Privacy, Security, and Ethics

▲ Download the free *Computing Essentials 2014* app for videos, key term flashcards, quizzes, and the game, *Over the Edge!*

Competencies

After you have read this chapter, you should be able to:

1. Identify the most significant concerns for effective implementation of computer technology.
2. Discuss the primary privacy issues of accuracy, property, and access.
3. Describe the impact of large databases, private networks, the Internet, and the web on privacy.
4. Discuss online identity and the major laws on privacy.
5. Discuss cybercrimes including creation of malicious programs such as viruses, worms, Trojan horses, and zombies as well as denial of service attacks, Internet scams, social networking risks, cyberbullying, rogue Wi-Fi hotspots, theft, and data manipulation.
6. Detail ways to protect computer security including restricting access, encrypting data, anticipating disasters, and preventing data loss.
7. Discuss computer ethics including copyright law, software piracy, digital rights management, the Digital Millennium Copyright Act, as well as plagiarism and ways to identify plagiarism.

Why should I read this chapter?

In the past, protecting your privacy and security was pretty simple. You needed a paper shredder and perhaps an unlisted phone number. That was then and this is now. Now, in the digital age, personal security and privacy are much more complicated and difficult. Every minute there are thousands of malicious programs that are being spread across the Internet.

This chapter discusses privacy including identity theft, cookies, web bugs, and keystroke loggers. Additionally, you'll learn about viruses, worms, rogue Wi-Fi hotspots, and the risks associated with Facebook and other social networking sites. You will also learn how to protect your computer security using a variety of techniques including biometric scanners and encryption. To be competent and to be competitive in today's professional workplace, you need to know and to understand these things.

chapter 9

Introduction

Hi, I'm Anthony, and I'm an IT security analyst. I'd like to talk with you about privacy, security, and ethics, three critical topics for anyone who uses computers today. I would also like to talk about how you can protect your privacy, ensure your security, and act ethically.

The tools and products of the information age do not exist in a world by themselves. As we said in Chapter 1, an information system consists not only of procedures, software, hardware, data, and connectively but also of people. Because of people, computer systems may be used for both good and bad purposes.

There are more than one billion microcomputers in use today. What are the consequences of the widespread presence of this technology? Does technology make it easy for others to invade our personal privacy? When we apply for a loan or for a driver's license, or when we check out at the supermarket, is that information about us being distributed and used without our permission? When we use the web, is information about us being collected and shared with others?

This technology prompts lots of questions—very important questions. Perhaps these are some of the most important questions for the 21st century. Competent end users need to be aware of the potential impact of technology on people and how to protect themselves on the web. They need to be sensitive to and knowledgeable about personal privacy and organizational security.

People

As we have discussed, information systems consist of people, procedures, software, hardware, data, and connectivity. This chapter focuses on people. (See Figure 9-1.) While most everyone agrees that technology has had a very positive impact on people, it is important to recognize the negative, or potentially negative, impacts as well.

Effective implementation of computer technology involves maximizing its positive effects while minimizing its negative effects. The most significant concerns are

- **Privacy:** What are the threats to personal privacy, and how can we protect ourselves?

Figure 9-1 People are part of an information system

- **Security:** How can access to sensitive information be controlled, and how can we secure hardware and software?
- **Ethics:** How do the actions of individual users and companies affect society?

Let us begin by examining privacy.

Privacy

As you have seen, computing technology makes it possible to collect and use data of all kinds, including information about people. The websites you visit, the stores where you shop, and the television shows you watch are all examples of information about you. How would you feel if you learned such information was being collected or shared? Would it matter who was collecting it, or how it was being used, or whether it was even correct?

Privacy concerns the collection and use of data about individuals. There are three primary privacy issues:

- **Accuracy** relates to the responsibility of those who collect data to ensure that the data is correct.
- **Property** relates to who owns data and rights to software.
- **Access** relates to the responsibility of those who have data to control who is able to use that data.

Large Databases

Large organizations are constantly compiling information about us. The federal government alone has over 2,000 databases. Every day, data is gathered about us and stored in large databases. For example, telephone companies compile lists of the calls we make, the numbers called, and so on. A special telephone directory (called a **reverse directory**) lists telephone numbers sequentially. (See Figure 9-2.)

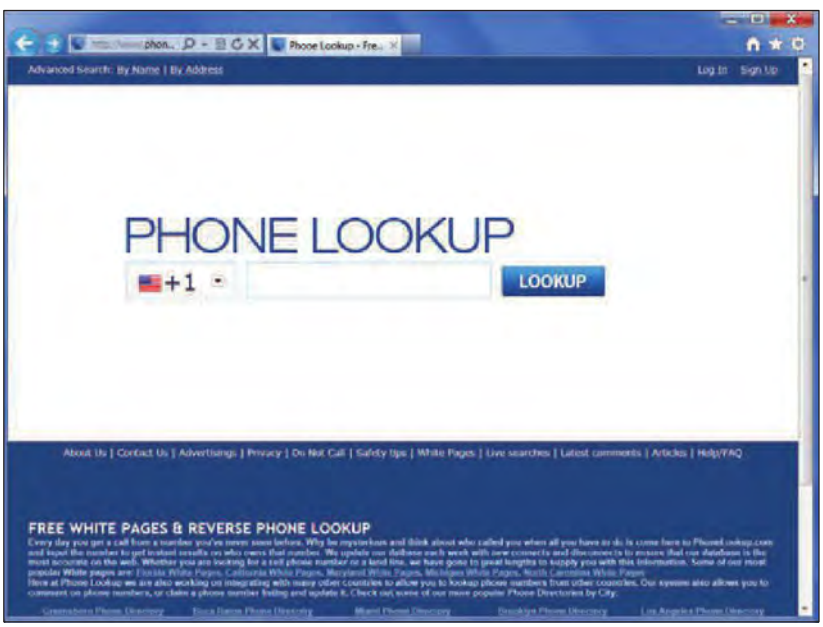


Figure 9-2 Reverse directory website

By entering just a telephone number, you can determine the name, address, and more information about the person registered with that number.

Credit card companies maintain user databases that track cardholder purchases, payments, and credit records. Supermarket scanners in grocery checkout counters record what we buy, when we buy it, how much we buy, and the price. Financial institutions, including banks and credit unions, record how much money we have, what we use it for, and how much we owe. Publishers of magazines, newspapers, and mail-order catalogues have our names, addresses, phone numbers, and what we order. Search engines record the search histories of their users including search topics and sites visited.

A vast industry of data gatherers known as **information resellers** or **information brokers** now exists that collects and sells such personal data. Using publicly available databases and in many cases nonpublic databases, information resellers create **electronic profiles** or highly detailed and personalized descriptions of individuals. Very likely, you have an electronic profile that includes your name, address, telephone number, Social Security number, driver's license number, bank account numbers, credit card numbers, telephone records, and shopping and purchasing patterns. Information resellers sell these electronic profiles to direct marketers, fund-raisers, and others. Many provide these services on the web for free or for a nominal cost. (See Figure 9-3.)

Your personal information, including preferences, habits, and financial data, has become a marketable commodity. This raises many issues, including

- **Collecting public, but personally identifying information:** What if people anywhere in the world could view detailed images of you, your home, or your vehicle? Using detailed images captured with a specially equipped van, Google's Street View project allows just that. Street View makes it possible to take a virtual tour of many cities and neighborhoods from any computer with a connection to the Internet. (See Figure 9-4.) Although the images available on Street View are all taken in public locations, some have objected to the project as being an intrusion on their privacy.

