TION

Computer-assisted crimes, such as identity theft and stalking, were discussed in Chapter 14, "White Collar Crime and Larceny." In such crimes the computer is a tool used to assist in the commission of the offense. **Cybercrime** differs from computer-assisted crime in that the computer itself is the target.

This chapter explores the conditions that had to exist before cybercrime could emerge; offenders and offenses; the differences between traditional crime and cybercrime; cybercrime tools and services; the types of computer intrusions that make cybercrime possible; and other related topics.

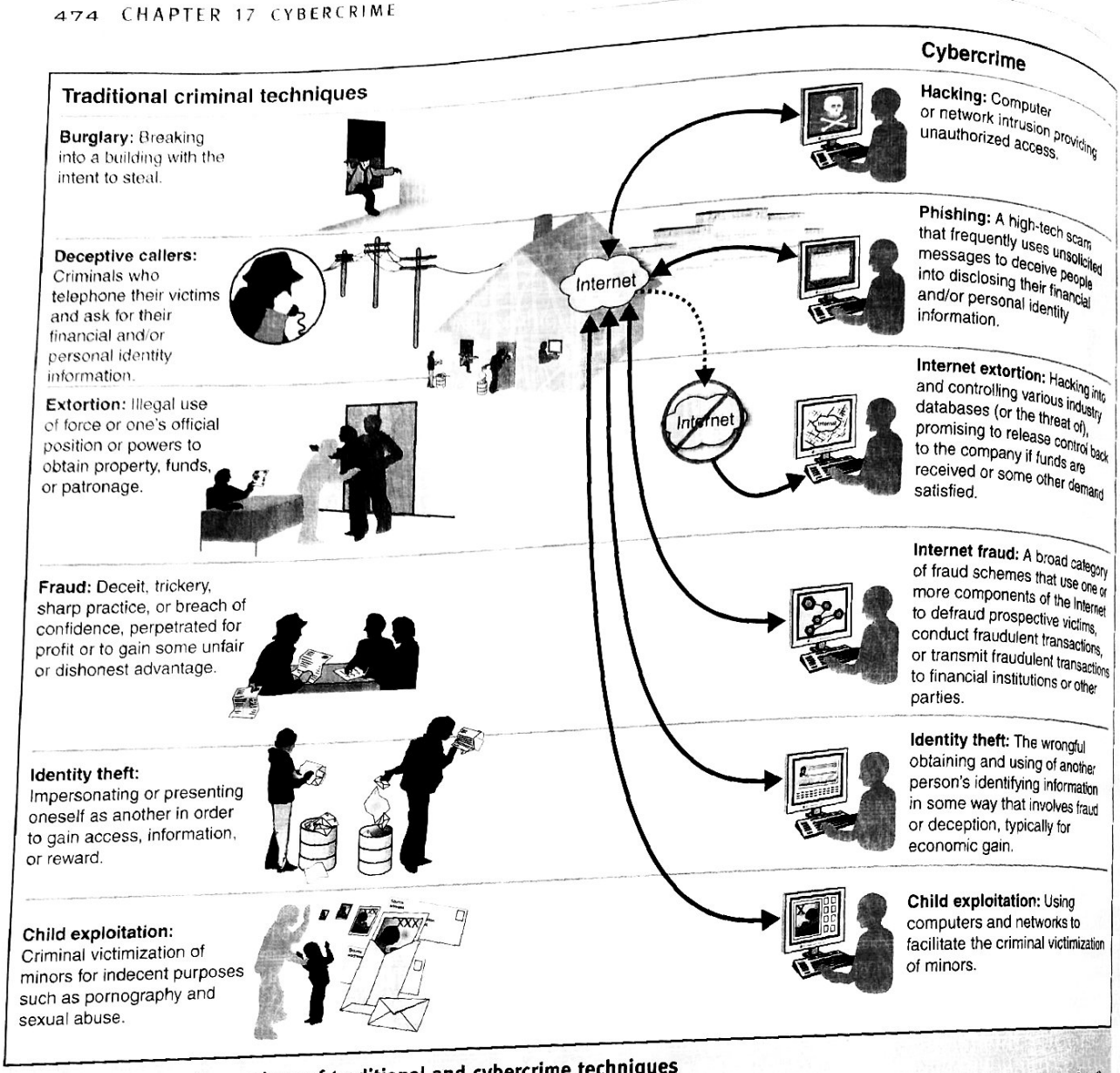
CHAPTER OUTLINE

CYBERCRIME: AN OVERVIEW

Cybercrime is more profitable than illegal drug trafficking.[1] In 2009 worldwide costs to consumers and businesses exceed 1 trillion dollars,[2] 8 billion of it occurring in the United States, where 20% of online consumers were victimized in a single year.[3] Their median loss was $575.[4]

There were two prerequisites for the emergence of cybercrime: (1) computers had to be commonplace, and (2) they had to be linked in a network. The first electronic computer was built in 1942, and the first personal computer (PC) was the Kenbak-1, introduced in 1971, although fewer than 50 were ever built. Radio Shack began selling the TRS-80 in the late 1970s; IBM jumped into the PC market in 1981; and the Apple Macintosh appeared three years later. Joseph Licklider, in 1962, conceived of what is now called the Internet, with his idea of a "Galactic Network." A rudimentary form of the Internet, ARPANET, was publically demonstrated in 1972, the same year Ray Tomlinson developed e-mail. In those early years the Internet was largely used only by the government and universities. However, the rapid development of the PC market and the commercialization of the net in the early 1990s quickly led to a worldwide network; the first online service provider for consumers was Delphi (1992). Presently, over 200 million Internet searches are performed daily.[5]

The satisfaction of the two prerequisites set the stage for a new breed of criminals who (1) didn't have to leave the comfort of their homes to commit crimes; (2) were invisible/anonymous, avoiding the dangers of personal contact with their victims; (3) could strike anywhere in the world; (4) were enabled to approach thousands of potential victims simultaneously; (5) executed crimes that victims might never detect or be too embarrassed to report; (6) committed crimes that might be discovered only much later, hampering investigations; (7) stood to reap profits far beyond those associated with conventional crimes; and (8) didn't have to worry about fencing tangible stolen property—for example, televisions and cars—because what they stole was intangible property—for instance, they looted checking, savings, and casino accounts.[6] Figure 17-1 illustrates some of the differences between traditional and cybercrime techniques.



▲ **FIGURE 17-1 Comparison of traditional and cybercrime techniques**
(No author, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats* [Washington, D.C.: General Accountability Office, June 2007], p. 6)

CYBERCRIME TOOLS AND SERVICES RELATED TO THEFT AND FRAUD

Cybercrime tools and services are being mass marketed on the Internet. They are found on publicly accessible web forums, such as Internet Relay Chat (IRC); the major vendors are principally located in Russia, Eastern Europe, and Malaysia.[7] Sellers and buyers also communicate by ICQ software (pronounced "I seek you"). Table 17-1 summarizes three major categories of cybercrime tools and services related to theft and fraud.

