms and create a malicious link that injects unwanted code into a Web site.
Cyber-bullying	Using computer technology to harm another person.
Cyber-extortion	Requiring a company to pay money to keep an extortionist from harming a computer or a person.
Data diddling	Changing data before, during, or after it is entered into the system.
Data leakage	Unauthorized copying of company data.
Denial-of-service attack	An attack designed to make computer resources unavailable to its users. For example, so many e-mail messages that the Internet service provider's e-mail server is overloaded and shuts down.
Dictionary attack	Using software to guess company addresses, send employees blank e-mails, and add unreturned messages to spammer e-mail lists.
DNS spoofing	Sniffing the ID of a Domain Name System (server that converts a Web site name to an IP address) request and replying before the real DNS server.
Eavesdropping	Listening to private voice or data transmissions.

(Continued)

TABLE 6-1 Continued

Technique	Description
Economic espionage	The theft of information, trade secrets, and intellectual property.
E-mail threats	Sending a threatening message asking recipients to do something that makes it possible to defraud them.
E-mail spoofing	Making a sender address and other parts of an e-mail header appear as though the e-mail originated from a different source.
Evil twin	A wireless network with the same name as another wireless access point. Users unknowingly connect to the evil twin; hackers monitor the traffic looking for useful information.
Hacking	Unauthorized access, modification, or use of computer systems, usually by means of a PC and a communications network.
Hijacking	Gaining control of someone else's computer for illicit activities.
IP address spoofing	Creating Internet Protocol packets with a forged IP address to hide the sender's identity or to impersonate another computer system.
Identity theft	Assuming someone's identity by illegally obtaining confidential information such as a Social Security number.
Internet auction fraud	Using an Internet auction site to commit fraud.
Internet misinformation	Using the Internet to spread false or misleading information.
Internet terrorism	Using the Internet to disrupt communications and ecommerce.
Internet pump-and-dump fraud	Using the Internet to pump up the price of a stock and then sell it.
Key logger	Using spyware to record a user's keystrokes.
Lebanese looping	Inserting a sleeve into an ATM so that it will not eject the victim's card, pretending to help the victim as a means to discover his or her PIN, and then using the card and PIN to drain the account.
Logic bombs and time bombs	Software that sits idle until a specified circumstance or time triggers it, destroying programs, data, or both.
Malware	Software that can be used to do harm.
Man-in-the-middle (MITM) attack	A hacker placing himself between a client and a host to intercept network traffic; also called *session hijacking*.
Masquerading/impersonation	Accessing a system by pretending to be an authorized user. The impersonator enjoys the same privileges as the legitimate user.
Packet sniffing	Inspecting information packets as they travel the Internet and other networks.
Password cracking	Penetrating system defenses, stealing passwords, and decrypting them to access system programs, files, and data.
Pharming	Redirecting traffic to a spoofed Web site to obtain confidential information.
Phishing	Communications that request recipients to disclose confidential information by responding to an e-mail or visiting a Web site.
Phreaking	Attacking phone systems to get free phone access; using phone lines to transmit viruses and to access, steal, and destroy data.
Piggybacking	1. Clandestine use of someone's Wi-Fi network. 2. Tapping into a communications line and entering a system by latching onto a legitimate user. 3. Bypassing physical security controls by entering a secure door when an authorized person opens it.
Podslurping	Using a small device with storage capacity (iPod, Flash drive) to download unauthorized data from a computer.
Posing	Creating a seemingly legitimate business, collecting personal data while making a sale, and never delivering items sold.
Pretexting	Acting under false pretenses to gain confidential information.
Rootkit	Software that conceals processes, files, network connections, and system data from the operating system and other programs.
Round-down fraud	Truncating interest calculations at two decimal places and placing truncated amounts in the perpetrator's account.
Ransomware	Software that encrypts programs and data until a ransom is paid to remove it.
Salami technique	Stealing tiny slices of money over time.
Scareware	Malicious software of no benefit that is sold using scare tactics.

TABLE 6-1 Continued

Technique	Description
Scavenging/dumpster diving	Searching for confidential information by searching for documents and records in garbage cans, communal trash bins, and city dumps
Sexting	Exchanging explicit text messages and pictures.
Shoulder surfing	Watching or listening to people enter or disclose confidential data.
Skimming	Double-swiping a credit card or covertly swiping it in a card reader that records the data for later use.
SMS spoofing	Using short message service (SMS) to change the name or number a text message appears to come from.
Social engineering	Techniques that trick a person into disclosing confidential information.
Software piracy	Unauthorized copying or distribution of copyrighted software.
Spamming	E-mailing an unsolicited message to many people at the same time.
Splog	A spam blog that promotes Web sites to increase their Google PageRank (how often a Web page is referenced by other pages).
Spyware	Software that monitors computing habits and sends that data to someone else, often without the user's permission.
Spoofing	Making electronic communications look like someone else sent it.
SQL injection attack	Inserting a malicious SQL query in input in such a way that it is passed to and executed by an application program.
Steganography	Hiding data from one file inside a host file, such as a large image or sound file.
Superzapping	Using special software to bypass system controls and perform illegal acts.
Tabnapping	Secretly changing an already open browser tab using JavaScript.
Trap door	A back door into a system that bypasses normal system controls.
Trojan horse	Unauthorized code in an authorized and properly functioning program.
Typosquatting/URL hijacking	Web sites with names similar to real Web sites; users making typographical errors are sent to a site filled with malware.
Virus	Executable code that attaches itself to software, replicates itself, and spreads to other systems or files. Triggered by a predefined event, it damages system resources or displays messages.
Vishing	Voice phishing, in which e-mail recipients are asked to call a phone number that asks them to divulge confidential data.
War dialing	Dialing phone lines to find idle modems to use to enter a system, capture the attached computer, and gain access to its network(s).
War driving/rocketing	Looking for unprotected wireless networks using a car or a rocket.
Web cramming	Developing a free and worthless trial-version Web site and charging the subscriber's phone bill for months even if the subscriber cancels.
Web-page spoofing	Also called *phishing*.
Worm	Similar to a virus; a program rather than a code segment hidden in a host program. Actively transmits itself to other systems. It usually does not live long but is quite destructive while alive.
Zero-day attack	Attack between the time a software vulnerability is discovered and a patch to fix the problem is released.

