#  CHAPTER 6

 **COMPUTER FRAUD AND ABUSE TECHNIQUES**

**SUGGESTED ANSWERS TO 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?**

The perpetrator may have been an external hacker or he may have been an employee with knowledge of the system.

It seems likely that the perpetrator was responsible for the sluggishness, as he called soon after it started. To cause the sluggishness, the perpetrator may have:

* Infected the system with a **virus** or **worm**.
* **Hacked** into the system and **hijacked** the system, or a large part of its processing capability.

 To break into the system, the perpetrator may have:

* Used pretexting, which is creating and using an invented scenario (the [pretext](http://en.wikipedia.org/wiki/Pretext)) to increase the likelihood that a victim will divulge information or do something they would not normally do. In this case, the perpetrator pretended to be an IBM software troubleshooter to get a log-on ID and password.
* Used masquerading</keyterm> or <keyterm linkend="ch05kt32" role="strong" preference="1">impersonation</keyterm>, which is pretending to be an authorized user to access a system. This was possible in this case once the perpetrator obtained the log-on ID and password. Once inside the system, the perpetrator has all the privileges attached to the user ID and password given to him.
* Infected it with a **Trojan horse, trap door,** **logic or time bomb**, or some other malware.
* Made unauthorized use of **superzap**, a software utility that bypasses regular system controls.

**What could USL do to avoid these types of incidents in the future?**</para></question><question id="ch05ques04" label="5.4">

* + Determine how the perpetrator caused the sluggishness and implement the controls need to prevent it from happening again.
	+ Conduct a complete security review to identify and rectify and security weaknesses.
	+ Only reveal passwords and logon numbers to authorized users whose identities have been confirmed. When someone calls and indicates they are an IBM employee, verify their identity by calling IBM back on their known and published service number. Even better would be to call and talk to the IBM representative assigned to USL.
	+ Provide employee training aimed at helping them not fall victim to the many forms of social engineering.
	+ After providing outsiders with temporary user IDs and passwords, block their use as soon as the need for them is passed.

Other control considerations that could reduce the incidence of unauthorized access include:

* Improved control of sensitive data.
* Alternate repair procedures.
* Increased monitoring of system activities.

**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.**

 Hacking is the unauthorized access, modification, or use of an electronic device or some element of a computer system. Hacking represents illegal trespassing and is punishable as a federal crime under the 1986 Computer Fraud and Abuse Act.

Hacking has increased significantly in popularity for several reasons. Perhaps the most important is the increasing use of personal computers and the Internet and the corresponding rise in the number and the skill level of the users. In other words, there are more systems to break into, and there are more people capable of breaking in.

 Most hackers are motivated by monetary rewards. Hackers have found many ways to profit handsomely from their hacking activities. Others hackers seek to destroy data, to make unauthorized copies of the data, or to damage the system in some way.

Some hackers are motivated by the challenge of breaking and entering a system and many do so with no intent to do harm. They may feel that hacking is a "right" enjoyed by computer users in a "free information" society. Many of these benign hackers also argue that hacking rarely does any harm to a computer system and is acceptable behavior.

**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.**

 **<para>What conditions made the UCLA system a potential breeding ground for the virus?**

* Many computers, providing numerous potential hosts.
* Users are allowed to create and store programs.
* Users share programs regularly.
* Numerous external data storage devices are used each day by students without adequate controls over their contents.
* University students send lots of emails and download lots of software, music, and videos from the Internet, all of which are excellent ways to pass viruses to others.

**What symptoms indicated that a virus was present?**

* Destroyed or altered data and programs.
* The inability to boot the system or to access data on a hard drive.
* Clogged communications.
* Hindered system performance.

However, the system did not print disruptive images or messages on the screen. Some people who write viruses cause some sort of message or image to appear to give some indication that the system has been compromised.

**<para>**

**SUGGESTED ANSWERS TO THE 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.**

 **a. What is a computer virus? Cite at least three reasons why no system is completely safe from a computer virus.**

 A computer virus is a segment of executable code that attaches itself to an application program or some other executable component. When the hidden program is triggered, it makes unauthorized alterations in the way a system operates.