Figure 9-3 Information reseller's website

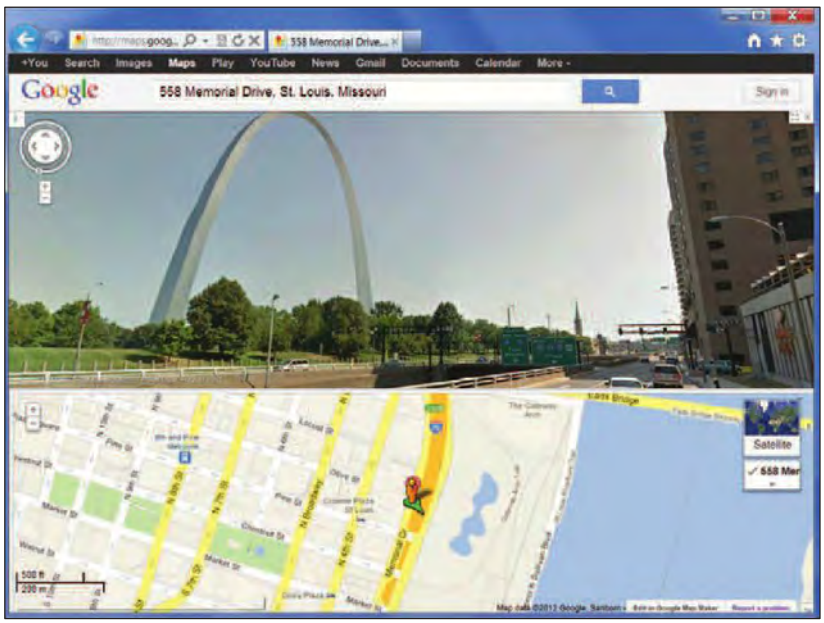


Figure 9-4 Google Street View

As digital cameras and webcams become cheaper and software becomes more sophisticated, it is likely that many more issues involving personal privacy in public spaces will need to be addressed. Such a combination of computing technologies could, for example, make real-time tracking of individuals in public places possible.

- **Spreading information without personal consent:** How would you feel if an employer were using your Facebook, Google+, or other social networking profiles to make decisions about hiring, placement, promotion, and firing? It is a common practice today for many organizations.

How would you feel if someone obtained a driver's license and credit cards in your name? What if that person then assumed your identity to buy clothes, cars, and a house? It happens every day. Every year, nearly 10 million people are victimized in this way. It is called **identity theft**. Identity theft is the illegal assumption of someone's identity for the purposes of economic gain. It is one of the fastest-growing crimes in the country. To learn more about identity theft and how to minimize your risk, visit our website at www.computing2014.com and enter the keyword **theft**.

- **Spreading inaccurate information:** How would you like to be turned down for a home loan because of an error in your credit history? This is much more common than you might expect. What if you could not find a job or were fired from a job because of an error giving you a serious criminal history?

tips

Identity theft is a growing problem, and can be financially devastating if you are a victim. Thieves are after anything that can help them steal your identity, from your Social Security number and date of birth to account information and passwords. Here are some steps to help protect your identity.

1. Be careful what you write on the Internet. Never post personal information on forums or social networking areas that are public or in response to an e-mail from someone you do not know or trust.
2. Only do business on the Internet with companies you know to be legitimate.
3. When selling a computer, be sure to completely remove all personal information from the hard drive.
4. Monitor your credit. Each year, you are entitled to a free personal credit report from each of the three major credit reporting agencies. Monitor your credit by requesting a report every four months from a different reporting agency. The official site for this service is www.annualcreditreport.com.

To see more tips, visit our website at www.computing2014.com and enter the keyword tips.

This can and has happened due to simple clerical errors. In one case, an arresting officer while completing an arrest warrant incorrectly recorded the Social Security number of a criminal. From that time forward, this arrest and the subsequent conviction became part of another person's electronic profile. This is an example of **mistaken identity** in which the electronic profile of one person is switched with another.

It's important to know that you have some recourse. The law allows you to gain access to those records about you that are held by credit bureaus. Under the **Freedom of Information Act**, you are also entitled to look at your records held by government agencies. (Portions may be deleted for national security reasons.)

concept check

What are the three primary privacy issues?

What are information resellers, electronic profiles, identity theft, and mistaken identity?

What is the Freedom of Information Act?

Private Networks

Suppose you use your company's electronic mail system to send a co-worker an unflattering message about your supervisor or to send a highly personal message to a friend. Later you find the boss has been spying on your exchange. This is legal, and a recent survey revealed that nearly 75 percent of all businesses search employees' electronic mail and computer files using so-called **employee-monitoring software**. (See Figure 9-5.) These programs record virtually everything you do on your computer. One proposed law would not prohibit

Figure 9-5 Employee-monitoring software

this type of electronic monitoring but would require employers to provide prior written notice. Employers also would have to alert employees during the monitoring with some sort of audible or visual signal. If you are employed and would like to know your company's current policy on monitoring electronic communication, contact your human relations department.

Explorations

Several organizations actively monitor privacy-related issues.

To learn more about one such organization, visit our website at www.computing2014.com and enter the keyword privacy.

The Internet and the Web

When you send e-mail on the Internet or browse the web, do you have any concerns about privacy? Most people do not. They think that as long as they are using their own computer and are selective about disclosing their names or other personal information, then little can be done to invade their personal privacy. Experts call this the **illusion of anonymity** that the Internet brings.

As we discussed in Chapter 8, every computer on the Internet is identified by a unique number known as an IP address. IP addresses can be used to trace Internet activities to their origin, allowing computer security experts and law enforcement officers to investigate computer crimes such as unauthorized access to networks or sharing copyright files without permission.

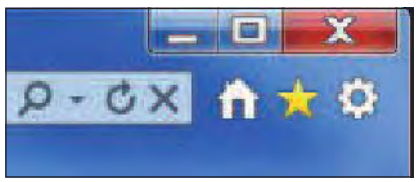
When you browse the web, your browser stores critical information onto your hard disk, typically without you being aware of it. This information, which contains records about your Internet activities, includes history and temporary Internet files.

- **History files** include the locations, or addresses, of sites that you have recently visited. This history file can be displayed by your browser in various locations, including the address bar (as you type) and the *History* tab. To view your browsing history using Internet Explorer 9, follow the steps in Figure 9-6.
- **Temporary Internet files**, also known as the **browser cache**, contain web page content and instructions for displaying this content. Whenever you visit a website, these files are saved by your browser. If you leave a site and then return later, these files are used to quickly redisplay web content.

Another way your web activity can be monitored is with **cookies**. Cookies are small data files that are deposited on your hard disk from websites you have visited. Based on your browser's settings, these cookies can be accepted or blocked. (See Figure 9-7). Although you will generally not be aware when a website generates a cookie, the personalized experiences you enjoy on the web are often a result of those cookies. While cookies are harmless in and of themselves, what makes them a potential privacy risk is that they can store information about you, your preferences, and your browsing habits. The information stored generally depends on whether the cookie is a first-party or a third-party cookie.

- A **first-party cookie** is one that is generated (and then read) only by the website you are currently visiting. Many websites use first-party cookies to store information about the current session, your general preferences, and your activity on the site. The intention of these cookies is to provide a personalized experience on a particular site. For example, when you revisit a particular electronic commerce site, a previously deposited cookie can provide information so that you can be greeted by name and presented with sales and promotions that interest you.