Summary and Case Conclusion

It took RPC two days to get its system back up to the point that the audit team could continue their work. RPC had been hit with multiple problems at the same time. Hackers had used packet sniffers and eavesdropping to intercept a public key RPC had sent to Northwest. That led to a man-in-the-middle attack, which allowed the hacker to intercept all communications about the pending merger. It also opened the door to other attacks on both systems.

Law enforcement was called into investigate the problem, and they were following up on three possibilities. The first was that hackers had used the intercepted information to purchase stock in both companies, leak news of the purchase to others via Internet chat rooms, and, once the stock price had been pumped up, to dump the stock of both companies. There did seem to be significant, unusual trading in the two companies' stock in the last few months. The second possibility was hackers exploiting system weaknesses they had found, stealing confidential data on RPC's customers, and causing considerable harm when they were done to cover their tracks. The third possibility was economic espionage and Internet terrorism. They received an anonymous tip that one of Northwest's competitors was behind the attack. It would take weeks or even months to track down all the leads and determine who had caused the problem and why.

Jason's research helped him understand the many ways outside hackers and employees attack systems. He never knew there were so many different things that could be spoofed in systems. He was also intrigued by some of the more technical attacks, such as cross-site scripting, buffer overflow attacks, man-in-the middle attacks, zero-day attacks, and SQL injection. He also found it interesting to learn about all the ways that people use computers to defraud other individuals and companies: Internet terrorism, misinformation, and auction fraud as well as cyber-bullying and cyber-extortion.

Jason was familiar with some of the social engineering techniques he read about, such as pretexting, posing, pharming, and phishing. However, he was unfamiliar with many of the techniques such as Lebanese looping, evil twin, chipping, and typosquatting. He had a similar experience when learning about malware. He was familiar with spyware, adware, Trojan horses, viruses, and key loggers. He learned many new things when he read about scareware, ransomware, steganography, rootkits, and bluebugging.

Jason's research also gave him a perspective on past and future uses of computer fraud and abuse techniques. He learned that many hacker attacks use more than one technique. For example, hackers often send spam e-mails that lure the victim to a Web site that downloads either a keylogger software or code that hijacks the computer and turns it into a botnet zombie or tries to trick the user into disclosing confidential information.

He also learned that hackers take advantage of people who share personal information on social networking sites. For example, a recent worm-based phishing attack targeted Twitter and Facebook users. Users received a message from a friend telling them they could accumulate more friends by clicking on a link. They were prompted to enter their account information, which was used to send the same message to all their friends.

With the harvested personal information that makes them more targeted than before, cyber attacks are increasingly successful in tricking even savvy users into making a mistake. For example, past phishing attacks used a generic spam e-mail message that was obviously bogus. Newer attacks use current-events issues or hot-button topics. Clicking on the accompanying links automatically downloads botware software. Attacks that are even more sophisticated use information about the intended target to make them look legitimate. For example, the e-mail may use stolen information, such as the victim's employer or a friend of family member, to induce them to open an attachment or visit a Web site.

Lastly, Jason learned there is a plethora of fraud software on the market and that hackers compete to make the most easy-to-use tools. In a recent month, six different Web exploit vendors released new products at the same time. As a result, hackers do not need to be programmers; they just need to know to whom they want to target and check a few boxes. For example, with Zeus, one of the most popular and successful data-stealing toolkits, cyber criminals can generate detailed reports on each Web site visited. They can also use the program's powerful search engine to browse through their victims' machines and find detailed information, such as which banks they use. Conversely, the best hackers are more knowledgeable than in the past and use sophisticated technologies. For example, zombies on a botnet used an automated SQL injection attack to compromise over 500,000 Web sites last year, stealing sensitive information and injecting malware into the site.

Key Terms

hacking 169
botnet 170
hijacking 170
bot herder 170
zombie 170
denial-of-service (DoS) attack 170
spamming 170
dictionary attack 170
splog 170
spoofing 171
e-mail spoofing 171

caller ID spoofing 171
IP address spoofing 171
Address Resolution Protocol (ARP) spoofing 171
MAC address 171
SMS spoofing 171
Web-page spoofing 171
DNS spoofing 171
zero-day attack 171
patch 171
cross-site scripting (XSS) 171
buffer overflow attack 172
SQL injection (insertion) 172
man-in-the-middle (MITM) attack 172
masquerading/impersonation 173
piggybacking 173
password cracking 173
war dialing 173
war driving 174
war rocketing 174
phreaking 174
data diddling 174
data leakage 174
podslurping 174
salami technique 174
round-down fraud 174
economic espionage 174
cyber-extortion 174
cyber-bullying 175
sexting 175
Internet terrorism 175
Internet misinformation 175
e-mail threats 175
Internet auction fraud 175
Internet pump-and-dump fraud 175
click fraud 175
Web cramming 176
software piracy 176
social engineering 176
identity theft 176
pretexting 177
posing 177
phishing 177
vishing 177
carding 178
pharming 178
evil twin 178
typosquatting/URL hijacking 178
tabnapping 179
scavenging/dumpster diving 179
shoulder surfing 179
Lebanese looping 179
skimming 179
chipping 179
eavesdropping 179
malware 179
spyware 179
adware 180
torpedo software 180
scareware 180
ransomware 181
key logging software 181
Trojan horse 181
time bomb/logic bomb 181
trap door/back door 182
packet sniffers 182
steganography programs 182
rootkit 182
superzapping 182
virus 183
worm 183
bluesnarfing 185
bluebugging 185