There are a number of reasons why no one is completely safe from a virus:

* Viruses are contagious and are easily spread from one system to another. A virus spreads when users share programs or data files, download data from the Internet, or when they access and use programs from external sources such as suppliers of free software.
* Viruses can spread very quickly. In a network environment, a virus can spread to thousands of systems in a relatively short period. When the virus is confined to a single machine or to a small network, it will soon run out of computers to infect.
* Many viruses lie dormant for extended periods without doing any specific damage except propagating itself. The hidden program leaves no external signs of infection while it is reproducing itself.
* Many computer viruses have long lives because they can create copies of themselves faster than the virus can be destroyed.

**b. Why do viruses represent a serious threat to information systems? What damage can a virus do to a computer system?**

 Viruses are a significant threat to information systems because they make unauthorized alterations to the way a system operates and cause widespread damage by destroying or altering data or programs. If adequate backup is not maintained, viral damage may also mean permanent loss of important or unique information, or time-consuming reentry of the lost information.

A virus can cause significant damage when it takes control of the computer, destroys the hard disk's file allocation table, and makes it impossible to boot (start) the system or to access data on a hard drive. They can also intercept and change transmissions, print disruptive images or messages on the screen, or cause the screen image to disappear. As the virus spreads, it takes up space, clogs communications, and hinders system performance.

**c. How does a virus resemble a Trojan horse?**

 A virus is like a Trojan horse in that it can lie dormant for extended periods, undetected until triggered by an event or condition.

**d. What steps can be taken to prevent the spread of a computer virus?**

Focus 6-1 lists the following steps individuals can take to keep their computers virus free:

<itemizedlist mark="bull" type="bl"><listitem><para><inst>• </inst>Install reputable and reliable antivirus software that scans for, identifies, and destroys viruses. Only use one antivirus program, as multiple programs conflict with each other.

* Do not fall for ads touting free anti-virus software, as much of it is fake and contains malware. Some hackers create websites 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 anti-virus 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 anti-virus program to clean it up.

<listitem><para><inst>• </inst>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.</para></listitem>

<listitem><para><inst>• </inst>Scan all incoming e-mail for viruses at the server level as well as when it hits users’ desktops.

* Do not download anything from an email 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. English is obviously not their first language. </para></listitem>
* All software should be certified as virus-free before loading it into the system. Be wary of software from unknown sources, as they may be virus bait—especially if their prices or functionality sound too good to be true. </para></listitem>

<listitem><para><inst>• </inst>Deal with trusted software retailers.</para></listitem>

<listitem><para><inst>• </inst>Some software suppliers use electronic techniques to make tampering evident. Ask if the software you are purchasing has such protection.</para></listitem>

<listitem><para><inst>• </inst>Check new software on an isolated machine with virus detection software. Software direct from the publisher has been known to have viruses.</para></listitem>

<listitem><para><inst>• </inst>Have two backups of all files. Data files should be backed up separately from programs to avoid contaminating backup data.</para></listitem>

<listitem><para><inst>• </inst>If you use flash drives, diskettes, or CDs, do not put them in strange machines as 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.</para></listitem></itemizedlist></sidebar>

**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***](http://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.***

 **a. What should Justin do about these e-mails?**

This is an attempt to acquire confidential information so that it can be used for illicit purposes such as identity theft. Since the email looks authentic and appears authoritative, unsuspecting and naïve employees are likely to follow the emails instructions.

 Justin should:

* Notify all employees and management that the email is fraudulent and that no information should be entered on the indicated website.
* Delete the email without responding to its sender.
* Launch an education program for all employees and management about computer fraud practices that could target their business.
* Notify Big Bank regarding the email.