1 **Select the *Favorites* button.**



2 **Select *History*.**

Figure 9-6 Viewing history files

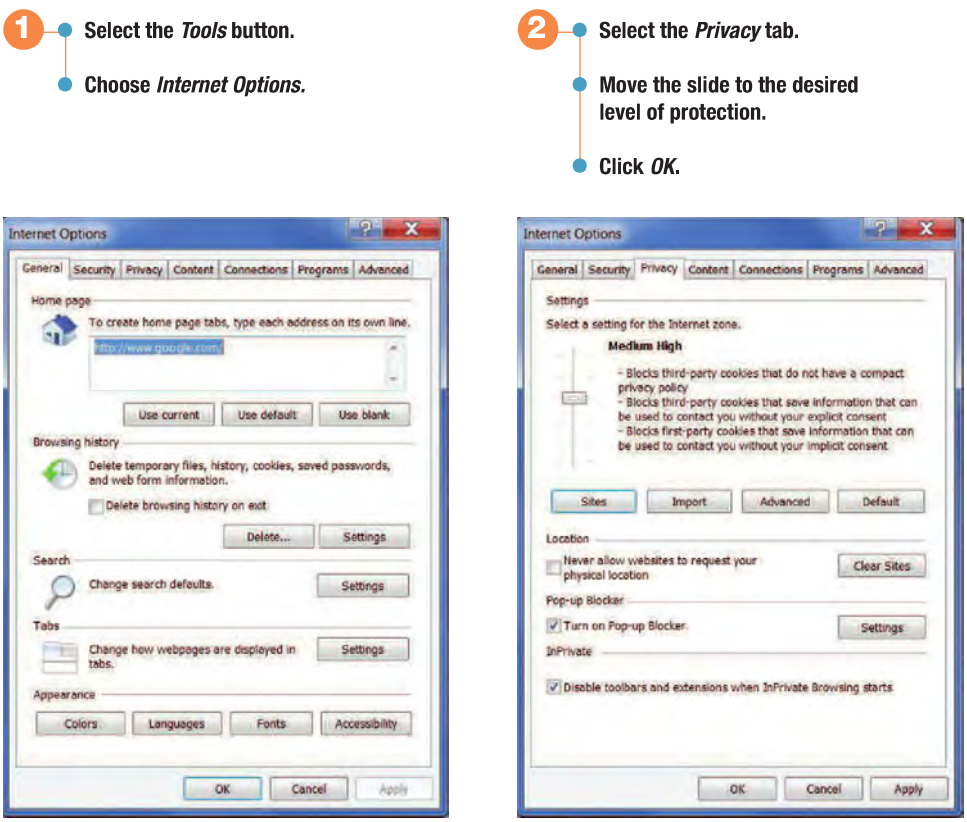


Figure 9-7 Blocking cookies

- A **third-party cookie** is usually generated by an advertising company that is affiliated with the website you are currently visiting. They are used by the advertising company to keep track of your web activity as you move from one site to the next. For this reason, they are often referred to as **tracking cookies**. Critics of this practice claim that your privacy is being violated because your activity is being recorded across multiple websites. Defenders of this practice argue that these cookies are beneficial because it helps websites deliver ads that interest you. For example, suppose you visit four different websites that employ the same advertising agency. The first three sites are about cars, but the fourth is a search engine. When you visit the fourth site, you will likely see a car advertisement because your cookie showed that you had been visiting car-related websites.

Some users are not comfortable with idea of web browsers storing so much information in the form of cookies, history, and temporary Internet files. For this reason, browsers now offer users an easy way to delete their browsing history. (See Figure 9-8.) In addition, most browsers also offer a **privacy mode**, which ensures that your browsing activity is not recorded on your hard disk. For example, Internet Explorer 9 provides **InPrivate Browsing** accessible from the *Tools* button, and Safari provides **Private Browsing** accessible from the *Safari* option on the main menu.

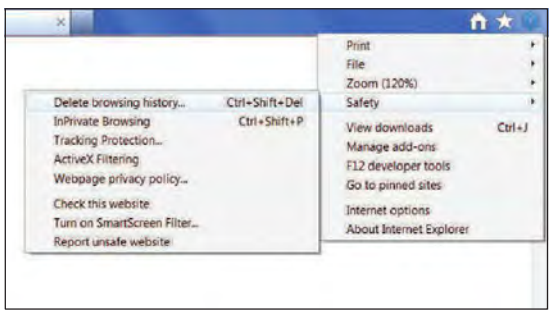
Although these web browser files can concern many individuals, several other threats could potentially violate your privacy. **Web bugs**, which are invisible images or HTML code hidden within a web page or e-mail message, can be used to transmit information without your knowledge. When a user opens an e-mail containing a web bug, information is sent back to the source of the bug. The receiving server will now know that this e-mail address is active. One of the most common web bugs is used by companies that sell active mailing lists to spammers. Because of this deception, many e-mail programs now block images and HTML code from unknown senders. It is up to the user to decide whether or not to allow such content to be displayed for current and future messages. To see how web bugs work, visit our website at www.computing2014.com and enter the keyword **bugs**.

The most dangerous type of privacy threat comes in the form of spyware. The term **spyware** is used to describe a wide range of programs that are designed to secretly record and report an individual's activities on the Internet. Some of these programs can even make changes to your browser in order to deceive you and manipulate what you see online. **Computer monitoring software**, also known as **keystroke loggers**, is perhaps the most invasive and dangerous type of spyware. These programs record every activity and keystroke made on your computer system, including credit card numbers, passwords, and e-mail messages. Computer monitoring software can be deposited onto your hard drive without your knowledge by a malicious website or by someone installing the program directly onto your computer. While such software is deadly in the hands of criminals, it can be legally used by companies monitoring employees or law enforcement officials who are collecting evidence.

Unfortunately, many spyware programs go undetected, largely because users have no idea they are infected. Spyware will run in the background, invisible to the average user. Other times, it disguises itself as useful software, such as a security program. Various studies have demonstrated that an alarming number of computers are infected with spyware. The financial impact to individuals, companies, and financial institutions is estimated at billions of dollars.

One of the best defenses against spyware is to exercise caution when visiting new websites and downloading software from an unknown source. Another defense involves using a category of software known as **antispyware** or **spy removal programs**, which are designed to detect and remove various types of privacy threats. (See Figure 9-9.) For a list of some of these programs, see Figure 9-10.

1. Select the *Tools* button.
   - Choose *Safety*.
   - Choose *Delete browsing history*.



2. Select check boxes for items to be deleted.
   - Choose *Delete*.

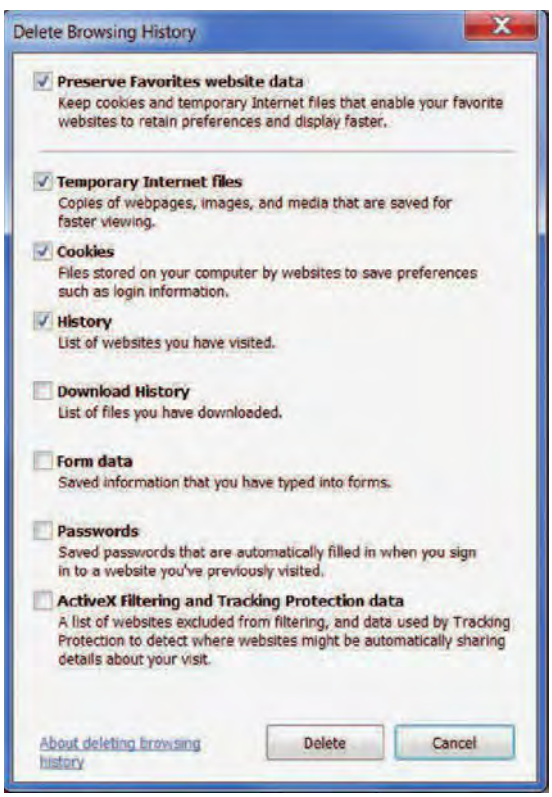


Figure 9-8 Deleting browsing

Figure 9-9 Antispyware

Program	Website
Ad-Aware	www.lavasoft.com
SUPERAntiSpyware	www.superantispyware.com
Spyware Doctor	www.spydoctor.com
Windows Defender	www.microsoft.com

Figure 9-10 Antispyware programs

Online Identity

Another aspect of Internet privacy comes from **online identity**, the information that people voluntarily post about themselves online. With the popularity of social networking, blogging, and photo- and video-sharing sites, many people post intimate details of their lives without considering the consequences. Although it is easy to think of online identity as something shared between friends, the archiving and search features of the web make it available indefinitely to anyone who cares to look. There are any number of cases of people who have lost their jobs on the basis of posts on social media websites. These job losses range from a teacher (using off-color language and photos showing drinking) to a chief financial officer of a major corporation (discussing corporate dealings and financial data). The cases include college graduates being refused a job because of Facebook posts. How would you feel if information you posted about yourself on the web kept you from getting a job?

Major Laws on Privacy

Some federal laws governing privacy matters have been created. For example, the **Gramm-Leach-Bliley Act** protects personal financial information, the **Health Insurance Portability and Accountability Act (HIPAA)** protects medical records, and the **Family Educational Rights and Privacy Act (FERPA)** restricts disclosure of educational records. To learn more about existing privacy laws, visit our website at www.computing2014.com and enter the keyword law.

Most of the information collected by private organizations is not covered by existing laws. However, as more and more individuals become concerned about controlling who has the right to personal information and how that information is used, companies and lawmakers will respond.

concept check

- What is employee-monitoring software? Describe the illusion of anonymity.
- What is a history file? What are temporary Internet files? Compare first- and third-party cookies. What is privacy mode?
- Define spyware, web bugs, keystroke loggers, antispyware programs, and online identity.
- Describe three federal laws to protect privacy.