AIS IN ACTION

Chapter Quiz

1. A set of instructions to increase a programmer's pay rate by 10% is hidden inside an authorized program. It changes and updates the payroll file. What is this computer fraud technique called?

a. virus
b. worm
c. trap door
d. Trojan horse

2. Which computer fraud technique involves a set of instructions hidden inside a calendar utility that copies itself each time the utility is enabled until memory is filled and the system crashes?

a. logic bomb
b. trap door
c. virus
d. Trojan horse

3. Interest calculations are truncated at two decimal places, and the excess decimals are put into an account the perpetrator controls. What is this fraud called?

a. typosquatting
b. URL hijacking
c. chipping
d. round-down fraud

4. A perpetrator attacks phone systems to obtain free phone line access or uses telephone lines to transmit viruses and to access, steal, and destroy data. What is this computer fraud technique called?

a. phishing
b. phreaking
c. pharming
d. vishing

5. Fraud perpetrators threaten to harm a company if it does not pay a specified amount of money. What is this computer fraud technique called?
   a. cyber-terrorism
   b. blackmailing
   c. cyber-extortion
   d. scareware

6. Techniques used to obtain confidential information, often by tricking people, are referred to as what?
   a. pretexting
   b. posing
   c. social engineering
   d. identity theft

7. What type of software secretly collects personal information about users and sends it to someone else without the user's permission?
   a. rootkit
   b. torpedo software
   c. spyware
   d. malware

8. What type of software conceals processes, files, network connections, memory addresses, systems utility programs, and system data from the operating system and other programs?
   a. rootkit
   b. spyware
   c. malware
   d. adware

9. Which type of computer attack takes place between the time a software vulnerability is discovered and the time software developers release a software patch that fixes the problem?
   a. posing
   b. zero-day attack
   c. evil twin
   d. software piracy

10. Someone redirects a Web site's traffic to a bogus Web site, usually to gain access to personal and confidential information. What is this computer fraud technique called?
    a. vishing
    b. phishing
    c. pharming
    d. phreaking

Discussion Questions

6.1. When U.S. Leasing (USL) computers began acting sluggishly, computer operators were relieved when a software troubleshooter from IBM called. When he offered to correct the problem they were having, he was given a log-on ID and password. The next morning, the computers were worse. A call to IBM confirmed USL's suspicion: Someone had impersonated an IBM repairman to gain unauthorized access to the system and destroy the database. USL was also concerned that the intruder had devised a program that would let him get back into the system even after all the passwords were changed. What techniques might the impostor have employed to breach USL's internal security? What could USL do to avoid these types of incidents in the future?

6.2. What motives do people have for hacking? Why has hacking become so popular in recent years? Do you regard it as a crime? Explain your position.

6.3. The UCLA computer lab was filled to capacity when the system slowed and crashed, disrupting the lives of students who could no longer log into the system or access data to prepare for finals. IT initially suspected a cable break or an operating system failure, but diagnostics revealed nothing. After several frustrating hours, a staff member ran a virus detection program and uncovered a virus on the lab's main server. The virus was eventually traced to the computers of unsuspecting UCLA students. Later that evening, the system was brought back online after infected files were replaced with backup copies. What conditions made the UCLA system a potential breeding ground for the virus? What symptoms indicated that a virus was present?

Problems

6.1. A few years ago, news began circulating about a computer virus named Michelangelo that was set to "ignite" on March 6, the birthday of the famous Italian artist. The virus attached itself to the computer's operating system boot sector. On the magical date, the virus would release itself, destroying all of the computer's data. When March 6 arrived, the virus did minimal damage. Preventive techniques limited the damage to isolated personal and business computers. Though the excitement surrounding the virus was largely illusory, Michelangelo helped the computer-using public realize its systems' vulnerability to outside attack.

Required

a. What is a computer virus? Cite at least three reasons why no system is completely safe from a computer virus.
b. Why do viruses represent a serious threat to information systems? What damage can a virus do to a computer system?
c. How does a virus resemble a Trojan horse?
d. What steps can be taken to prevent the spread of a computer virus?

6.2. The controller of a small business received the following e-mail with an authentic-looking e-mail address and logo:

From: *Big Bank [antifraud@bigbank.com]*
To: *Justin Lewis, Controller, Small Business USA*
Subject: *Official Notice for all users of Big Bank!*

Due to the increased incidence of fraud and identity theft, we are asking all bank customers to verify their account information on the following Web page: www.antifraudbigbank.com

Please confirm your account information as soon as possible. Failure to confirm your account information will require us to suspend your account until confirmation is made.

A week later, the following e-mail was delivered to the controller:

From: *Big Bank [antifraud@bigbank.com]*
To: *Justin Lewis, Controller, Small Business USA*
Subject: *Official Notice for all users of Big Bank!*

Dear Client of Big Bank,
Technical services at Big Bank is currently updating our software. Therefore, we kindly ask that you access the website shown below to confirm your data. Otherwise, your access to the system may be blocked.
web.da-us.bigbank.com/signin/scripts/login2/user_setup.jsp
We are grateful for your cooperation.