Buying malicious tools and services on the Internet from anonymous vendors in foreign countries has resulted in many would-be cybercriminals being scammed and left empty handed. These "wannabes" are in no position to complain to anyone about their losses, and "honest" malicious tools and services vendors, referred to as "verified sellers,"[8] stand to lose potential sales if their industry is generally seen as fraudulent. As a result, independent "guarantors" often act as the middlemen in the sales process for 3–5% of the selling cost, ensuring that the exact terms of the contract are met.[9] Guarantors hold the buyer's money, verify that the software works as advertised, and then transmit the money to the vendor and the product to the buyer.

TABLE 17-1 Cybercrime Tools and Services

TOOLS/SERVICES	DESCRIPTION	PERCENTAGE OF MARKET SHARE
Malicious Software	Ready to run crimeware is often purchased on the Internet—e.g., viruses, worms, and spyware. Cost ranges from less than $10 for a simple virus to over $5,000 for advanced capability programs. The Trojan horse is the most commonly sold malicious software at approximately $750 per copy. (Malicious software is discussed later in this chapter.) Some sites offer free downloads of older versions of malicious software that may be useable or that places a virus on the downloader's computer.	39
Cybercrime Services	Examples include distribution of spam and pop-up messages, and denial of service attacks to shut down websites.	34
Stolen Data	Includes bank, savings, checking, credit card, PayPal, iTunes, and casino account numbers; user names and passwords; identity documents—for example, data from scanned passports—are also available to assume new identities or engage in fraud. Offenders may use or sell data "harvested."	27

Source: Bill Chu, Thomas J. Holt, and Gail Joon Ahn, "Examining the Creation, Distribution, and Function of Malware On-Line," (Washington, D.C.: U.S. Department of Justice, March 2010), pp. 7–8, with some changes and additions.

OFFENDERS AND OFFENSES

Not so long ago, computer enthusiasts hacked into computers out of curiosity or for excitement. Now, the overwhelming motive is for financial gain. Hackers/crackers who use their skills to illegally make money are called **"black hatters"**; those who use them for good—for example, for identifying security risks in computer systems and notifying corporations and other entities of their vulnerability—are designated as **"white hatters."**

Cybercrime is a major source of profit for some transnational criminal organizations (TCOs).[10] During the first six months of 2010, cyberattacks increased from 60 million to nearly 180 million.[11] Hong Kong Triad groups are funding the academic education of some members to acquire degrees in computer science, software engineering, and information systems in order to commit lucrative cybercrimes.[12] Al Qaeda is also acquiring cybercrime expertise to fund its operations.[13]

The triads are in competition with other TCOs, including well-educated members of groups in Russia and Eastern Europe; this competition is so keen that recently the black market price for stolen credit card numbers has dropped from 7$ to 10$ to 1$.[14] **"Carders"** are cybercriminals who primarily profit from selling stolen credit card numbers. MasterCard International reported that in a single year more than 40 million consumer credit card numbers were accessed by hackers.[15] In 2011 Sony reported that sensitive information was stolen from 102 million user accounts.

In cases for which perpetrator data is available, 76% of cybercriminals are male, and most range in age from 14 to 30 years. Hackers are often described as "antisocial loners," which is not very useful for investigators. More helpful is Table 17-2, a taxonomy or classification scheme that categorizes cybercriminals by type, characteristics, motivation, and skill. This table is not a fixed hierarchy of offenders, but it does provide a framework for thinking about the capabilities and threats posed by different cybercriminals. To a degree, Table 17-2 is limited in that it represents "pure" categories, when in fact cyberoffenders may be active in several different categories. Table 17-3 summarizes data about cybercrime perpetrators and complainants. It suggests that offenders have a preference not to victimize people living in the offenders' own state.

COMPUTER INTRUSIONS

Computer intrusions are accomplished by the use of malware, a term derived from combining *mal*icious and soft*ware*. **Malware** is intended to (1) deny use of computers; (2) covertly gain control over computers, for example, through the use of a Remote Administrator Tool (RAT);

TABLE 17-2 Taxonomy of Cybercriminals

TYPE	CHARACTERISTICS	MOTIVATION	SKILL LEVEL
1. Novice	• Limited computer/programming skills • Use software ("tool kits") written by others, e.g., SpyEye, IcePack, XRumer, and KanBe, which cost from $700 to several thousand dollars • Referred to as "script kiddies" or "script bunnies" • Commit simple cybercrimes, e.g., virus attack	• Thrill seeking • Ego enhancement • Prove themselves to others • Collect "trophies"	Low
2. Cyberpunks	• Higher skills than novices • Can write some of their own programs • Better understanding of systems they attack • Deface web pages, send spam • Many engage in account data thefts, cyberfraud	• Media attention • Financial gain	Moderate
3. Internals/ Insiders	• Often information technology (IT) professionals • Represent greatest risk because in position of trust • Historically have triggered great losses • Inflated sense of their importance/value • Have strong sense of entitlement	• Typically revenge • Feel slighted, e.g., not promoted • Disgruntled, seek to "right" a "wrong" done to them	High
4. Petty Crooks	• Some are making transition from novice or street to cybercrimes • Not interested in notoriety/attention, keep low profile • May work to obtain requisite skills, e.g., attend technical school • May show a progression in skill or interest over time, such as moving to professional criminals category	• Greed, financial gain • In small number of cases may act out of revenge, e.g., former employer, ex-girl/boyfriend	Moderate
5. Virus Writers	• Often in transition to some other category • Age of VWs varies • Stop or shift to another category during mid- to late-20s	• Mixed motives • Motives may be similar to novices and petty criminals	Very high
6. Old Guard Hackers	• Generally have no criminal intent • However, disregard for others' property may cause operational interruption or other losses • Enjoy technical challenge of hacking • Write but generally do not use tool kits they sell to novices	• Curiosity • Need for challenges	Very high
7. Professional Criminals	• Some number are well trained former intelligence operatives—Russia, Eastern Block European countries and some Asian gangs • Crime is their career field • Seldom arrested; convicted even less often • Choose lucrative targets, e.g., banks, casinos, intellectual property (e.g., games, movies, recipes) • Fully exploit the potential of the Internet as a crime tool • Apolitical, will commit national security espionage for profit, even against their own governments • "Guns for hire," if the price for accepting a "project" is right • High tolerance for risk	• Money and financial gain • Life-style attractive	Very high

CONTINUED

TABLE 17-2 CONTINUED

	CHARACTERISTICS	MOTIVATION	SKILL LEVEL
8. Information/ Espionage Warfare	• Targets are defense industry corporations to nations • Disrupt, destabilize, corrupt, exploit, or otherwise compromise operational capabilities, e.g., production schedules, satellites, military unit communications, and data integrity/reliability • Theft of national security information, e.g., stealth capabilities of aircraft and submarines, weapons in development • May be conducted, or sponsored by corporate competitors, a national government, or contracted with professional criminal gangs	• Highly trained, skilled, and experienced, • May be very patriotic • Profit motivation may be primary	Highest

Source: Markus Rogers, "A Two-Dimensional Circumplex Approach to the Development of a Hacker Taxonomy," *Digital Investigation*, Vol. 3, Issue 2, 2006, pp. 98–100, with some changes and additions.