Security

We are all concerned with having a safe and secure environment to live in. We are careful to lock our car doors and our homes. We are careful about where we walk at night and whom we talk to. This is personal security. What about computer security? What if someone gains unauthorized access to our computer or other computers that contain information about us? These people are commonly known as computer **hackers**. It should be noted that not all hackers are intent on malicious actions and that not all are criminals. **Security** involves protecting individuals and organizations from theft and danger. Computer security specifically focuses on protecting information, hardware, and software from unauthorized use, as well as preventing or limiting the damage from intrusions, sabotage, and natural disasters.

environment

Did you know that the U.S. Department of Defense considers certain environmental issues to be potential threats to national security? There are currently two environmental research programs that are being funded by this department. The Strategic Environmental Research and Development Program (SERDP) focuses on research on innovative technology that can help to reduce environmental risks while enhancing and sustaining military readiness. The Environmental Security Technology Certification Program (ESTCP) is responsible for demonstrating and validating the most promising technologies. To see more environmental facts, visit our website at www.computing2014.com and enter the keyword environment.

Cybercrime

Cybercrime or **computer crime** is any criminal offense that involves a computer and a network. It was recently estimated that cybercrime affects over 400 million people and costs over $400 billion each year. Cybercrimes can take various forms including the creation of malicious programs, denial of service attacks, Internet scams, theft, and data manipulation.

Malicious Programs A **cracker** is someone who creates and distributes malicious programs. These programs are called **malware**, which is short for **mal**icious soft**ware**. They are specifically designed to damage or disrupt a computer system. The three most common types of malware are viruses, worms, and Trojan horses.

- **Viruses** are programs that migrate through networks and operating systems, and most attach themselves to different programs and databases. While some viruses are relatively harmless, many can be quite destructive. Once activated, these destructive viruses can alter and/or delete files. Creating and knowingly spreading a virus is a very serious crime and a federal offense punishable under the **Computer Fraud and Abuse Act**.

  Unfortunately, new computer viruses are appearing all the time. The best way to stay current is through services that keep track of viruses on a daily basis. For example, Symantec tracks the most serious virus threats. See Figure 9-11.
- **Worms** are programs that simply replicate themselves over and over again. Once active in a network, the self-replicating activity clogs computers and networks until their operations are slowed or stopped. A recent worm traveled across the world within hours, stopping tens of thousands of computers along its way. Unlike a virus, a worm typically does not attach itself to a program or alter and/or delete files. Worms, however, can carry a virus. Once a virus has been deposited by a worm onto an unsuspecting computer system, the virus

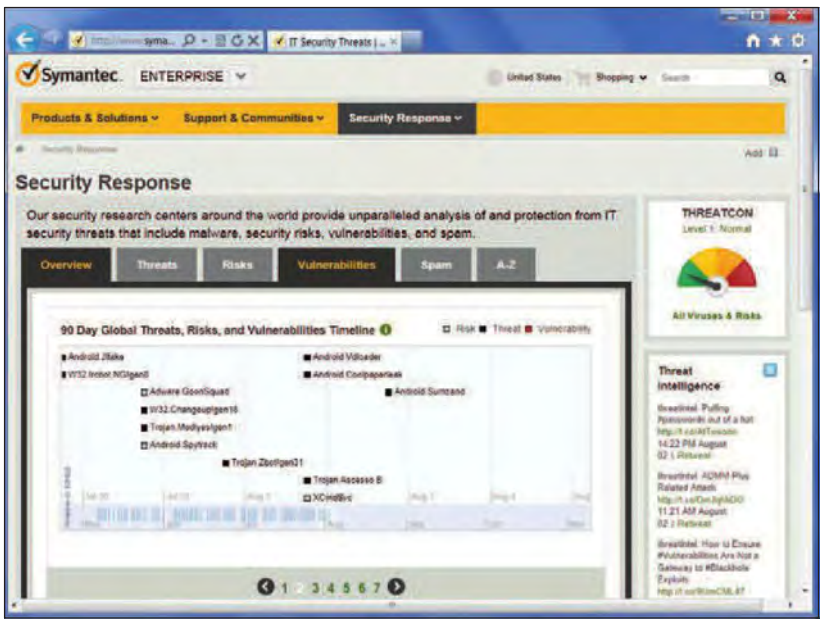


Figure 9-11 Tracking viruses

will either activate immediately or lie dormant until some future time. For example in 2010, the Stuxnet worm infected several networks in Iran. One of these networks was used by Iran's nuclear program. Soon after the infection, several key pieces of nuclear equipment became permanently disabled.

Viruses and worms typically find their way into microcomputers through e-mail attachments and programs downloaded from the Internet. Because viruses can be so damaging, computer users are advised to never open an e-mail attachment from an unknown source and to exercise great care in accepting new programs and data from any source.

As we discussed in Chapter 4, antivirus programs alert users when certain kinds of viruses and worms enter their system. Two of the most widely used are McAfee VirusScan and Norton AntiVirus. Unfortunately, new viruses are being developed all the time, and not all viruses can be detected.

- **Trojan horses** are programs that come into a computer system disguised as something else. Trojan horses are not viruses. Like worms, however, they can be carriers of viruses. The most common types of Trojan horses appear as free computer games and free screen saver programs that can be downloaded from the Internet. When a user downloads one of these programs, a virus is deposited on the computer system. The virus then begins its mischief. One of the most dangerous types of Trojan horse claims to provide free antivirus programs. When a user downloads one of these programs, the Trojan horse starts with a virus that locates and disables any existing virus protection programs before depositing other viruses.

Zombies are computers infected by a virus, worm, or Trojan horse that allows them to be remotely controlled for malicious purposes. A collection of zombie computers is known as a **botnet**, or **robot network**. Botnets harness the combined power of many zombies for malicious activities like password cracking or sending junk e-mail. Because they are formed by many computers distributed across the Internet, botnets are hard to shut down even after they are detected. Unfortunately for individual computer owners, it also can be difficult to detect when a personal computer has been compromised.

Type	Description
Identity theft	Individuals pose as ISPs, bank representatives, or government agencies requesting personal information. Once obtained, criminals assume a person's identity for a variety of financial transactions.
Chain letter	Classic chain letter instructing recipient to send a nominal amount of money to each of five people on a list. The recipient removes the first name on the list, adds his or her name at the bottom, and mails the chain letter to five friends. This is also known as a pyramid scheme. Almost all chain letters are fraudulent and illegal.
Auction fraud	Merchandise is selected and payment is sent. Merchandise is never delivered.
Vacation prize	"Free" vacation has been awarded. Upon arrival at vacation destination, the accommodations are dreadful but can be upgraded for a fee.
Advance fee loans	Guaranteed low-rate loans available to almost anyone. After applicant provides personal loan-related information, the loan is granted subject to payment of an "insurance fee."

Figure 9-12 Common Internet scams

Denial of Service A **denial of service (DoS) attack** attempts to slow down or stop a computer system or network by flooding a computer or network with requests for information and data. The targets of these attacks are usually Internet service providers (ISPs) and specific websites. Once under attack, the servers at the ISP or the website become overwhelmed with these requests for service and are unable to respond to legitimate users. As a result, the ISP or website is effectively shut down.

Internet Scams A **scam** is a fraudulent or deceptive act or operation designed to trick individuals into providing personal information or spending their time and money for little or no return. An **Internet scam** is simply a scam using the Internet. Internet scams are becoming a serious problem and have created financial and legal problems for many thousands of people. Almost all the scams are initiated by a mass mailing to unsuspecting individuals.

A technique often employed by scammers is **phishing** (pronounced "fishing"). Phishing attempts to trick Internet users into thinking a fake but official-looking website or e-mail is legitimate. Phishing has grown in sophistication, replicating entire websites like PayPal to try to lure users into divulging their financial information.

See Figure 9-12 for a list of common types of Internet scams.