Required

a. What should Justin do about these e-mails?
b. What should Big Bank do about these e-mails?
c. Identify the computer fraud and abuse technique illustrated.

6.3. A purchasing department received the following e-mail.

Dear Accounts Payable Clerk,
You can purchase everything you need online—including peace of mind—when you shop using Random Account Numbers (RAN). RAN is a free service for Big Credit Card customers that substitutes a random credit card number in place of your normal credit card number when you make online purchases and payments. This random number provides you with additional security. Before every online purchase, simply get a new number from RAN to use at each new vendor. Sign up for an account at www.bigcreditcard.com. Also, take advantage of the following features:

- *Automatic Form automatically completes a vendor's order form with the RAN, its expiration date, and your shipping and billing addresses.*

- *Set the spending limit and expiration date for each new RAN.*
- *Use RAN once or use it for recurring payments for up to one year.*

Required

Explain which computer fraud and abuse techniques could be prevented using a random account number that links to your corporate credit card.

6.4. Computer Fraud and Abuse Techniques.

Match the Internet-related computer fraud and abuse technique in the left column with the scenario in the right column. Terms on the left may be used once, more than once, or not at all.

____ 1. Adware

____ 2. Botnet

____ 3. Bot herder

____ 4. Click fraud

____ 5. DoS

____ 6. E-mail threats

____ 7. Hijacking

____ 8. Internet misinformation

____ 9. Internet terrorism

____ 10. Key logger

____ 11. Pharming

____ 12. Phishing

____ 13. Spamming

____ 14. Splog

____ 15. Spyware

____ 16. Spoofing

____ 17. Typosquatting

a. Software that monitors and reports a user's computing habits

b. A program stored in a Web page that is executed by a Web browser

c. Sending an e-mail instructing the recipient to do something or else suffer adverse consequences

d. Using the Internet to pass off the work of another as your own

e. E-mailing an unsolicited message to many people at the same time

f. Creating Web sites with names similar to real Web sites so users making errors while entering a Web site name are sent to a hacker's site

g. An e-mail warning regarding a virus that, in reality, does not exist

h. A spam blog that promotes affiliated Web sites to increase their Google PageRank

i. Software that collects consumer surfing and purchasing data

j. E-mails that look like they came from a legitimate source but are actually from a hacker who is trying to get the user to divulge personal information

k. Making an e-mail look like it came from someone else

l. Gaining control of a computer to carry out unauthorized illicit activities

m. Using the Internet to disrupt communications and e-commerce

n. Diverting traffic from a legitimate Web site to a hacker's Web site to gain access to personal and confidential information

o. A network of hijacked computers

p. Using a legion of compromised computers to launch a coordinated attack on an Internet site

q. Use of spyware to record a user's keystrokes

r. Hackers that control hijacked computers

s. Circulating lies or misleading information using the world's largest network

t. Overloading an Internet service provider's e-mail server by sending hundreds of e-mail messages per second from randomly generated false addresses

u. Inflating advertising revenue by clicking online ads numerous times

6.5. Computer Fraud and Abuse Techniques.

Match the computer fraud and abuse technique in the left column with the scenario in the right column. Terms on the left may be used once, more than once, or not at all.

___ 1. Bluebugging
___ 2. Bluesnarfing
___ 3. Eavesdropping
___ 4. Evil twin
___ 5. Packet sniffing
___ 6. Phreaking
___ 7. Piggybacking
___ 8. Vishing
___ 9. War dialing
___ 10. War driving

a. Intercepting Internet and other network transmissions
b. E-mails instructing a user to call a phone number where they are asked to divulge personal information
c. Searching for unprotected wireless networks in a vehicle
d. Gaining access to a protected system by latching onto a legitimate user
e. Decoding and organizing captured network data
f. Intercepting and/or listening in on private voice and data transmissions
g. Deep packet filtering
h. Searching for modems on unprotected phone lines in order to access the attached computer and gain access to the network(s) to which it is attached
i. Making phone calls and sending text messages using another user's phone without physically holding that phone
j. Using telephone lines to transmit viruses and to access, steal, and destroy data
k. Capturing data from devices that use Bluetooth technology
l. Devices that hide IP addresses
m. A rogue wireless access point masquerading as a legitimate access point

6.6. Computer Fraud and Abuse Techniques.

Match the computer fraud and abuse technique in the left column with the scenario in the right column. Terms on the left may be used once, more than once, or not at all.

___ 1. Chipping
___ 2. Data diddling
___ 3. Data leakage
___ 4. Identity theft
___ 5. Round-down
___ 6. Salami technique
___ 7. Scavenging

a. Illegally obtaining confidential information, such as a Social Security number, about another person so that it can be used for financial gain
b. Searching through garbage for confidential data
c. Covertly swiping a credit card in a card reader that records the data for later use
d. Embezzling small fractions of funds over time
e. Inserting a chip that captures financial data in a legitimate credit card reader
f. Copying company data, such as computer files, without permission
g. Concealing data within a large MP3 file
h. Use of spyware to record a user's keystrokes
i. Altering data during the IPO (Input-Process-Output) cycle
j. Placing truncated decimal places in an account controlled by the perpetrator

6.7. Computer Fraud and Abuse Techniques.

Match the computer fraud and abuse technique in the left column with the scenario in the right column. Terms on the left may be used once, more than once, or not at all.