**b. What should Big Bank do about these e-mails?**

* Immediately alert all customers about the email and ask them to forward any suspicious email to the bank security team. But this needs to be done via the bank’s web site, not by an email message. Banks need to consistently never use email in ways similar to this type of attack.
* Establish a quick and convenient method that encourages customers and employees to notify Big Bank of suspicious emails.
* The warnings received by customers and employees should be investigated and remedial actions should be taken.
* Notify and cooperate with law enforcement agencies so the perpetrator can be apprehended.
* Notify the ISP from which the email originated, demanding that the perpetrator’s account be discontinued.

**c. Identify the computer fraud and abuse technique illustrated.**

 This computer fraud and abuse technique is called phishing. Its purpose is to get the information need to commit identity theft. The perpetrator probably also used brand spoofing of Big Bank’s web site.

**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***](http://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.***

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

</para></problem>

 Banks actually offer a service like this. For example, Citi Bank offers a program called Virtual Account Numbers.

 Students will likely present many different solutions to this problem. Table 6-1 in the text provides a comprehensive list of computer fraud and abuse techniques that the students may draw upon. Potential solutions should at least include:

* identity theft
* packet sniffing
* Spyware
* eavesdropping to capture the card number.

Using RAN can limit the amount of money stolen. If the card or card number is stolen, it can only be used for the specific vendor and time for which it is issued. In addition, it can only be used for one purchase or only a set number of purchases identified when the card number was issued. At any rate, restricting the card to only a specific merchant and for a specific time and number of transactions severely restricts the thief's ability to steal.

Using RAN can help prevent identity fraud. Since the card is only linked to the actual customer at the bank, the identity of the customer is shielded to anyone who steals the card or the card number. The thief would need to hack into the bank’s system to find the identity of the RAN cardholder since it would not be printed on the card itself.

Also, RAN can frustrate those who capture card numbers through packet sniffing, spyware, and eavesdropping. These techniques may capture the card number, but once the thieves have it, their ability to exploit the card for monetary gain is severely restricted.

**PERHAPS MORE IMPORTANT:** even though banks offer these types of services, this email may be a clever Phishing expedition and a recipient should not respond to the email or click on the indicated link. This prevents the recipient from being the victim of an attack or malicious malware.

If a person was interested in the service, he should contact his bank and ask about it. Alternatively, he could research the service and call those who offer it.

**6.4 <para>Match the internet related computer fraud and abuse technique in the left column with the scenario in the right column. Terms may be used once, more than once, or not at all.</para>**

|  |  |
| --- | --- |
| **1. Adware** | i. Software that collects consumer surfing and purchasing data. |
| **2. Botnet** | o. A network of hijacked computers. |
| **3. Bot herder** | r. Hackers that control hijacked computers. |
| **4. Click fraud** | u. Inflating advertising revenue by clicking online ads numerous times. |
| **5. DoS** | t. Overloading an Internet service provider’s e-mail server by sending hundreds of e-mail messages per second from randomly generated false addresses. |
| **6. E-mail threats** | c. Sending an e-mail instructing the recipient to do something or they will suffer adverse consequences. |
| **7. Hijacking** | l. Gaining control of a computer to carry out unauthorized illicit activities.  |
| **8. Internet misinformation** | s. Circulating lies or misleading information using the world’s largest network. |
| **9. Internet terrorism** | m. Using the Internet to disrupt communications and e-commerce. |
| **10. Key logger** | q. Use of spyware to record a user’s keystrokes. |
| **11. Pharming** | n. Diverting traffic from a legitimate Web site to a hacker’s Web site to gain access to personal and confidential information. |
| **12. Phishing** | 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. |
| **13. Spamming** | e. E-mailing an unsolicited message to many people at the same time. |
| **14. Splog** | h. A spam blog that promotes affiliated Web sites to increase their Google PageRank. |
| **15. Spyware** | a. Software that monitors and reports a user’s computing habits. |
| **16. Spoofing** | k. Making an e-mail look like it came from someone else. |
| **17. Typosquatting** | 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. |

**6. 5 <para>Match the data communications-related computer fraud and abuse technique in the left column with the scenario in the right column. Terms may be used once, more than once, or not at all.**