Social Networking Risks As we have discussed in Chapter 2, social networking is designed for open sharing of information among individuals that share a common interest. Unfortunately, this openness can put individuals using social networking sites at risk. Some have lost their jobs after posting unflattering remarks about their supervisor or after discussing their dislike of their current job. Others post detailed personal information such as their birth dates, family member names, home addresses, and photos of their children. This information can be used by others to steal personal identities and commit other types of crimes. Always exercise caution when providing information on Facebook, Twitter, and other social networking sites. Always use the privacy settings and controls that are provided at the social networking sites you use. (See Figure 9-13.)

Cyberbullying A fairly recent and all-too-common phenomenon, **cyberbullying** is the use of the Internet, cell phones, or other devices to send or post content intended

ethics

Sharing personal information in a social network like Facebook is a voluntary activity. However, many individuals do not fully understand the complex sharing and privacy policies of these networks. This often causes unintentional sharing with people outside their intended social circle. The social networks themselves have come under fire from privacy groups, saying that these companies act unethically by using complex settings and policies to get users to share more information than intended. This information is in turn shared with advertisers. Do you think social networks act unethically when it comes to personal information? To see more ethical issues, visit our website at www.computing2014.com and enter the keyword ethics.

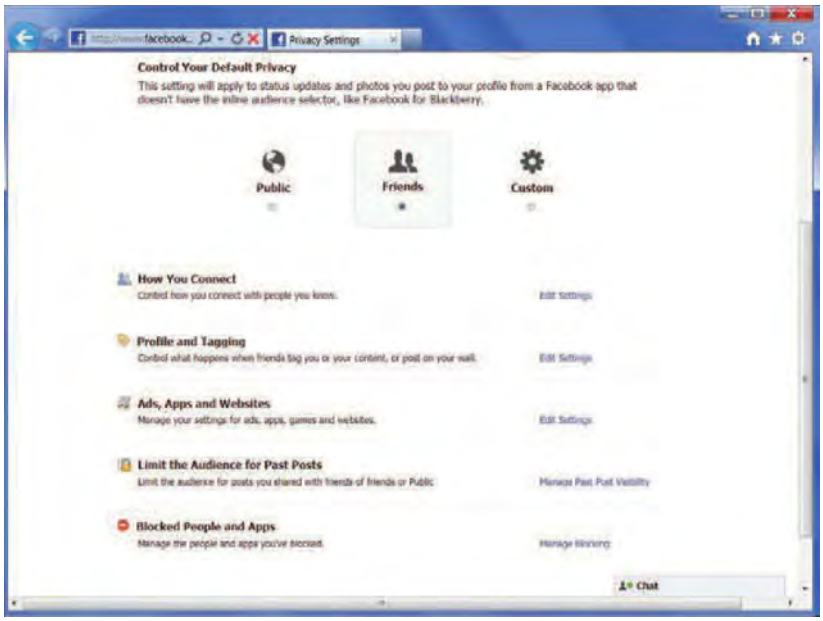


Figure 9-13 Facebook privacy controls

to hurt or embarrass another person. Although not always a crime, it can lead to criminal prosecution. Cyberbullying includes sending repeated unwanted e-mails to an individual who has stated that he or she wants no further contact with the sender, ganging up on victims in electronic forums, posting false statements designed to injure the reputation of another, maliciously disclosing personal data about a person that could lead to harm to that person, and sending any type of communication that is threatening or harassing. Never participate in cyberbullying, and discourage others from participating in this dangerous and hateful activity.

Rogue Wi-Fi Hotspots Free Wi-Fi networks are available almost everywhere from libraries to fast-food restaurants and coffee shops. **Rogue Wi-Fi hotspots** imitate these free networks. These rogue networks operate close to the legitimate free hotspots and typically provide stronger signals that many users unsuspectingly connect to. Once connected, the rogue networks capture any and all information sent by the users to legitimate sites including user names and passwords.

Theft Theft can take many forms—of hardware, of software, of data, of computer time. Thieves steal equipment and programs, of course, but there are also white-collar crimes. These crimes include the theft of data in the form of confidential information such as preferred-client lists. Another common crime is the use (theft) of a company's computer time by an employee to run another business.

Data Manipulation Finding entry into someone's computer network and leaving a prankster's message may seem like fun, which is why hackers do it. It is still against the law. Moreover, even if the manipulation seems harmless, it may cause a great deal of anxiety and wasted time among network users.

The **Computer Fraud and Abuse Act** makes it a crime for unauthorized persons even to view—let alone copy or damage—data using any computer across state lines. It also prohibits unauthorized use of any government computer or a computer used by any federally insured financial institution. Offenders can be sentenced to up to 20 years in prison and fined up to $100,000.

Computer Crime	Description
Malicious programs	Include viruses, worms, and Trojan horses
DoS	Causes computer systems to slow down or stop
Internet scams	Are scams over the Internet usually initiated by e-mail and involving phishing
Social networking risks	Includes posting work-related criticisms and disclosure of personal information
Cyberbullying	Is using the Internet, cell phones, or other devices to send/post content intended to hurt or embarrass another person
Rogue Wi-Fi hotspots	Imitate legitimate Wi-Fi hotspot in order to capture personal information
Theft	Includes hardware, software, and computer time
Data manipulation	Involves changing data or leaving prank messages

Figure 9-14 Computer crimes

For a summary of computer crimes, see Figure 9-14. For a brief history of computer crimes, visit our website at www.computing2014.com and enter the keyword crime.

concept check

- What is cybercrime? What are malicious programs?
- Compare viruses, worms, and Trojan horses. What are zombies?
- What are denial of service attacks? Internet scams? Social networking risks?
- What is cyberbullying? A rogue Wi-Fi hotspot? Data theft and manipulation?

Measures to Protect Computer Security

There are numerous ways in which computer systems and data can be compromised and many ways to ensure computer security. Some of the principal measures to ensure computer security are restricting access, encrypting messages, anticipating disasters, and preventing data loss.

Restricting Access Security experts are constantly devising ways to protect computer systems from access by unauthorized persons. Sometimes security is a matter of putting guards on company computer rooms and checking the identification of everyone admitted. Other times it is using **biometric scanning** devices such as fingerprint and iris (eye) scanners. (See Figure 9-15.) There are numerous applications that use face recognition to allow access to a computer system.

tips

With so many security threats out there, as well as tools to counter those threats, you can easily feel helpless and overwhelmed. Here is an easy-to-follow list of best practices that can help protect the security of your computer and valuable data:

1. **Security tools.** An Internet security suite (which includes an antivirus program), together with the firewall that is included with most operating systems, will keep most threats from harming your computer.
2. **Software updates.** Always ensure that your operating system, security suites, and other crucial programs are set to receive updates as soon as the companies make them available.
3. **E-mail and attachments.** Avoid opening any e-mail that seems suspicious or is from a person or organization you do not know. Be even more careful with links and attachments. Also remember that the e-mail accounts belonging to your friends and family members could be compromised, so be careful with attachments and links from them that seem suspicious.
4. **Passwords.** Use a strong password for your operating system log-in, and a different strong password for each website log-in. Do not share passwords with anyone and do not leave them in obvious places, such as on a notebook next to your computer or in an unencrypted Word document.
5. **Wireless encryption.** Use WPA2 encryption for your home's wireless router.

To see other tips, visit our website at www.computing2014.com and enter the keyword tips.

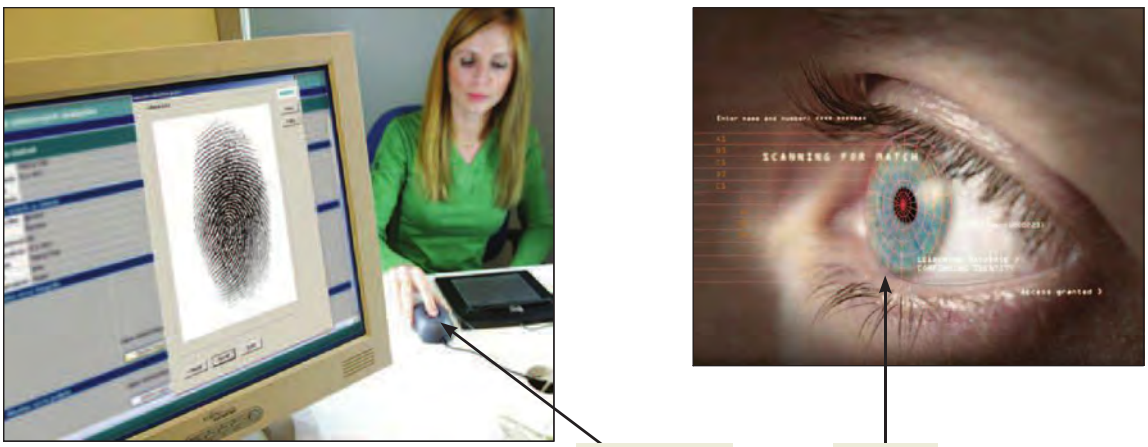


Figure 9-15 Biometric scanning devices

For example, many microcomputer systems use Dell's FastAccess face recognition application to prevent unauthorized access. There are also several face recognition apps for mobile devices including Face Recognition by iNFINITE Studios LLC.