TABLE 17-3 Cybercrime Perpetrators and Complainants per 100,000 People

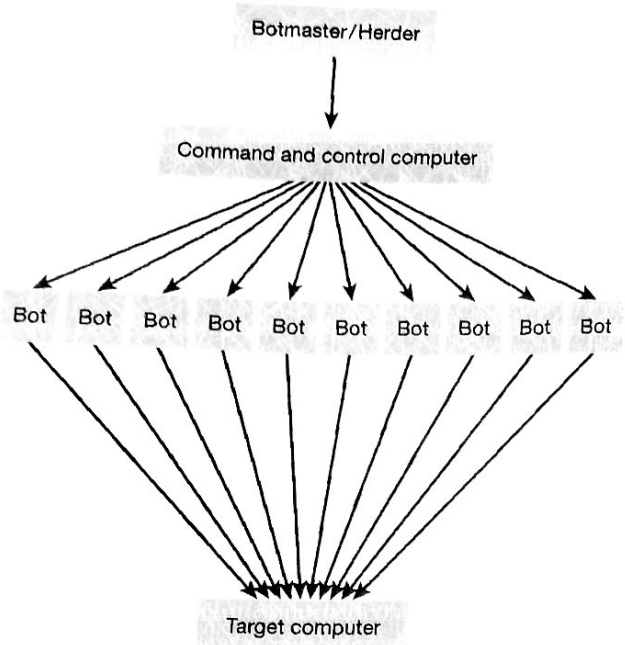
RANK	STATE	PERPETRATORS PER 100,000 PEOPLE	RANK	STATE	COMPLAINANTS PER 100,000 PEOPLE
1	District of Columbia	116.00	1	Alaska	485.91
2	Nevada	106.73	2	New Jersey	166.74
3	Washington	81.33	3	Colorado	143.21
4	Montana	68.20	4	Nevada	135.75
5	Utah	60.22	5	District of Columbia	131.90
6	Florida	57.28	6	Oregon	124.18
7	Georgia	56.99	7	Maryland	121.67
8	Wyoming	56.40	8	Arizona	121.01
9	North Dakota	51.01	9	Washington	120.56
10	New York	48.10	10	Florida	116.25

Source: No author, *2009 Internet Crime Report* (Washington, D.C.: Internet Crime Complaint Center, the National White Collar Crime Center and the Bureau of Justice Assistance, 2010), pp. 7 and 9.

(3) secretly access or intercept computer data; and (4) subvert the operation of computers for personal profit. Many of the techniques discussed in this section are being adapted for attacks on smartphones.

Although malware is often for a single purpose, the clear trend of cybercriminals is to use multipurpose or **"blended threat" malware** —for example, the ABC Virus, which includes spyware, control from remote sites, and data theft capabilities. Malware may be transmitted with downloaded images, a "spoofing" e-mail, which appears to come from a legitimate source, such as a bank; Valentine's Day and Christmas cards; files saved on CDs and flash drives that are shared with other users; fake free security software offers; "You have won an instant $100" messages; bogus news, storm, or sports reports; or by other means discussed in this chapter, such as drive-bys. This section addresses common malware intrusions; there is some inherent overlap in these categories—for instance, an infostealer Trojan horse can also be categorized as spyware.

1. *Botnets:* A **"herder" ("botmaster")** uses malware to hijack hundreds to tens of thousands of computers and is able to remotely control them all, including the ability to update the malware and to introduce other programs such as spyware. Hijacked computers are called **zombies** (robots, or **bots**). The malware creating the bot "lies low," waiting for commands from the herder and thus is difficult for security software to detect.



▲ **FIGURE 17-2 Typical botnet**

A **botnet** is a network of zombies or bots (Figure 17-2). The Georgia Institute of Technology estimates that globally 15% of all computers may be zombies.[16] The herder makes money from repeatedly selling clandestine botnet access to others to use for pop-up advertising or other purposes, at an average cost of 37 cents per week for each zombie.[17] A herder with 10 weekly clients for a botnet with 10,000 zombies could gross $1.9 million annually.

Computers are often hijacked by what appear to be legitimate e-mail messages. A growing method is **"drive-bys,"** which occurs as a user-unintended side-effect of visiting a website; Drive-bys are made possible by exploiting web browser vulnerabilities. For example, a person on Facebook sees a video on YouTube that friends might be interested in and sends the link to them. When the friends click on the link, the malware is surreptitiously installed. A variation of this involves seemingly innocent celebrity websites that are actually malicious; click on one, and a drive-by occurs. In 2009 Jessica Biel was the most dangerous celebrity site to visit; in 2010 it was Cameron Diaz; visits to celebrity websites creates a 10% chance of being a drive-by victim.[18]

2. *Viruses:* At any one time there may be as many as 16,000 viruses floating around. The *primary purpose* of a **virus** is to replicate as many times as possible and to cause as much mischief or damage as possible. A number of programs provide a good level of security from infection, including Norton, AntiVirus, McAfee, Intego, and Kaspersky.

A virus is an unauthorized software program that is surreptitiously inserted into an executable program on a single computer.[19] When a user launches the infected program, the virus looks for other executable programs in which to place a copy of its malicious code. Thus, the typical virus requires human intervention to spread itself. The user may spread the virus to other computers—for example, if it has attached itself to outgoing e-mail. Infected computers may run slower and slower as more programs are infected. The viruses can also reformat a hard drive, causing the loss of all data, or odd/taunting messages may appear on the screen.

Polymorphic and metamorphic viruses are similar in that they each make changes to their replicants to hide from security software, but they do so differently. A **polymorphic virus,** such as Virut, encrypts its replicant into an alternate form, but it must then decrypt itself back into its original form to execute. In contrast, a **metamorphic virus** completely rewrites itself each time it reproduces. No metamorphic replicant or "child" looks like its parent.

Worms are considered a variant or subclass of viruses and therefore are substantially similar to them. The key difference between the two is once inserted into a computer, a worm can distribute itself across the Internet without any action by the computer user because it is self-contained and does not have to be part of another software program.