**</para>**

|  |  |
| --- | --- |
| **1. Bluebugging** | i. Making phone calls and sending text messages using another user’s phone without physically holding that phone. |
| **2. Bluesnarfing** | k. Capturing data from devices that use Bluetooth technology. |
| **3. Eavesdropping** | f. Intercepting and/or listening in on private voice and data transmissions. |
| **4. Evil twin** | m. A rogue wireless access point masquerading as a legitimate access point. |
| **5. Packet sniffing** | a. Intercepting Internet and other network transmissions. |
| **6. Phreaking** |  j. Using telephone lines to transmit viruses and to access, steal, and destroy data. |
| **7. Piggybacking** | d. Gaining access to a protected system by latching on to a legitimate user. |
| **8. Vishing** | b. E-mails instructing a user to call a phone number where they are asked to divulge personal information. |
| **9. War dialing** | 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. |
| **10. War driving** | c. Searching for unprotected wireless networks in a vehicle. |

**6.6 <para>Match the data related computer fraud and abuse technique in the left column with the scenario in the right column. Terms may be used once, more than once, or not at all.</para>**

|  |  |
| --- | --- |
| **1. Chipping** | e. Inserting a chip that captures financial data in a legitimate credit card reader. |
| **2. Data diddling** | i. Altering data during the IPO (Input-Process-Output) cycle. |
| **3. Data leakage** | f. Copying company data, such as computer files, without permission. |
| **4. Identity theft** | a. Illegally obtaining confidential information, such as a Social Security number, about another person so that it can be used for financial gain. |
| **5. Round-down** | j. Placing truncated decimal places in an account controlled by the perpetrator. |
| **6. Salami technique** | d. Embezzling small fractions of funds over time. |
| **7. Scavenging** | b. Searching through garbage for confidential data. |

**6.7 <para>Match the data security computer fraud and abuse technique in the left column with the scenario in the right column. Terms may be used once, more than once, or not at all.</para>**

|  |  |
| --- | --- |
| **1. Dictionary attack** | j. Using software to guess company addresses, send them blank e-mails, and adding unreturned messages to spammer e-mail lists. |
| **2. Hacking** | w. Gaining access to a computer system without permission. |
| **3. Logic bomb** | s. Software that sits idle until a specified circumstance or time triggers it. |
| **4. Malware** | l. Software used to do harm. |
| **5. Masquerading** | n. Pretending to be a legitimate user, thereby gaining access to a system and all the rights and privileges of the legitimate user. |
| **6. Password cracking** | c. Capturing and decrypting passwords to gain access to a system. |
| **7. Piggybacking** | e. Using a wireless network without permission. |
| **8. Posing** | x. Creating a seemingly legitimate business, collecting personal information while making a sale, and never delivering the item sold. |
| **9. Pretexting** | u. Acting under false pretenses to gain confidential information. |
| **10. Rootkit** | q. Software that conceals processes, files, network connections, and system data from the operating system and other programs. |
| **11. Shoulder surfing** | v. Observing or listening to users as they divulge personal information. |
| **12. Skimming** | f. Covertly swiping a credit card in a card reader that records the data for later use. |
| **13. Social engineering** | r. Methods used to trick someone into divulging personal information. |
| **14. Software piracy** | p. Unauthorized copying or distribution of copyrighted software. |
| **15. Steganography** | g. Concealing data within a large MP3 file. |
| **16. Superzapping** | a. Special software used to bypass system controls. |
| **17. Trap door** | i. Entering a system using a back door that bypasses normal system controls. |
| **18. Trojan horse** | k. Unauthorized code in an authorized and properly functioning program. |
| **19. Virus** | b. A segment of executable code that attaches itself to software. |
| **20. Worm** | m. A program that can replicate itself and travel over networks. |
| **21. Zero-day attack** | h. Attack between the time a software vulnerability is discovered and a patch to fix the problem is released. |