Oftentimes it is a matter of being careful about assigning passwords to people and of changing the passwords when people leave a company. **Passwords** are secret words or phrases (including numbers, letters, and special characters) that must be keyed into a computer system to gain access. For many applications on the web, users assign their own passwords. Windows 8 includes an application, Picture Password, that accepts a series of gestures over a picture of the users choice to gain access.

The strength of a password depends on how easily it can be guessed. A **dictionary attack** uses software to try thousands of common words sequentially in an attempt to gain unauthorized access to a user's account. For this reason, words, names, and simple numeric patterns make weak or poor passwords. Strong passwords have at least eight characters and use a combination of letters, numbers, and punctuation marks. It is also important not to reuse passwords for different accounts. If one account is compromised, that password might be tried for access to other systems as well. For example, if a low-security account such as an online web forum is compromised, that password could also be tried on higher-security accounts such as banking websites.

As mentioned in previous chapters, individuals and organizations use security suites and firewalls to protect and control access to their computers.

- **Security suites** provide a collection of utility programs designed to protect your privacy and security while you are on the web. To learn more about selecting and using security suites, see Making IT Work for You: Security Suites on pages 257 and 258.
- **Firewalls** act as a security buffer between a corporation's private network and all external networks, including the Internet. All electronic communications coming into and leaving the corporation must be evaluated by the firewall. Security is maintained by denying access to unauthorized communications.

Encrypting Data Whenever information is sent over a network or stored on a computer system, the possibility of unauthorized access exists. The solution is **encryption**, the process of coding information to make it unreadable except to

Explorations

How strong is your password?

To test the strength of a password and discover valuable tips, visit our website at www.computing2014.com and enter the keyword password.

Making IT work for you

SECURITY SUITES

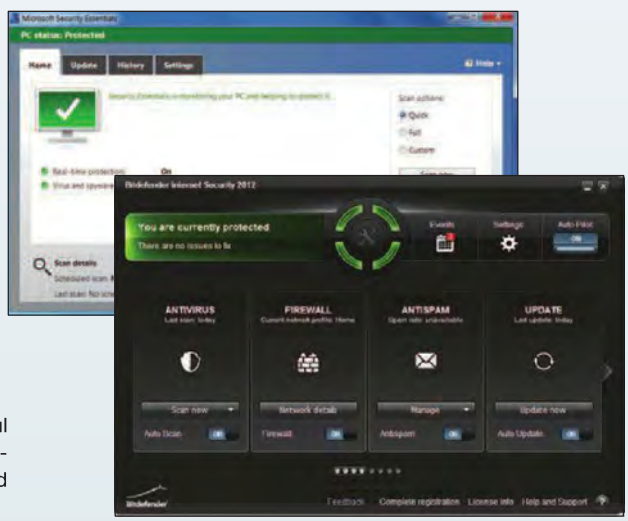
Do you currently have software that protects you and your computer from various types of threats? Are they separate programs that have to be managed individually? If so, then you may find that a security suite is a more convenient solution. These suites are software packages that include various utilities that help protect your computer from malware, hackers, and many other types of threats.

Standard Utilities Most security suites provide the following features to protect you and your computer:

- **Antivirus**
- **Antispyware**
- **Firewall**
- **Phishing detection**
- **Privacy/identity protection**
- **Parental controls**

At a minimum, all products will have antivirus and antispyware capabilities. You will be protected by a real-time scanner that is loaded into your computer's RAM each time you log into your system.

Factors to Consider With so many security suites, it may be difficult to make a choice. Experts generally consider the following factors:



- ***Detection*. How well does it detect threats? Does it miss too many?**
- ***False-positives*. How many times does it mistake a safe file for a threat?**
- ***Threat removal*. How well does it eliminate malicious files from your machine?**
- ***Performance*. Does it slow down your system significantly while it is in RAM? How fast does it complete a system scan?**
- ***Interface*. Is the software easy to use and configure?**

For specific recommendations and rankings, it is useful to read expert reviews and test results. Search for "security suites" on reliable online sources such as pcworld.com and cnet.com.

Free Resources There are several ways to obtain security tools at no cost:

- ***Free antivirus.*** **Many reputable companies, such as Avast and AVG, create free antivirus products in order to promote their more feature-rich versions (which do cost money). Although they are offered as free downloads, these tools will generally perform their detection and removal jobs quite well.**
- ***ISP provided.*** **Most Internet service providers include a security suite with your Internet subscription. Make sure this offer is a permanent and not a limited trial. Many individuals have found themselves unprotected because their antivirus subscription expired!**
- ***Microsoft Security Essentials.*** **Windows does not include an antivirus; however, Microsoft does offer this product as a free download on its website if you are running a genuine copy of Windows.**

- ***Online scans.*** **Several products, such as Trend Micro's *HouseCall* and Panda Security's *ActiveScan,* offer web-based scanning of your computer when you visit their websites. Generally speaking, this is useful only when you suspect that your computer is already infected.**

The web is continually changing, and some of the specifics presented in this Making IT Work for You may have changed.

To learn about other ways to make information technology work for you, visit our website at www.computing2014.com and enter the keyword miw.

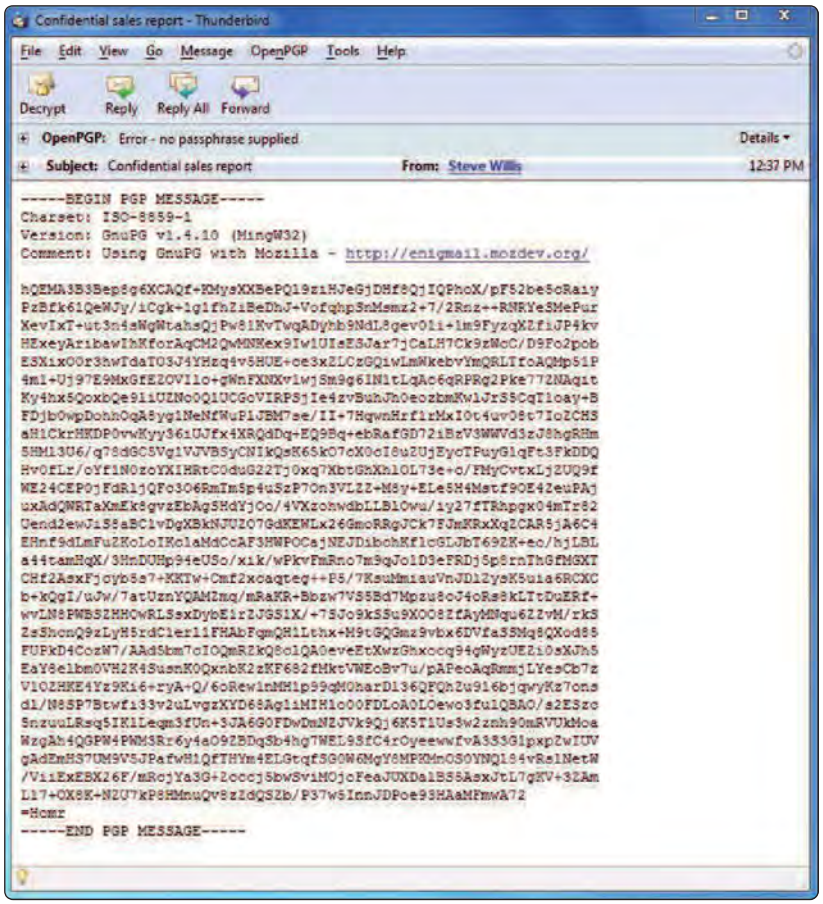


Figure 9-16 **Encrypted e-mail**

those who have a special piece of information known as an **encryption key**, or, simply, a **key**. Some common uses for encryption include

- **E-mail encryption:** Protects e-mail messages as they move across the Internet. One of the most widely used personal e-mail encryption programs is Pretty Good Privacy. (See Figure 9-16.)
- **File encryption:** Protects sensitive files by encrypting them before they are stored on a hard drive. Files can be encrypted individually, or specialized software can be used to encrypt all files automatically each time they are saved to a certain hard drive location. (See Figure 9-17.)
- **Website encryption:** Secures web transactions, especially financial transactions. Web pages that accept passwords or confidential information like a credit card number are often encrypted.