One of the most famous worms was the e-mail that appeared in 2000 with the tag line of "I Love You." When recipients clicked on its "love letter" attachment, the virus was installed. Originating in the Philippines, this worm affected 10% of all Internet users in nine days by sending itself automatically to everyone on each infected computer's contact list. It is estimated that this virus created losses of $15 billion.[20]

The software security firm Sophos estimates that an unprotected computer connected for the first time to the Internet has a 40% chance of getting a worm within 10 minutes; that risk reaches 94% after an hour.[21]

In 2010, just two years after it was discovered, the Conficker worm had infected 7 million computers. Its encryption code is so sophisticated that only a small number of people would have the skill to write it; moreover, Conficker is adept at reappearing even after some antivirus packages have eliminated it.[22]

3. *Time, logic, and e-mail bombs:* A **time bomb** is programmed to "go off" at a particular time or date, such as April Fool's Day, Halloween, or Friday the 13th. A **logic bomb** is "detonated" when a specific event occurs—for example, all personnel records are erased when an electronic notation is made that a particular person was fired. **E-mail bombs** are

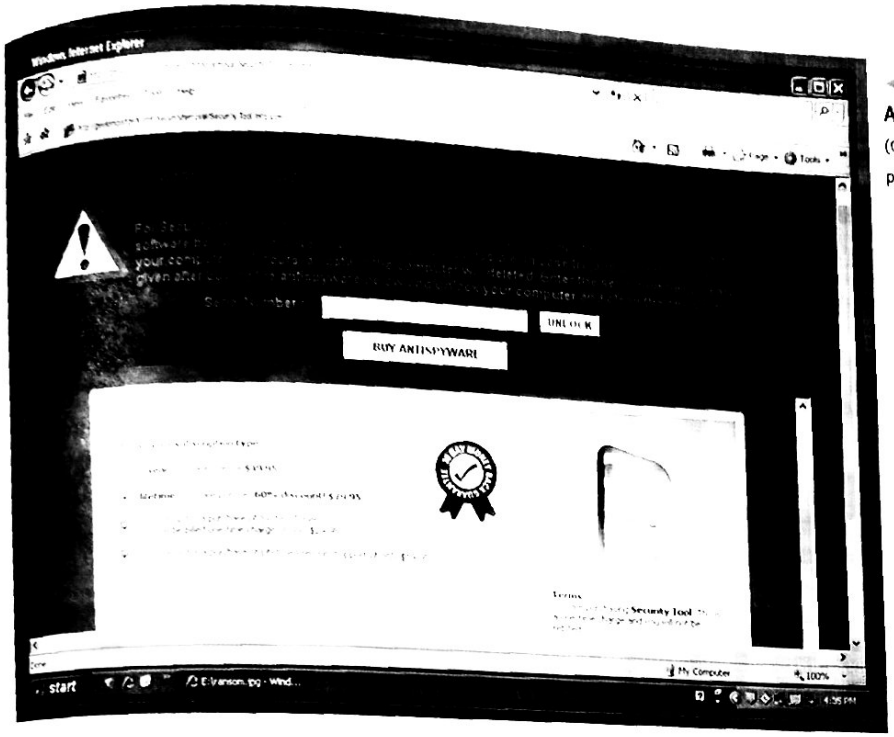


FIGURE 17-3
A typical ransomware message
(© McGraw-Hill Companies, Inc./Mark Dierker, photographer)

intended to overwhelm a person's e-mail account by surreptitiously subscribing it to dozens or even hundreds of mailing lists. Alternatively, 10 knowledgeable people might be able to collectively send 650,000 e-mail messages in an hour to a single user's account. In such circumstances, the Internet service provider usually suspends the use of the e-mail account, disrupting the ability of the victim to use it. Such a circumstance is called a **denial of service (DoS)** attack.

On a larger scale, a botnet herder can use all of his/her zombies to overwhelm even the largest servers, in a **distributed** (across the botnet) **denial of service (DDoS)** attack. DDoSers are also referred to as **flooders,** and their known corporate victims include Yahoo!, Amazon, and CNN. In 2007 Tallinn, Estonia, decided to relocate a Soviet-era monument from the center of the city to the suburbs. Two days of rioting by ethnic Russians was followed by DDoS attacks against Estonian agencies. Many believe that the attacks were conducted by or on behalf of the Russian government.

DDoS threats can also be used for extortion. Russian gangs successfully extorted millions of dollars from 50 online casinos and betting businesses in 30 different countries by threatening such attacks; the profitability from remaining online 24 hours a day was greater than the extortion paid by the victims.[23]

4. *Ransomware:* Also known as a cryptovirus, **ransomeware** holds the data on a computer or the use of the computer hostage until a payment is made (Figure 17-3). Ransomware encrypts the target's files—for example, through a CryZip Trojan—and the attacker tells the victim to make a payment of a specified amount to an E-Gold, a Yandex, or a WebMoney account to receive the decryption key.[24] Alternatively, the attacker requires the victim to prepay for a certain value of goods with a specific business in a foreign country. The goods are used or traded by the attacker, or the "business" may simply exist on paper and the attacker receives the ransom from the sale of it.

   Ransomware encryption methods are too sophisticated to be easily cracked, and pressure is placed on the victim by the notification "For every 30 minutes that goes by without full payment, one file will be deleted."[25] Although ransomware attacks have been aimed primarily at businesses, individual personal computer users have also been victimized with the demanded payment in the $200–$300 range.

   Movieland, also known as Moviepass.tv and Popcorn.net, allegedly puts displays or plays music on a computer that cannot be closed or turned off. Movieland's creators claimed the "users" did not pay the required $29.95 for the program after the trial period, and users state that their systems were being held hostage.[26]

5. *Dead drop:* To avoid personal contact, intelligence agents use a location called a **dead drop** or drop zone to leave and pick up messages. Similarly, some cybercriminals prefer to distance themselves from incriminating files; they use another computer or server, a virtual dead drop, sometimes

called an egg drop or drop zone, on which to store the data they have stolen.[27] The attackers sell the data or use it to commit cybercrimes themselves.

6. *Trojan horse:* There are numerous platforms for delivering **Trojan horses.** One way is to offer what appears to be legitimate software program with a title that mimics a well-known package that many users may try, such as a free download of a "Web Accelerator." The Trojan horse piggybacks on the Web Accelerator download. In another version, a pop-up appears on the screen with "Yes" and "No" buttons to answer the question "Do You Want to Optimize Your Internet Access?" No matter which button is pushed, the Trojan horse is downloaded. Another pop-up that functions in the same manner is a window that offers some type of a browser plugin.

   Symantec, a leading antivirus company, recognizes three categories of Trojans: (1) backdoor, with a primary purpose of establishing the opportunity for remote access at some later time; (2) downloader, with the main goal of facilitating the downloading of some other type of software, most usually additional malware; and (3) infostealer, with an objective of stealing information, such as account names, numbers, and passwords.[28]

7. *Spyware:* **Spyware** is a broad term that sometimes is used to mean the same thing as malware but more narrowly is thought of as a surveillance tool, such as the infostealer form of a Trojan horse. Webroot, an antivirus software company, audited 19,480 businesses in 71 countries and found an average of 19 pieces of spyware.[29] Crimes involving stolen passwords result in losses of $2.75 billion annually.[30]

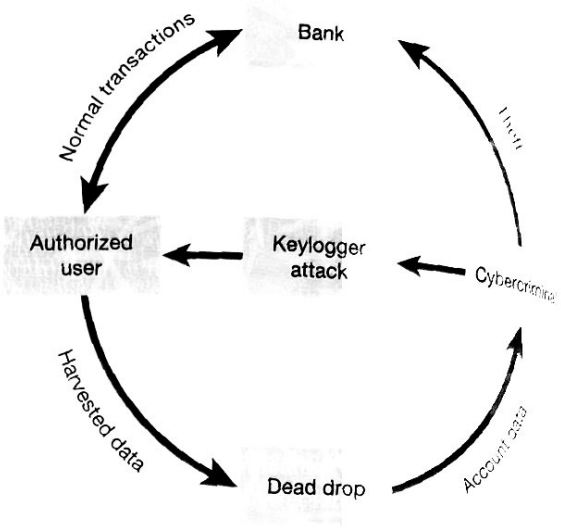
   A keystroke logger, referred to as a keylogger, may be the most common form of spyware. As shown in Figure 17-4, a **keylogger** secretly "harvests" every keystroke that a computer user makes and thus steals sensitive data for profit.