**6.8 Match the data security computer fraud and abuse technique in the left column with the scenario in the right column. Terms may be used once, more than once, or not at all.</para>**

|  |  |
| --- | --- |
| **1 Address Resolution Protocol (ARP)** | 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. |
| **2 Buffer overflow attack** | j. So much input data that storage is exceeded; excess input contains code that takes control of the computer. |
| **3 C</inst></wol>Carding** | x. Verifying credit card validity. |
| **4 Caller ID spoofing** | r. Displaying an incorrect phone number to hide the caller’s identity. |
| **5 Cyber extortion** | u. A demand for payment to ensure a hacker does not harm a computer. |
| **6 Cyber bullying** | q. Using social networking to harass another person |
| **7 Economic espionage** | v. Theft of trade secrets and intellectual property. |
| **8 E</inst></wol>E-mail spoofing** | k. Making an electronic communication appear as though it originated from a different source. |
| **9 IP address spoofing** | l. Creating packets with a forged address to impersonate another computing system. |
| **10 Internet auction fraud** | w. Using a site that sells to the highest bidder to defraud another person |
| **11 Internet pump-and-dump fraud** | <listitem><para><inst>g. Using the Internet to inflate a stock price so it can be sold for a profit. |
| **12 Lebanese looping** | a. Inserting a sleeve to trap a card in an ATM, pretending to help the owner to obtain a PIN, and using the card and PIN to drain the account. |
| **13 Man-in-the-middle (MITM) attack** | t. A hacker placing himself between a client and a host to intercept network traffic. |
| **14 Podslurping** | c. Using a small storage device to download unauthorized data from a computer. |
| **15 Ransomware** | s. Software that encrypts programs and data until a payment is made to remove it. |
| **16 Scareware** | e. Malicious software that people are frightened into buying. |
| **17 Sexting** | h. Exchanging explicit messages and pictures by telephone. |
| **18 SQL Injection** | i. Inserting a malicious database query in input in a way that it can be executed by an application program. |
| **19 SMS spoofing** | n. Changing the name or number a text message appears to come from. |
| **20 XSS attack** | 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. |
| **21 Tabnapping** | 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.**

Each of these real-world scenarios were taken from news accounts of computer fraud and abuse. There may be other valid answers, but the answers shown below are what the news accounts and experts investigating the case said were used to perpetrate the fraud.

|  |  |
| --- | --- |
| **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.”** | Hacking |
| **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.** | Password cracking |
| **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.**  | Denial of service attack |
| **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.** | SMS spoofing |
| **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.** | Salami technique |
| **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.** | Round-down fraud |
| **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.** | Cyber-extortion |
| **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.** | Denial-of-service attack used to perpetrate cyber-terrorism |
| **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.** | Phishing |
| **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.**  | Pharming |
| **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.** | Evil twin |
| **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.** | Key logging |
| **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.** | Trojan horse |
| **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.** | Time/logic bomb |
| **o. A man accessed millions of ChoicePoint files by claiming in writing and on the phone to be someone he was not.** | Pretexting |
| **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.** | Worm/virus. Although it was called the Melissa virus, it was actually a worm |
| **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.** | Scareware |
| **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.**  | SQL injection attack inserted code that redirected victims to malicious Web servers. |
| **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.** | A Trojan virus inserted a keystroke logger on computers. These computers created a botnet that captured and sent bank data to hackers who sold it.  |
| **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.** | The program that caused the pop-ups was Hotbar adware. |
| **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.** | * Fraudsters used **identity theft** tactics (such as **phishing)** to get victim’s Ameritrade account information.
* **Social engineering** tactics were used to get Ameritrade to process the transfers.
* A telephone **denial of service** attack gave the attacker time to drain the victim’s financial accounts.
 |
| **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.** | **Cyber-extortion**. The **email threat** was sent to extort $800 from the victim and his family. |
| **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.** | This is **vishing (**phishing done by voice instead of email).  |

**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.**

This case is based on an actual attack. The solution represents the actual events of the attack and the hospital's response.

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

By 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.

The problem does not state how the problem was finally fixed. What actually happened is that on Tuesday the hospital's antivirus vendor figured out which malware the hackers had used to get into the network and wrote a virus signature that blocked new code from coming in. Together with the code the internal IT staff wrote, the hospital was able to clean up its computers. All of the infected computers had to have their hard drives wiped clean and their software reinstalled, at an estimated cost of $150,000.