____ 1. Dictionary attack
____ 2. Hacking
____ 3. Logic bomb
____ 4. Malware
____ 5. Masquerading
____ 6. Password cracking
____ 7. Piggybacking
____ 8. Posing
____ 9. Pretexting
____ 10. Rootkit
____ 11. Shoulder surfing
____ 12. Skimming
____ 13. Social engineering
____ 14. Software piracy
____ 15. Steganography
____ 16. Superzapping
____ 17. Trap door
____ 18. Trojan horse
____ 19. Virus
____ 20. Worm
____ 21. Zero-day attack

a. Special software used to bypass system controls

b. A segment of executable code that attaches itself to software

c. Capturing and decrypting passwords to gain access to a system

d. Malicious computer code that specifically targets a computer's start-up instructions

e. Using a wireless network without permission

f. Covertly swiping a credit card in a card reader that records the data for later use

g. Concealing data within a large MP3 file

h. Attack occurring between the discovery of a software vulnerability and the release of a patch to fix the problem

i. Entering a system using a back door that bypasses normal system controls

j. Using software to guess company addresses, send employees blank e-mails, and add unreturned messages to spammer e-mail lists

k. Unauthorized code in an authorized and properly functioning program

l. Software used to do harm

m. A program that can replicate itself and travel over networks

n. Pretending to be a legitimate user, thereby gaining access to a system and all the rights and privileges of the legitimate user

o. Special code or password that bypasses security features

p. Unauthorized copying or distribution of copyrighted software

q. Software that conceals processes, files, network connections, and system data from the operating system and other programs

r. Methods used to trick someone into divulging personal information

s. Software that sits idle until a specified circumstance or time triggers it

t. The act of duplicating software, music, or movies

u. Acting under false pretenses to gain confidential information

v. Observing or listening to users as they divulge personal information

w. Gaining access to a computer system without permission

x. Creating a seemingly legitimate business, collecting personal information while making a sale, and never delivering the item sold

6.8. Computer Fraud and Abuse Techniques.

Match the computer fraud and abuse technique in the left column with the scenario in the right column. Terms on the left may be used once, more than once, or not at all.

___ **1.** Address Resolution Protocol (ARP) spoofing

___ **2.** Buffer overflow attack

___ **3.** Carding

___ **4.** Caller ID spoofing

___ **5.** Cyber-extortion

___ **6.** Cyber-bullying

___ **7.** Economic espionage

___ **8.** E-mail spoofing

___ **9.** IP address spoofing

___ **10.** Internet auction fraud

___ **11.** Internet pump-and-dump fraud

___ **12.** Lebanese looping

___ **13.** Man-in-the-middle (MITM) attack

___ **14.** Podslurping

___ **15.** Ransomware

___ **16.** Scareware

___ **17.** Sexting

___ **18.** SQL Injection

___ **19.** SMS spoofing

___ **20.** XSS attack

___ **21.** Tabnapping

a. Inserting a sleeve to trap a card in an ATM, pretending to help the owner and thereby obtaining the PIN, and using the card and PIN to drain the account

b. A segment of executable code that attaches itself to software

c. Using a small storage device to download unauthorized data from a computer

d. Malicious computer code that specifically targets a computer's start-up instructions

e. Malicious software that people are frightened into buying

f. Covertly swiping a credit card in a card reader that records the data for later use

g. Using the Internet to inflate a stock price so it can be sold for a profit

h. Exchanging explicit messages and pictures by telephone

i. Inserting a malicious database query in input in a way that it can be executed by an application program

j. So much input data that storage is exceeded; excess input contains code that takes control of the computer

k. Making an electronic communication appear as though it originated from a different source

l. Creating packets with a forged address to impersonate another computing system

m. Fake computer networking protocol messages sent to an Ethernet LAN to determine a network host's hardware address when only its IP address is known

n. Changing the name or number a text message appears to come from

o. Special code or password that bypasses security features

p. A link containing malicious code that takes a victim to a vulnerable Web site. Once there, the victim's browser executes the malicious code embedded in the link.

q. Using social networking to harass another person

r. Displaying an incorrect phone number to hide the caller's identity

s. Software that encrypts programs and data until a payment is made to remove it

t. A hacker placing himself between a client and a host to intercept network traffic

u. A demand for payment to ensure a hacker does not harm a computer

v. Theft of trade secrets and intellectual property

w. Using a site that sells to the highest bidder to defraud another person

x. Verifying credit card validity

y. Secretly changing an already open browser tab

6.9. Identify the computer fraud and abuse technique used in each the following actual examples of computer wrongdoing.

a. A teenage gang known as the "414s" broke into the Los Alamos National Laboratory, Sloan-Kettering Cancer Center, and Security Pacific Bank. One gang member appeared in *Newsweek* with the caption "Beware: Hackers at play."

b. Daniel Baas was the systems administrator for a company that did business with Acxiom, who manages customer information for companies. Baas exceeded his authorized access and downloaded a file with 300 encrypted passwords, decrypted the password file, and downloaded Acxiom customer files containing personal information. The intrusion cost Acxiom over $5.8 million.

c. Cyber-attacks left high-profile sites such as Amazon.com, eBay, Buy.com, and CNN Interactive staggering under the weight of tens of thousands of bogus messages that tied up the retail sites' computers and slowed the news site's operations for hours.

d. Susan Gilmour-Latham got a call asking why she was sending the caller multiple adult text messages per day. Her account records proved the calls were not coming from her phone. Neither she nor her mobile company could explain how the messages were sent. After finding no way to block the unsavory messages, she changed her mobile number to avoid further embarrassment by association.

e. A federal grand jury in Fort Lauderdale claimed that four executives of a rental-car franchise modified a computer-billing program to add five gallons to the actual gas tank capacity of their vehicles. Over three years, 47,000 customers who returned a car without topping it off ended up paying an extra $2 to $15 for gasoline.