   Keyloggers may be hardware or software. KeyGhost makes a hardware version that is roughly the size of a small thumb and is easily installed. The keyboard cord is plugged into the keylogger, which in turn is inserted into the back of the computer. There are two families of keylogger software: (1) ZeuS, Zbot, and Wsnpoem, whose attack channel is spam e-mails that trick users into opening them, and (2) Limbo2 and Nethel, which are downloaded as a drive-by when users visit a malicious website.[31] There are over 200 unique programs designed to steal passwords via keylogging.[32]

   Some spyware is relatively benign, learning what sites a user visits on the Internet to shape marketing strategies. However, an accumulation of benign spyware slows down a computer's speed.

8. *Rootkits:* In many computer operating systems (OSs), the "root" is a "superuser" account for system administration. A "kit" is the malware introduced into the computer. A **rootkit** gives an attacker "super powers" over computers—for example, the ability to steal sensitive personal information.

   Rootkits—for instance, TDSS—are considered the most sophisticated type of malware and are quickly emerging as the largest intrusion threat to computers.[33] There are at least five different "flavors" of rootkits. A common one, after being introduced into a computer, alters the OS so that it can remain hidden indefinitely. Rootkits do not replicate or ordinarily do not cause damage to files.



▲ **FIGURE 17-4 Keylogger attack**

9. *Scareware:* A **scareware** attack often starts with a pop-up message on your screen, "Virus Activity Detected!" claiming that your computer has a virus—and for $19.95 you can download antivirus software to fix the problem (Figure 17-5). The unwary user who buys the software thinks the problem is resolved, but the software is really useless and delivers malware, and the vendor sells the user's credit card number. In 2010 a new method of delivering scareware, using a bogus update to the Firefox web browser, was discovered in England.

INVESTIGATION OF CYBERCRIMES

FEDERAL EFFORTS

The FBI and the United States Secret Service (USSS) have prominent roles in investigating computer assisted cybercrimes. The FBI has a four fold mission in this area: (1) to stop those behind the most serious

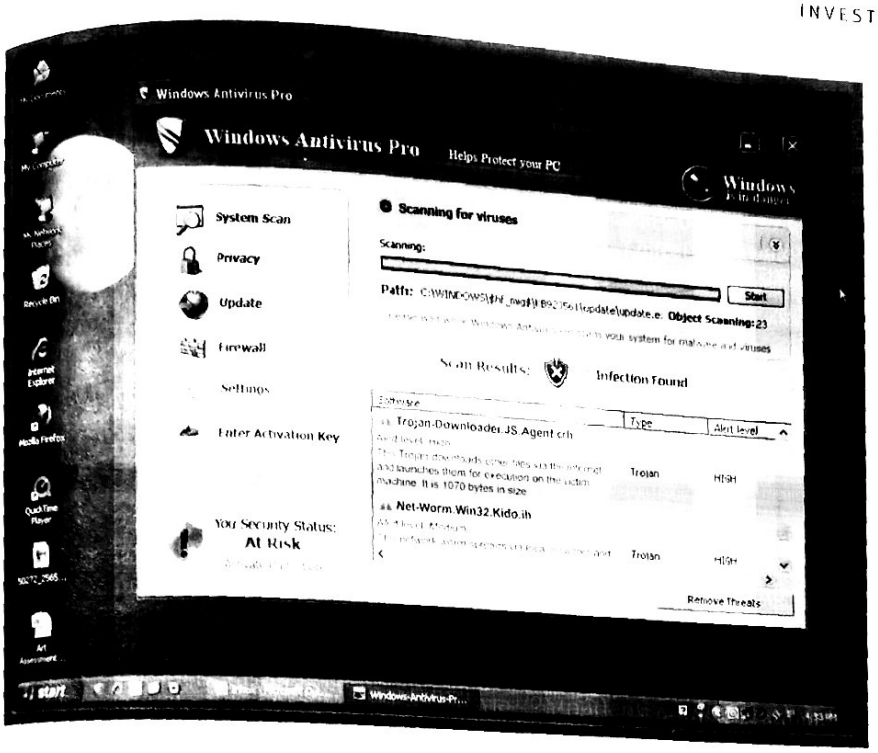


FIGURE 17-5
Typical scareware message
(© McGraw-Hill Companies, Inc./Mark Dierker, photographer)

intrusions and the spread of malware; (2) to identify and thwart online sexual predators who use the Internet to meet and exploit children and those who produce, possess, or share child pornography; (3) to counteract operations that target U.S. intellectual property, endanger national security or competitiveness; and (4) to dismantle national and transnational organized criminal enterprises engaging in Internet fraud.

The USSS has broad jurisdiction to investigate computer crimes, including unauthorized access to protected computers, identity theft, DDoS attacks involving disruption of e-commerce or extortion, and distribution of malware. The USSS has established Electronic Crimes Task Forces (ECTFs) (Figure 17-6) in approximately 20 cities across the country, bringing together the expertise of federal, state, and local agencies and representatives from industry and the academic community. The mission of ECTFs is the prevention, detection, mitigation, and aggressive investigation of attacks on the United States' financial institutions and critical infrastructures.

Many federal agencies participate on ECTFs and lead or serve on other investigative task forces (TFs) spread

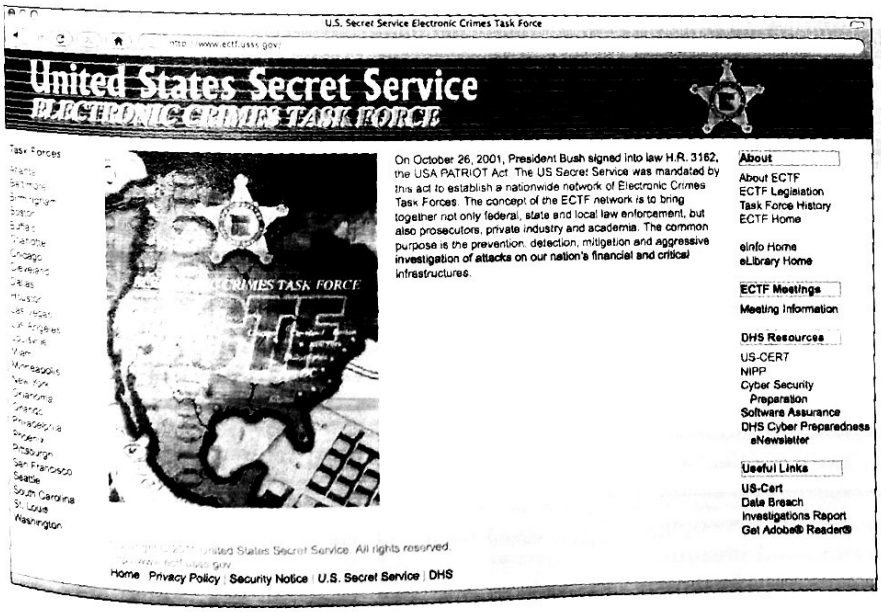


FIGURE 17-6
Website for the United States Secret Service Electronic Crimes Task Force

across the country. Among the federal agencies participating in these efforts are United States Attorney's Offices, the FBI, United States Postal Inspection Service (USPIS), and the U.S. Immigration and Customs Enforcement (ICE). The Social Security Administration (SSA) participates in approximately 100 such TFs. Many of these TFs are aimed at specific computer assisted crimes, such as identity theft, advance fee schemes, and exploitation of children.