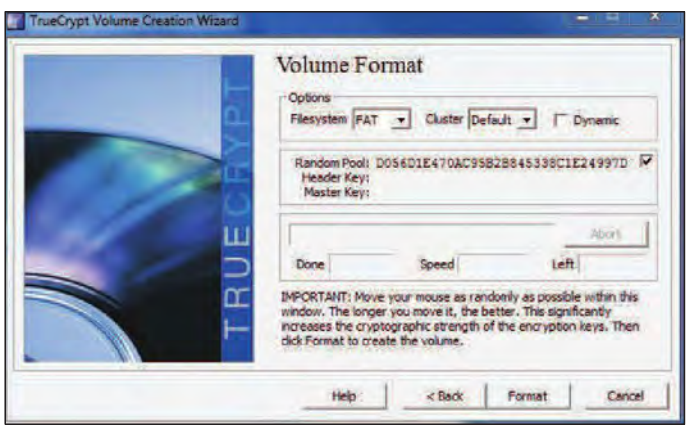


Figure 9-17 **File encryption**

The most common protocol for website encryption is **https (hypertext transfer protocol secure)**. As we discussed in Chapter 2, **http (hypertext transfer protocol)** is the most widely used Internet protocol. The https adds a security level to http. Every URL that begins with *https* requires that the browser and the connecting site encrypt all messages, providing a safer and more secure transmission.

- **Virtual private networks: Virtual private networks (VPNs)** encrypt connections between company networks and remote users such as workers connecting from home. This connection creates a secure virtual connection to a company LAN across the Internet.
- **Wireless network encryption:** Restricts access to authorized users on wireless networks. **WPA2 (Wi-Fi Protected Access)** is the most widely used wireless network encryption for home wireless networks. WPA2 is typically established for a wireless network through the network's wireless router. While the specifics vary between routers, WPA2 is usually set through the router's settings options.

Anticipating Disasters Companies (and even individuals) should prepare themselves for disasters. **Physical security** is concerned with protecting hardware from possible human and natural disasters. **Data security** is concerned with protecting software and data from unauthorized tampering or damage. Most large organizations have a **disaster recovery plan** describing ways to continue operating until normal computer operations can be restored.

Preventing Data Loss Equipment can always be replaced. A company's *data,* however, may be irreplaceable. Most companies have ways of trying to keep software and data from being tampered with in the first place. They include careful screening of job applicants, guarding of passwords, and auditing of data and programs from time to time. Some systems use redundant storage to prevent loss of data even when a hard drive fails. We discussed RAID in Chapter 7, which is a commonly used type of redundant storage. Backup batteries protect against data loss due to file corruption during unexpected power outages.

Making frequent backups of data is essential to prevent data loss. Backups are often stored at an off-site location to protect data in case of theft, fires, floods, or other disasters. Students and others often use flash drives and cloud storage as discussed in Chapter 7 to back up homework and important papers. Incremental backups store multiple versions of data at different points in time to prevent data loss due to unwanted changes or accidental deletion. To see how you could use a cloud-based backup service, see Making IT Work for You: Cloud-Based Backup on pages 261 and 262.

See Figure 9-18 for a summary of the different measures to protect computer security.

Measure	Description
Restricting access	Limit access to authorized persons using such measures as passwords and firewalls.
Encrypting data	Code all messages sent over a network.
Anticipating disasters	Prepare for disasters by ensuring physical security and data security through a disaster recovery plan.
Preventing data loss	Routinely copy data and store it at a remote location.

Figure 9-18 Measures to protect computer security

Making IT work for you

CLOUD-BASED BACKUP

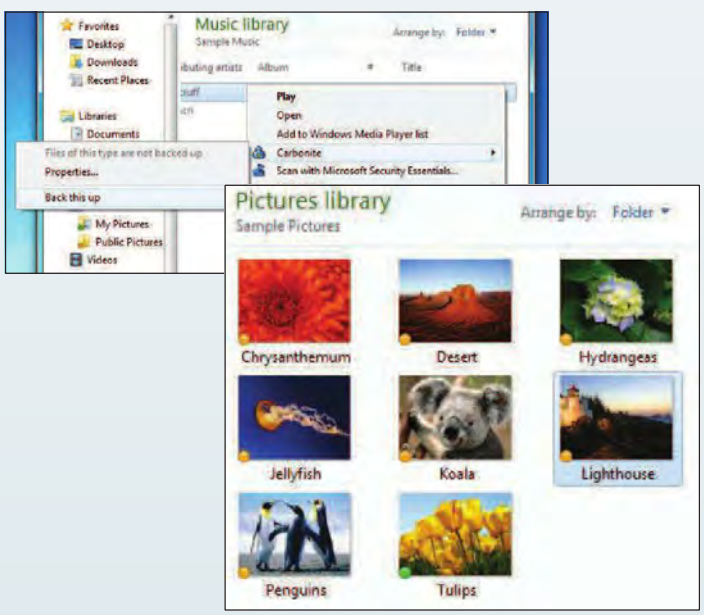
Do you remember to make frequent backups of your irreplaceable data files, such as photos and documents? Would you like a service that remembers to do the backups for you and places them in a very reliable location? If so, then a cloud-based backup service, such as Carbonite, is the solution for you.

Getting Started Carbonite offers a free trial to its backup service. Once the trial ends, you will have to pay an annual fee to continue using it. To get started with the trial:

1. **Visit www.carbonite.com, and click the *Try It For Free* button for home users.**
2. **Create an account, and then click the *Install Now* button to download the software.**
3. **Start the installation process, and when prompted, select the *Automatic* backup settings for easy setup.**

After installation, Carbonite InfoCenter will launch and begin scanning your system for files to back up.

Managing Files for Backup During the free trial, Carbonite will not automatically back up certain types of files (such as music and video). Regardless, you can still select these files manually and request that they be backed up.



1. **Go to a folder that contains photos, such as *Sample Pictures* in Windows. If you see an orange or a green icon at the bottom left of the files, that means they have been backed up (green) or are waiting to be backed up (orange).**
2. **Now, go to a folder where you have music files. Notice that they do not have an icon in the corner.**
3. **Right-click a music file, select *Carbonite,* and click *Back this up.* This file is now marked with an orange icon (you may have to refresh your window) and will be backed up in due time.**

Restoring your Files Both your files and folder structure are securely backed up on Carbonite's servers. Although the Carbonite InfoCenter window has a restore area, this guide will show you how to view your backups on Carbonite's website for easy downloading from wherever you are.

1. **Go to Carbonite's website, and click the *Log In* button. Enter your log-in information. You will be taken to a screen where you can see both computer and account information.**
2. **Click the *Restore* button, and you will be given a choice to restore all your files or to select individual files to be downloaded.**
3. **Click the *Remote Access* button.**
4. **Browse your backups by drives, folders, or users on your machine.**
5. **Select a particular file or folder, and then click the *Download* button.**

To maintain access to your files, you will have to sign up for a yearly subscription once the free trial ends. The affordable "Home" option is sufficient for most users. However, if you need to back up files that are stored on an external hard drive, the "HomePlus" plan may be best.

The web is continually changing, and some of the specifics presented in this Making IT Work for You may have changed.

To learn about other ways to make information technology work for you, visit our website at www.computing2014.com and enter the keyword miw.

concept check

- Discuss biometric scanning, passwords, dictionary attack, and firewalls.
- What is encryption? What is WPA2?
- Define physical security, data security, and disaster recovery plans.