f. A mail-order company programmer truncated odd cents in sales-commission accounts and placed them in the last record in the commission file. Accounts were processed alphabetically, and he created a dummy sales-commission account using the name of Zwana. Three years later, the holders of the first and last sales-commission accounts were honored. Zwana was unmasked and his creator fired.

g. MicroPatent, an intellectual property firm, was notified that their proprietary information would be broadcast on the Internet if they did not pay a $17 million fee. The hacker was caught by the FBI before any damage was done.

h. When Estonia removed a Russian World War II war memorial, Estonian government and bank networks were knocked offline in a distributed DoS attack by Russian hackers. A counterfeit letter of apology for removing the memorial statue was placed on the Web site of Estonia's prime minister.

i. eBay customers were notified by e-mail that their accounts had been compromised and were being restricted unless they re-registered using an accompanying hyperlink to a Web page that had eBay's logo, home page design, and internal links. The form had a place for them to enter their credit card data, ATM PINs, Social Security number, date of birth, and their mother's maiden name. Unfortunately, eBay hadn't sent the e-mail.

j. A teenager hijacked the eBay.de domain name and several months later the domain name for a large New York ISP. Both hijacked Web sites pointed to a site in Australia.

k. Travelers who logged into the Alpharetta, Georgia, airport's Internet service had personal information stolen and picked up as many as 45 viruses. A hacker had set up a rogue wireless network with the same name as the airport's wireless access network.

l. Criminals in Russia used a vulnerability in Microsoft's server software to add a few lines of Java code to users' copies of Internet Explorer. The code recorded the users' keyboard activities, giving the criminals access to usernames and passwords at many banking Web sites. The attacks caused $420 million in damage.

m. America Online subscribers received a message offering free software. Users who opened the attachments unknowingly unleashed a program hidden inside another program that secretly copied the subscriber's account name and password and forwarded them to the sender.

n. Rajendrasinh Makwana, an Indian citizen and IT contractor who worked at Fannie Mae's Maryland facility, was terminated at 1:00 P.M. on October 24. Before his network access was revoked, he created a program to wipe out all 4,000 of Fannie Mae's servers on the following January 31.

o. A man accessed millions of ChoicePoint files by claiming in writing and on the phone to be someone he was not.

p. A 31-year-old programmer unleashed a Visual Basic program by deliberately posting an infected document to an alt.sex Usenet newsgroup using a stolen AOL account. The program evaded security software and infected computers using the Windows operating system and Microsoft Word. On March 26, the Melissa program appeared on thousands of e-mail systems disguised as an important message from a colleague or friend. The program sent an infected e-mail to the first 50 e-mail addresses on the users' Outlook address book. Each infected computer would infect 50 additional computers, which in turn would infect another 50 computers. The program spread rapidly and exponentially, causing considerable damage. Many companies had to disconnect from the Internet or shut down their e-mail gateways because of the vast amount of e-mail the program was generating. The program caused more than $400 million in damages.

q. Microsoft filed a lawsuit against two Texas firms that produced software that sent incessant pop-ups resembling system warnings. The messages stated "CRITICAL ERROR MESSAGE! REGISTRY DAMAGED AND CORRUPTED" and instructed users to visit a Web site to download Registry Cleaner XP at a cost of $39.95.

r. As many as 114,000 Web sites were tricked into running database commands that installed malicious HTML code redirecting victims to a malicious Web server that tried to install software to remotely control the Web visitors' computers.

s. Zeus records log-in information when the user of the infected computer logs into a list of target Web sites, mostly banks and other financial institutions. The user's data is sent to a remote server where it is used and sold by cyber-criminals. The new version of Zeus will significantly increase fraud losses, given that 30% of Internet users bank online.

t. It took Facebook 15 hours to kill a Facebook application that infected millions of PCs with software that displays a constant stream of pop-up ads. The program posted a "Sexiest Video Ever" message on Facebook walls that looked like it came from a friend. Clicking the link led to a Facebook installation screen, where users allowed the software to access their profiles and walls. Once approved, the application told users to download an updated, free version of a popular Windows video player. Instead, it inserted a program that displayed pop-up ads and links. A week later a "Distracting Beach Babes" message did the same thing.

u. Robert Thousand, Jr. discovered he lost $400,000 from his Ameritrade retirement account shortly after he began receiving a flood of phone calls with a 30-second recording for a sex hotline. An FBI investigation revealed that the perpetrator obtained his Ameritrade account information, called Ameritrade to change his phone number, created several VoIP accounts, and used automated dialing tools to flood the dentist's phones in case Ameritrade called his real number. The perpetrator requested multiple monetary transfers, but Ameritrade would not process them until they reached Thousand to verify them. When the transfers did not go through, the attacker called Ameritrade, gave information to verify that he was Thousand, claimed he had been having phone troubles, and told Ameritrade he was not happy that the transfers had not gone through. Ameritrade processed the transfers, and Thousand lost $400,000.

v. The Internet Crime Complaint Center reports a "hit man" scam. The scammer claims that he has been ordered to assassinate the victim and an associate has been ordered to kill a family member. The only way to prevent the killings is to send $800 so an Islamic expatriate can leave the United States.

w. In an economic stimulus scam, individuals receive a phone call from President Obama telling them to go to a Web site to apply for the funds. To receive the stimulus money, victims have to enter personal identification information, complete an online application, and pay a $28 fee.