STATE AND LOCAL EFFORTS

Computer/cyber/high-technology/electronic crime units are commonly found in all larger municipal and county agencies, although their mission, expertise, and capabilities vary widely. As departmental size decreases, so does the probability that such units exist. These "poor cousins" and larger agencies both face barriers to establishing and growing an effective computer-, cyber-, or electronic-crimes unit, because: (1) the needs for, and benefits of, an electronic crimes unit are not well understood; (2) many local agencies cannot alone afford to provide adequate office space, purchase the necessary hardware and software, or dedicate and train the staff required; (3) administrators are reluctant to engage in the hard and uncertain work of recruiting qualified information technology partners from industry and the academic community; (4) support for such units is often nonexistent or low, especially for administrators who are trying to meet more basic service delivery needs; (5) the inability to fully staff such units means that where they do exist, their mission may be restricted to a few crimes—for example, identity theft, child pornography, online child predators, cyberbullying and stalking, and nondelivery of merchandise ordered online—because the "unit" consists of a single officer; (6) it is difficult to retain trained and experienced officers; (7) existing laws may be inadequate; and (8) prosecutorial expertise may be lacking.[34]

Of necessity, many local agencies depend on the computer-crime expertise of their state investigative agency, state police, or state patrol. These state agencies are often staffed with a combination of officers trained in computer-crime investigation and civilian information technology specialists. In addition to a staff located at headquarters, qualified personnel are usually located within troop commands or other geographical districts. These agencies also operate TFs, as do State Attorney Generals and local prosecutors. A number of local agencies have also cooperated in founding their own units, the services of which are shared.

LEGAL CONSIDERATIONS

Federal laws pertaining to computer-assisted and cyber-crimes are comprehensive, although the corresponding state statutes vary in their sophistication and breadth. As with other types of crime, investigators must be thoroughly familiar with the applicable federal and state laws. In particular, knowledge of the federal Electronic Communications Privacy Act (ECPA) of 1986 and its subsequent amendments is essential. ECPA violations may result in criminal charges being brought against officers, personal civil liability, and the suppression of evidence. Therefore, investigators should be guided by their department's policies and those of the local prosecuting authority.

CONSENT SEARCHES

Search and seizure were discussed in Chapter 2, "Legal Aspects of Investigation." Consent searches are revisited here within the personal computer-crime context, because unlike warrant applications there is no judicial official screening to guide investigators' actions when a consent search is sought in the field.[35]

Whenever reasonably possible, investigators' should seek a warrant. However, many times a request to search on the basis of consent may be a sound, even prudent, course of action, because a consent search does not require probable cause. To avoid conflicting accounts that may arise later, the party granting consent should execute a written consent form (Figure 17-7) prepared by the local prosecuting authority. When the examination of a computer system is contemplated, the consent form should specify in broad terms that computer and other electronic evidence may be searched. Computer case law continues to evolve, and the discussion here is for general information and is not a guide to authoritative practice.

The general rules for **consent searches** is that the police can rely on a person's *actual authority* to consent to a search or the *apparent authority* of such other parties they reasonably believe can grant a search of the premises—for example, an adult guest who has "the run of the household" while the owners are absent.[36]

The consent must be freely and voluntary given; police threats such as "Let us look at your computer files or we'll arrest your girlfriend and take away your children" will nullify the consent.[37] Different fact situations determine whether investigators can conduct a consent search:

1. If the persons with actual or apparent authority to consent are not native English speakers and appear to lack meaningful comprehension, the burden is heavier on the government to show the consent was voluntary.[38] It must be demonstrated *before* the search that such persons comprehended the situation well enough to understand the action to which they consented.
2. The extent of a consent search is limited by the subject and scope of the consent—for example, consent to "search the computer in my son's room" does not extend to household computers located elsewhere.

CONSENT TO SEARCH FORM

I, _____, presently residing at _____ have been informed of my right to refuse to consent to a search. I have not been promised anything nor have I been threatened in any manner. My consent is given freely and voluntarily. I have been advised that I can modify or withdraw my consent at any time.

I authorize and consent to a search of the _____ by _____ located at _____ personnel as he/she shall designate, including any containers of each and every kind.

The officer(s) are authorized by me to seize and take custody of any notes, letters, pages, papers, records, materials or other property, including computers, together with all of their components, related processing and internal and external storage devices, scanners, routers, printers, display monitors, modems, and any and all accessories and property the officers believe to be pertinent to their investigation.

The officer(s) are authorized by me to search for and seize electronic data within the authority, consent, and scope given above. The officer(s) may use any means to search any or all files, including deleted, encrypted, and password protected files.

I also authorize the officer(s) to remove to another place(s) they deem appropriate any property, equipment, or other material related to their investigation, to sort out, read, examine, analyze, evaluate, test, and reproduce it. I also authorize these actions by those the officer(s) may designate to perform them.

Date: _____ Time: _____

Signature of Consenting Party: _____

Witness Signature: _____

Witness Signature: _____

◄FIGURE 17-7
Consent to search form oriented toward personal computers
Source: Priscilla Adams, Consent Searches (Oxford, Mississippi: National Center for Justice and the Rule of Law, University of Mississippi Law School, 2010), p. 6 with modifications.

In *United States v. Stierhoff* (549 F.3d 19, 2008) a defendant suspected of stalking signed a broadly worded consent form for the Rhode Island State Police to search the room he rented as a residence and in which his computer was located. Over $140,000 in cash and financial records in the room suggested the possibility of a separate tax evasion case. When investigators began examining his computer, Stierhoff verbally narrowed his consent to the files containing his "love poems." However, the police also opened a file labeled "Offshore," which deepened their suspicions about tax evasion. Later that night, investigators, with a separate consent form from Stierhoff, searched the defendant's storage unit and found more evidence of tax evasion. The Internal Revenue Service was notified. Stierhoff was later convicted at separate trials of stalking and failure to pay taxes on over $1 million during a four-year period. His lone "victory" was that both the tax evasion trial and appeal courts agreed that the evidence from the "Offshore" file was not admissible. This case illustrates that consent may be modified or withdrawn at any time.

United States v. Wong (334 F.3d 831, 2003) shows the importance of being patient and using a warrant when possible. The investigation of a murder led to the seizure of a computer under warrant. The investigator later obtained a search warrant to have it forensically examined for graphic files pertaining to the case. Child pornography was found, which the court held was a plain view exception to the Fourth Amendment.