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

The primary attack used was a Zero-day attack that exploited a newly found weakness in Microsoft’s operating system that did not yet have a patch written to correct the weakness. The perpetrators hacked into the hospital's network and used various forms of malware, including adware (pop-up ads) and worms.

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

The hospital's network is now protected by Computer Associate's Pest Patrol, which blocks adware and spyware, and Cisco MARS, an intrusion detection system. Northwest's I.T. staffers no longer wait for vendors, particularly Microsoft, to certify software patches before applying fixes—they evaluate and test patches themselves. In the case of the attack, the Windows flaw that the attack slipped through had not yet been patched on the hospital's PCs. Fortunately, the hospital's servers escaped the attack because they had been patched.

**Aftermath:**

The hackers were a 19-year old California man, Christopher Maxwell, and two juveniles. Based in part on evidence supplied by the hospital, Maxwell pleaded guilty to conspiracy and intentionally causing damage to a protected computer. He was sentenced to 37 months in federal prison and ordered to pay $112,500 in restitution to the hospital.

**SUGGESTED ANSWERS TO THE CASES**

**6.1** **1. How did Shadowcrew members concealed their identities?**

* Used aliases when working online
* Communicated via proxy servers
* Rented commercial mailboxes under false names

**How can average citizens protect their identities while interacting online?**

* Use discretion in revealing personal information online. Individuals who use chat rooms, for instance, should avoid identifying themselves with their actual names, birthdays, or other identifying information.
* Do not give out personal information online unless absolutely necessary.

**2. How has the Internet made detecting and identifying identity fraudsters difficult?**

By using aliases, fraudulent email accounts, and proxy servers, thieves make it difficult to detect and punish deviant behavior.

**3. What are some of the most common electronic means of stealing personal information?**

* Accessing public and victim-provided data
* Phishing and spoofing
* Pharming
* Posing
* Spyware and keylogging
* Skimming and chipping

**4. What is the most common way that fraudsters use personal data?**

The most common way that fraudsters use personal data is to commit credit card fraud. This may include abuse to existing accounts or the opening of new, fraudulent accounts. Credit card fraud accounts for 26% of identity fraud cases.

**5. What measures can consumers take to protect against the online brokering of their personal data?**

* Avoid giving out their personal data – online or otherwise – whenever possible.
* Avoid filling out online surveys or polls that request identifying information.
* Make sure that websites are secure before submitting any personal information.
* If store clerks request information like name, phone number, or address when you are making a purchase, question the necessity of providing such information.

**6. What are the most effective means of detecting identity theft?**

* Regularly monitoring credit reports
* Checking account statements thoroughly
* Review the annual Social Security Personal Earnings and Benefits Estimate Statement

See Focus 9-1 for more information of detecting identity theft

1. **What pieces of personal information are most valuable to identity fraudsters?**
* Name
* Address
* Date of birth
* Social Security number (SSN)
* Driver’s license number
* Mother’s maiden name
* Account numbers
* Card expiration dates
* Internet passwords
* Personal Identification Numbers (PIN)
* User IDs for online account access
* Security numbers from back of credit and debit cards
* Other identifying information

**The rest of the story:**

One of the results of Operation Firewall was the convictions of Andrew Mantovani, Chad Hatten, and James Ancheta.

* Mantovani, a 24-year-old college student and a Shadowcrew co-founder, was sentenced to 32 months in federal prison, a $5,000 fine, and three years of probation.
* Hatten, a 36-year-old, received 90 months in federal prison, 24 months for “aggravated identity theft” and 66 months for access device fraud. Hatten must also endure three years of supervised release.
* James Ancheta, a 21-year-old “bot” creator that seized control of more than 400,000 computers to install revenue-generating adware and sold his bots to other users, was sentenced to 57 months in federal prison for his crimes. Ancheta was ineligible for parole and restricted from touching a computer until three years after his release.