6.10. On a Sunday afternoon at a hospital in the Pacific Northwest, computers became sluggish, and documents would not print. Monday morning, the situation became worse when employees logged on to their computers. Even stranger things happened—operating-room doors would not open, pagers would not work, and computers in the intensive care unit shut down. By 10:00 A.M., all 50 IT employees were summoned. They discovered that the hospital was under attack by a botnet that exploited a Microsoft operating system flaw and installed pop-up ads on hospital computers. They got access to the first computer on Sunday and used the hospital's network to spread the infection to other computers. Each infected computer became a zombie that scanned the network looking for new victims. With the network clogged with zombie traffic, hospital communications began to break down. The IT staff tried to halt the attack by shutting off the hospital's Internet connection, but it was too late. The bots were inside the hospital's computer system and infecting other computers faster than they could be cleaned. Monday afternoon IT figured out which malware the bots were installing and wrote a script, which was pushed out hourly, directing computers to remove the bad code. The script helped to slow the bots down a bit.

(*Source:* D. Gage, *Baseline Security* February 6, 2007.)

Required

a. What could the hospital do to stop the attack and contain the damage?

b. Which computer fraud and abuse technique did the hackers use in their attack on the hospital?

c. What steps should the hospital have taken to prevent the damage caused by the attack?

Case 6-1 Shadowcrew

At 9:00 P.M., Andrew Mantovani, cofounder of the group Shadowcrew, received a knock at his door while chatting on his computer. For Mantovani and 27 others, that knock marked the end of Shadowcrew, which provided online marketplaces and discussion forums for identity thieves. Shadowcrew members used the organization's Web site to traffic in stolen Social Security numbers, names, e-mail addresses, counterfeit driver's licenses, birth certificates, and foreign and domestic passports. It also shared best practices for carrying out fraudulent activity. By the time it was shut down, Shadowcrew had trafficked in at least 1.7 million credit cards and it was responsible for more than $4.3 million in fraud losses.

Considered the online equivalent of the Russian Mafia, Shadowcrew operated as a highly sophisticated and hierarchical organization. All users operated under aliases, never revealing their true names or other personal information. Operations and communications were conducted using proxy servers that hid the location and identity of the users. Shadowcrew users were divided into five different roles: administrators, moderators, reviewers, vendors, and members.

Administrators Shadowcrew administrators were the heads of the organization.

Moderators A dozen moderators, chosen from the general membership based on proven skill in fraudulent activity, controlled the flow of information.

Reviewers Reviewers tested the quality of illicit goods (credit cards, passports, etc.) trafficked on the Shadowcrew site. For example, reviewers would run a test called a "dump check" on credit card numbers by hacking into a retailer's cash register system. The fraudster accessed the system through back doors used by technical support personnel to remotely perform maintenance or repairs. The reviewer would then enter a trivial charge of $1 or $2 to see whether the charge was approved. Reviewers would then write up and post detailed descriptions of the credit cards or other merchandise tested.

Vendors Vendors managed the sale of stolen data. Prices were posted and products were sold using an auction forum much like eBay. Payments were processed via Western Union money transfers or an electronic currency and were made using a fraud victim's stolen data.

Members Thousands of people used the Shadowcrew Web site to gather and share information on committing identity fraud. Shadowcrew practiced open registration, but more sensitive discussion areas were password protected, and members needed another trusted member to vouch for them in order to join the forum.

Members could be promoted up the organization by providing quality products or by sharing new or unique tips or techniques for committing fraud. Shadowcrew punished acts of disloyalty. For instance, one disloyal group member had his actual name, address, and phone number posted on the Web site for all to see.

Shadowcrew's demise began when MasterCard informed the United States government that a hundred Web sites promoted and supported identity fraud. The United States Secret Service covertly infiltrated Shadowcrew. Acting as trusted members, agents set up a Virtual Private Network (VPN) over which Shadowcrew leaders could conduct illicit business. The VPN allowed the Secret Service to track the organization's doings and discover the real identities and locations of Shadowcrew users.

It was vital that all arrests occur simultaneously, because any one of the targets could instantly warn the others via Shadowcrew's discussion forum. With the help of the Justice Department, the Homeland Security Department, the Royal Canadian Mounted Police, Europol, and local police departments, authorities simultaneously knocked on the suspects' doors at precisely 9:00 P.M. The operation led to 28 arrests, 21 in the United States. Rather than immediately deactivating the Web site, investigators replaced the home page with the following warning: "Activities by Shadowcrew members are being investigated by the United States Secret Service." Under a picture of hands clutching bars of a jail cell, agents listed the criminal charges that Shadowcrew members faced and called on visitors to turn themselves in: "Contact your local United States Secret Service field office before we contact you!"

(*Source:* J. McCormick and D. Gage, *Baseline Security*, March 7, 2005.)

1. How did Shadowcrew members conceal their identities? How can average citizens protect their identities while interacting online?
2. How has the Internet made detecting and identifying identity fraudsters difficult?
3. What are some of the most common electronic means of stealing personal information?
4. What is the most common way that fraudsters use personal data?
5. What measures can consumers take to protect against the online brokering of their personal data?
6. What are the most effective means of detecting identity theft?
7. What pieces of personal information are most valuable to identity fraudsters?

AIS IN ACTION SOLUTIONS

Quiz Key

1. A set of instructions to increase a programmer's pay rate by 10% is hidden inside an authorized program. It changes and updates the payroll file. What is this computer fraud technique called?
   a. virus (Incorrect. A virus damages a system using a segment of executable code that attaches itself to software, replicates itself, and spreads to other systems or files.)
   b. worm (Incorrect. A worm is a program that hides in a host program and copies and actively transmits itself directly to other systems.)
   c. trap door (Incorrect. A trap door is entering a system using a back door that bypasses normal system controls.)
   ▶ d. Trojan horse (Correct. Placing unauthorized computer instructions, such as fraudulently increasing an employee's pay, in an authorized and properly functioning program is an example of a Trojan horse.)