3. When a person is asked for permission to search personal computers in a home, his/her mere silence does not rise to consent. If investigators falsely tell a person "we have a warrant to search your computer" the fruits of the search are not admissible.
4. Consent to enter a home does not constitute authority to conduct a search. A nonverbal gesture to "come in" is sufficient to enter the premises. Although mere entry does not authorize a search, investigators can act on plain view offenses—for example, child pornography pictures or drugs lying on a table.

5. Among those who cannot give law-enforcement officers consent to search private living areas for computers or other purposes are landlords and apartment managers. Under some rental agreements they may be able to enter and inspect for an agreement violation—for instance, if a nonpermissible pet is on the premises, if the tenant is given reasonable notice, if the manager does so at a reasonable time and conforms to other related provisions of the agreement. If evidence of a crime is observed—for instance, credit-card-making machines or computers being used to produce counterfeit currency—the manager's information can form the basis of probable cause for a search warrant. However, if the manager's intention is actually to "get the goods" on tenants and is essentially acting as a law-enforcement officer, the evidence will be inadmissible.

   Dormitory, sorority, and fraternity managers, and usually medical and administrative staff with respect to a patient's room, cannot give consent when there is a reasonable expectation of privacy.[39] Hospital security personnel responsible for protecting a patient's possessions, such as a laptop, do not appear to have a right to surrender them to investigators. Hotel managers cannot normally give consent to search private rooms, although they can if tenants have terminated their occupancy or eviction proceedings have been completed.
6. Spousal and domestic partner search consents for domiciles may be valid depending on the circumstances. If a spouse or partner is absent, consent by the other is usually approved by the courts. Even so, the courts have imposed restrictions; in *Trulock* v. *Freeh* (275 F.3d 391, 2002) a housemate consented to a search of the computer she shared jointly with her boyfriend; both accounts on the computer were password protected. The police found incriminating evidence in the boyfriend's account, but the court refused to admit the evidence on the basis that the use of a password created a reasonable expectation of privacy by him.

   If, however, the password is on a "sticky note" attached in plain view to the computer or has been shared with others, the courts may not be deferential to a claim of privacy. Encrypted files might create a privilege similar to password protected files. Short of password protection, defendants may claim an expectation of privacy based on instructions such as "no one is to use my computer except me" or keeping it locked up when not in use.

   If both spouses or partners are present and one affirmatively objects and the other consents, any search is unconstitutional (*Georgia* v. *Randolph* 547 U.S. 103, 2006). Under Randolph, the nonconsenting party must be physically present and immediately challenge any qualified co-occupant who consents.[40]

   In *U.S.* v. *Groves* (530 F. 3d 506, 2008) the question arose whether police could strategically plan to avoid the presence of a potentially nonconsenting cotenant. Groves was a convicted felon who did not consent to a search of his residence, shared with a live-in girlfriend. Three weeks later, knowing Groves was at work, the police revisited the Groves domicile and were granted entry by the girlfriend. The court held the search was constitutional because Grove was not "objecting at the door," and the police had no role in removing him from it.
7. Parents ordinarily have unlimited authority to consent to searches over the dissent of their children who are under 18 years old and living at home, because there is a recognized hierarchy in the family. However, if juveniles have created "private space," such as footlockers to which only they have a key, a right to privacy claim might be raised. If their children are older than 18 years, a parent may in some circumstances be able to give consent. However, if children are older than 18, pay rent, and have asserted their right to deny access to their room, the courts have held that parents' consent to search that private space is not valid.
8. Montana appears to be the only jurisdiction that has clear guidance as to whether a minor child can consent to a search of their parent's home; a child there who is 16 years or older may be able to authorize a search in the absence of both parents. Elsewhere, the fact situation will guide whether children can do so. As the Supreme Court noted, no one "would reasonably expect an eight-year-old to be in a position to authorize anyone to rummage through his parents' bedroom."[41] The authority of minors to consent to a search of their parents' home and computers has no "bright line" test.

   A search warrant is a better option than relying on the uncertain authority of a child. Nonetheless, *before* acting on a child's consent, investigators' should pursue a rigorous line of inquiry to determine if it is *reasonable* to believe such authority is valid. The courts will closely scrutinize the basis on which the police acted on the consent of children, including their, age, maturity, physical and mental state, intelligence, education, and the instructions their parents gave them—for example, "don't let anyone in the house unless it's an emergency."
9. The courts have held differently on whether a computer-repair person may allow the police access to a computer being repaired that has evidence on it. Some states have laws requiring computer-repair services to report crimes they detect—for example, credit card fraud.

   In *United States* v. *Grimes* (244 F.3d 375, 2001), the defendant's wife brought her husband's computer to a repair shop with the complaint that it wouldn't boot up. Subsequently, the repairman called the

wife and reported that there were a lot of image files, and he recommended deleting some of them, which the wife authorized. In the process of determining which files might be deleted, 17 pornographic images were discovered and reported to a local detective, who looked only at the 17 images and did not request that the repairman examine the remaining image files. The 17 files were copied on a floppy and given to an FBI agent, who patiently obtained a warrant to seize the computer, which was held to be lawful by the court.

10. Those on parole or probation may have their releases based on conditions creating diminished Fourth Amendment rights that approximate consent. In *United States* v. *Herndon* (501 F.3d 683, 692, 2007) a warrantless search of a probationer's computer was upheld, based on reasonable suspicion that he had violated the terms of his probation. Herndon's release prohibited him from using the Internet, and he was required to allow his probation officer to search his computer at any time for such use. After Herndon told his probationer officer he was using the Internet to look for a job, the officer drove to his residence and searched an external hard drive, finding child pornography. The court upheld the search, noting that Herndon's privacy rights were "dramatically reduced" by the terms of his release and the government's legitimate interest in preventing his recidivism.
11. *Routine* searches at border crossings or other points of entry into or departure from this country do not require a warrant, probable cause, reasonable suspicion, or consent. In *United States* v. *Arnold* ((523 F.3d 941, 946, 2008) the court ruled that reasonable suspicion was not required to search a laptop or other personal electronic devices, because it was a nondestructive intrusion akin to searching luggage. This decision did not address border searches involving password protected or encrypted files.

    More intrusive *nonroutine* searches of people that involve their dignity and privacy—for example, strip and body-cavity searches—require a degree of reasonable suspicion; destructive searches—for instance, cutting open panels in a car to look for drugs—fall into this category also.[42]
12. Although outside the scope of consent searches, it is noted that inventory searches that discover evidence of a crime are admissible if the searches are conducted pursuant to a departmental policy that is uniformly followed in similar cases and the inventory has a legitimate non-investigatory intent—for example, protection of the property of an arrestee. However, because the intent is to protect tangible personal property, it is unlikely that the examination of the files on a computer inventoried from the trunk of an impounded vehicle would pass judicial scrutiny.