2. Which computer fraud technique involves a set of instructions hidden inside a calendar utility that copies itself each time the utility is enabled until memory is filled and the system crashes?
   a. logic bomb (Incorrect. A logic bomb sabotages a system using a program that lies idle until some specified circumstance or a particular time triggers it.)
   b. trap door (Incorrect. A trap door is a means of bypassing normal system controls to enter a system.)
   ▶ c. virus (Correct. A virus damages a system using a segment of executable code that attaches itself to software, replicates itself, and spreads to other systems or files.)
   d. Trojan horse (Incorrect. Placing unauthorized computer instructions, such as fraudulently increasing an employee's pay, in an authorized and properly functioning program is an example of a Trojan horse.)

3. Interest calculations are truncated at two decimal places, and the excess decimals are put into an account the perpetrator controls. What is this fraud called?
   a. typosquatting (Incorrect. Typosquatting is the practice of setting up Web sites with names similar to real Web sites so that users who make typographical errors when typing Web site names are sent to a site filled with malware.)

b. URL hijacking (Incorrect. URL hijacking is another name for typosquatting, which is explained above.)

c. chipping (Incorrect. Chipping is planting a chip that records transaction data in a legitimate credit card reader.)

▶ d. round-down fraud (Correct.)

4. A perpetrator attacks phone systems to obtain free phone line access or uses telephone lines to transmit viruses and to access, steal, and destroy data. What is this computer fraud technique called?

a. phishing (Incorrect. Phishing is the practice of sending e-mails requesting recipients to visit a Web page and verify data or fill in missing data. The e-mails and Web sites look like legitimate companies, primarily financial institutions.)

▶ b. phreaking (Correct.)

c. pharming (Incorrect. Pharming is redirecting traffic to a spoofed Web site to gain access to personal and confidential information.)

d. vishing (Incorrect. Vishing is voice phishing, in which e-mail recipients are asked to call a phone number where they are asked to divulge confidential data.)

5. Fraud perpetrators threaten to harm a company if it does not pay a specified amount of money. What is this fraud technique called?

a. cyber-terrorism (Incorrect. Cyber-terrorism, or Internet terrorism, is using the Internet to disrupt communications and e-commerce.)

b. blackmailing (Incorrect. Blackmailing is the extortion of money or something else of value from a person by the threat of exposing a criminal act or discreditable information.)

▶ c. cyber-extortion (Correct.)

d. scareware (Incorrect. Scareware is software of limited or no benefit, often malicious in nature, that is sold using scare tactics. The most common scare tactic is a dire warning that the person's computer is infected with viruses, spyware, or some other catastrophic problem.)

6. Techniques used to obtain confidential information, often by tricking people, are referred to as what?

a. pretexting (Incorrect. Pretexting is one specific type of social engineering. It involves acting under false pretenses to gain confidential information.)

b. posing (Incorrect. Posing is one specific type of social engineering in which someone creates a seemingly legitimate business, collects personal information while making a sale, and never delivers the item sold.)

▶ c. social engineering (Correct.)

d. identity theft (Incorrect. Identity theft is a type of social engineering in which one person assumes another's identity, usually for economic gain, by illegally obtaining confidential information, such as a Social Security number.)

7. What type of software secretly collects personal information about users and sends it to someone else without the user's permission?

a. rootkit (Incorrect. A rootkit is software that conceals processes, files, network connections, and system data from the operating system and other programs.)

b. torpedo software (Incorrect. Torpedo software is software that destroys competing malware, resulting in "malware warfare" between competing developers.)

▶ c. spyware (Correct.)

d. malware (Incorrect. *Malware* is a general term that applies to any software used to do harm. There is a more specific correct answer to this question.)

8. What type of software conceals processes, files, network connections, memory addresses, systems utility programs, and system data from the operating system and other programs?

▶ a. rootkit (Correct.)

b. spyware (Incorrect. Spyware is software that is used to monitor computing habits and send that data to someone else, often without the computer user's permission.)

c. malware (Incorrect. Malware is any software that is used to do harm.)

d. adware (Incorrect. Adware is software used to collect Web-surfing and spending data and forward it to advertising or media organizations. It also causes banner ads to pop up on computer monitors as the Internet is surfed.)

9. Which type of computer attack takes place between the time a software vulnerability is discovered and the time software developers release a software patch that fixes the problem?

a. posing (Incorrect. Posing is creating a seemingly legitimate business, collecting personal information while making a sale, and never delivering the item sold.)

▶ **b.** zero-day attack (Correct.)

c. evil twin (Incorrect. An evil twin is a wireless network with the same name as a local wireless access point that unsuspecting people use, allowing hackers to monitor the network's traffic looking for useful information.)

d. software piracy (Incorrect. Software piracy is the illegal copying of computer software.)

10. Someone redirects a Web site's traffic to a bogus Web site, usually to gain access to personal and confidential information. What is this computer fraud technique called?

a. vishing (Incorrect. Vishing is voice phishing, in which e-mail recipients are asked to call a phone number where they are asked to divulge confidential data.)

b. phishing (Incorrect. Phishing is sending e-mails requesting recipients to visit a Web page and verify data or fill in missing data. The e-mails and Web sites look like legitimate companies, primarily financial institutions.)

▶ **c.** pharming (Correct.)

d. phreaking (Incorrect. Phreaking is attacking phone systems and using telephone lines to transmit viruses and to access, steal, and destroy data.