THE CRIME SCENE

COMPUTER AND PERIPHERAL EVIDENCE

Evidence related to computer-assisted and cybercrimes is subject to the same fundamentals of crime processing that were discussed earlier. Important evidence may be associated with many items, including tablets, computer notebooks and laptops, desktops, rack systems, and main frames, as well as external hard drives, printers, scanners, compact disks, flash drives, memory card readers, web cameras, and wireless access points and network servers. The existence of a wireless network should alert investigators to the possibility that evidence may also be located on devices located away from the primary crime scene, such as in another room or a garage.

Search warrants may be issued to cover both the seizure of the targeted computers and peripherals and the actual digital forensic examination of them, or separate search warrants may be used.

CRIME SCENE PROCESSING

If the resources are available, trained and experienced computer investigators are the best choice for processing a cybercrime scene. In many jurisdictions this option may not exist, and so the first responding officer will have that responsibility. In all instances, investigators must be sure of their legal authority to search and any applicable limits.

This section is not a definitive guide to processing computer crime scenes, which is properly covered by in-service training covering a full range of situations, such as searching corporate computers that may hold trade secrets and other confidential information. It does provide a perspective on common situations, but a department's policy is the definitive source for action.

Securing and Evaluating the Scene

1. Remove and exclude all persons from the area where evidence is to be collected.[43] Do not accept advice or assistance from "volunteers" whose actual motive may be to destroy evidence or misdirect the investigation.
2. If a wireless system is involved, direct non-investigative personnel to stay in a particular room until the possibility of potential evidence in rooms beyond where the computer is located is determined. If several persons of interest and/or suspects are present, they should be placed in separate rooms.
3. If a computer and other devices are off, leave them off. If they are on, do not move them, press any keys, check for DVDs, or click the mouse, because changes or damage to evidence may be triggered. If the computer is on but the screen is blank, *very slightly* move the mouse to see what information is displayed.

4. If the computer's power state cannot be immediately determined, look and listen for indications that it is on—for example, fans running, drives spinning, and light-emitting diodes (LEDs), and observe the monitor to see if the machine is on, off, or in a sleep mode.
5. If the computer is on, check the display for signs that files are being deleted or overwritten, such as the words *delete, format, remove, destroy, copy, move,* or *wipe*. Also check the monitor for signs that the computer is being remotely controlled. In all these cases, the immediate disconnection of power is recommended.
6. If the destruction of evidence is not a concern, the immediate disconnection of power is not recommended, because information, data, and images of apparent evidentiary value may be seen on the screen and photographed—for instance, financial documents, child pornography, identities of coconspirators/other suspects, text documents, chat rooms used. In such cases, assistance from investigators qualified to capture volatile data is essential.
7. If no destructive processes are running and if there is no information of evidentiary value on the screen, remove the power cord from the back of the computer.
8. Do not attempt to examine the computer's contents. This is highly technical and specialized work that should be undertaken only by qualified personnel.

Preliminary Interviews

In addition to other information, the following should be established:

1. Who owns the computers? For example, the homeowner, a renter, or a business?
2. Who uses the computer and its related devices? What are their login names, user account names, and instant messaging screen names?
3. What are the passwords for any password-protected accounts, and are any files encrypted? Whose accounts are these?
4. What e-mail, personal web, or social networking websites, such as MySpace and Facebook, accounts exist, whose are they, and what passwords are used?
5. What data-access restrictions, destructive devices or software, or automated applications are in use?
6. For wireless networks, where is all accessible equipment located?
7. Who provides the Internet service?
8. Whose name is on the Internet bill, and who actually pays the bill?
9. How is the Internet accessed? For example, cable, modem, Digital Subscriber Line (DSL), Wi-Fi, or T-1 leased service, which normally involves 20 or more people online simultaneously.

Documenting the Scene

1. Both in the report and by video and photography, identify the location, type of devices, their condition, and power status. Get views of all sides, including the backs, where cables are attached.
2. Record all activity and processes visible on the monitor.
3. Note all devices physically connected to the computer as well as the same for wireless components. Record their serial numbers, the content of "sticky notes" attached to them, and related written information.
4. Note the condition and power status of the computer's network access.
5. Document, photograph, and sketch all wires, cables, and devices connected to, or inserted in, the computer.
6. Tag every cable as to where each end was attached.
7. Document and photograph every wireless device in the locations at which they were found.
8. Document and photograph the locations of related evidence, such as printed pages of Internet addresses, financial records, images, and computer code, GPSs/maps/directions, electronic money transfers, books on hacking, software packages, lists of computers accessed and dead drops, credit card information, reproductions of signatures, checks and money orders, diaries and calendars, mail in victims' names, cash, fictitious identification, passwords and information on encryption and steganography. ("Steg" or "Stego" has been used for thousands of years. Historically, steg means writing in a cipher or code so that only the sender and the recipient know what the message means. In the context of computers, steg means hiding a file in a larger file so that others are not aware of its presence or meaning.)

Collecting and Transporting Evidence

The following steps should be followed when collecting and transporting computers and related devices:

1. Remove batteries from laptops and place tape over the power switch on all computers and associated devices. Disk-drive trays should also be taped closed.
2. Place all digital evidence in **antistatic packaging;** do not use regular plastic bags or other containers that can produce static electricity and condensation, both of which can damage or destroy evidence. Antistatic bags and packaging is often colored—for example, pink or light blue—to distinguish them from regular evidence bags, and they may have bubble wrap built into them to protect evidence. If antistatic bags or packaging are not available, wrap the evidence in sturdy manila/kraft paper.

3. Each computer and peripheral should be placed in a separate container to avoid cross-contamination. In some investigations, examining them for DNA evidence may become an important possibility.
4. Carefully pack all evidence to prevent it from being damaged from shock and vibration while being transported.
5. Keep digital evidence away from magnetic fields—for instance, those produced by radio transmitters and magnetically mounted emergency lights. Other transportation hazards include prolonged exposure to heated seats, hot car interiors and trunks, and static electricity produced by shuffling feet on carpets. Prolonged exposure to cold and humidity are also threats.
6. Regular procedures for handling other types of evidence, such as maintaining the chain of custody, should be carefully followed.

KEY TERMS

antistatic packaging
black hatters
blended threat malware
bot
botmaster
botnet
carder
computer-assisted crime
consent search
cybercrime
dead drop
denial of service (DoS) attack
distributed denial of service (DDoS) attack
drive-by
e-mail bomb
flooder
herder
keylogger
logic bomb
malware
metamorphic virus
polymorphic virus
ransomware
rootkits
scareware
spyware
time bomb
Trojan horse
virus
white hatters
worms
zombies

REVIEW QUESTIONS

1. How are computer-assisted and cybercrimes contrasted?
2. What two prerequisites were fulfilled before cybercrime could emerge?
3. What six advantages do cybercriminals have over traditional criminals?
4. What is malware?
5. How do black hatters and white hatters differ?
6. What is a botnet?
7. What is the primary purpose of a virus?
8. How are DoS/DDoS attacks carried out?
9. What is a drive-by?
10. How are scareware attacks executed?
11. Is there a difference between polymorphic and metamorphic viruses?
12. What is ransomware?
13. What are the basic components of a keylogger attack?
14. What are the general rules for a consent search?
15. What are major points of securing a computer crime scene?