Ethics

What do you suppose controls how computers can be used? You probably think first of laws. Of course, that is right, but technology is moving so fast that it is very difficult for our legal system to keep up. The essential element that controls how computers are used today is *ethics*.

Ethics, as you may know, are standards of moral conduct. **Computer ethics** are guidelines for the morally acceptable use of computers in our society. Ethical treatment is critically important to us all, and we are all entitled to ethical treatment. This includes the right to keep personal information, such as credit ratings and medical histories, from getting into unauthorized hands. These issues, largely under the control of corporations and government agencies, were covered earlier in this chapter. These issues and many more have been addressed in the Ethics boxes throughout this book. Now we'll examine two important issues in computer ethics where average users have a role to play.

Copyright and Digital Rights Management

Copyright is a legal concept that gives content creators the right to control use and distribution of their work. Materials that can be copyrighted include paintings, books, music, films, and even video games. Some users choose to make unauthorized copies of digital media, which violates copyright. For example, making an unauthorized copy of a digital music file for a friend might be a copyright violation.

Software piracy is the unauthorized copying and/or distribution of software. According to a recent study, software piracy costs the software industry over $30 billion annually. To prevent copyright violations, corporations often use **digital rights management (DRM)**. DRM encompasses various technologies that control access to electronic media and files. Typically, DRM is used to (1) control the number of devices that can access a given file and (2) limit the kinds of devices that can access a file. Although some companies see DRM as a necessity to protect their rights, some users feel they should have the right to use the media they buy—including movies, music, software, and video games—as they choose.

The **Digital Millennium Copyright Act** makes it illegal to deactivate or otherwise disable any antipiracy technologies including DRM technologies. The act also establishes that copies of commercial programs may not be legally resold or given away. It further makes it a crime to sell or to use programs or devices that are used to illegally copy software. This may come as a surprise to those who copy software including music and games from a friend or from the Internet. The law is clear: It is illegal to copy or download copyright-protected music and videos from the Internet without appropriate authorization.

Today, there are many legal sources for digital media. Television programs can be watched online, often for free, on television-network-sponsored sites. Sites like

environment

Do you feel that IT professionals have an ethical duty to consider the environmental impact of their actions? Many technology companies are already taking their responsibility to the environment very seriously. Some of them are "going green" and promoting their practices on their websites. Other companies are encouraging the recycling of their products to reduce the waste sent to landfills. A few are even competing to see which can develop the most energy-efficient products. To see more environmental facts, visit our website at www.computing2014.com and enter the keyword environment.

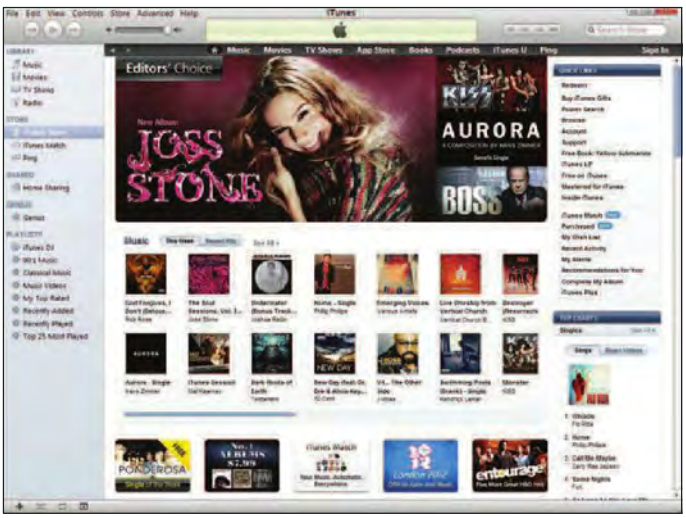


Figure 9-19 iTunes Music Store

Pandora allow listeners to enjoy music at no cost. There are several online stores for purchasing music and video content. A pioneer in this area is Apple's iTunes Music Store. (See Figure 9-19.)

Plagiarism

Another ethical issue is **plagiarism**, which means representing some other person's work and ideas as your own without giving credit to the original source. Although plagiarism was a problem long before the invention of computers, computer technology has made plagiarism easier. For example, simply cutting and pasting content from a web page into a report or paper may seem tempting to an overworked student or employee.

Correspondingly, computer technology has made it easier than ever to recognize and catch **plagiarists**. For example, services such as Turnitin are dedicated to preventing Internet plagiarism. This service will examine the content of a paper and compare it to a wide range of known public electronic documents including web page content. In this way, Turnitin can identify an undocumented paper or even parts of an undocumented paper. (See Figure 9-20.)

concept check

- What is the distinction between ethics and computer ethics?
- Define copyright, software privacy, digital rights management, and the Digital Millennium Copyright Act.
- What is plagiarism? What is Turnitin and what does it do?

ethics

Do you know of anyone who has copied parts of a web page from a variety of sites and combined the parts to form a term paper? Of course, such a practice is unethical and most likely illegal. Many schools and universities now use a program that can compare the content of a student's paper to published material on the web and previously submitted papers. Do you think it is ethical for instructors to employ a program that checks for plagiarism? Is there a risk that the program may confuse proper citations from the web with obvious cases of plagiarism? To see more ethical issues, visit our website at www.computing2014.com and enter the keyword ethics.

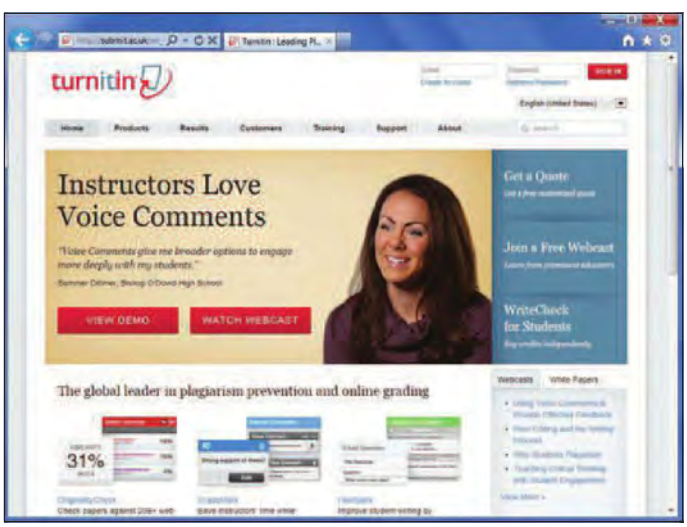


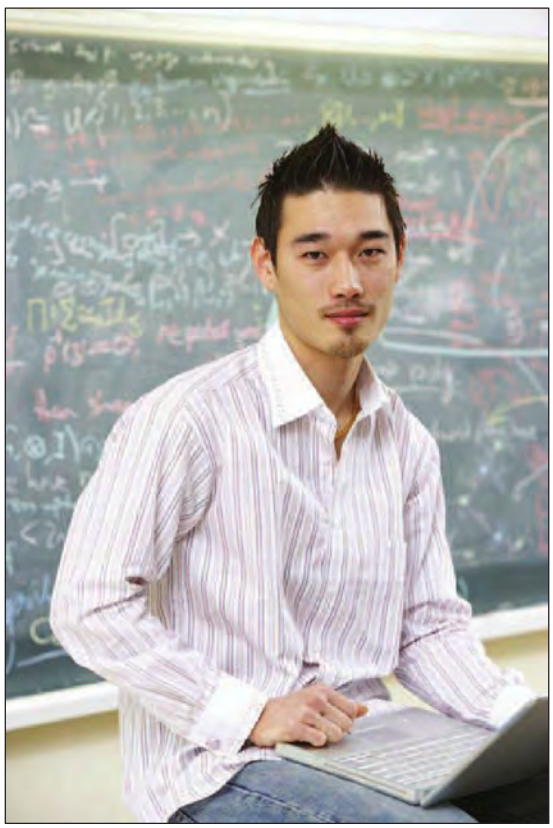
Figure 9-20 Turnitin website

Careers in IT

IT security analysts are responsible for maintaining the security of a company's network, systems, and data. Their goal is to ensure the confidentiality, integrity, and availability of information. These analysts must safeguard information systems against a variety of external threats, such as hackers and viruses, as well be vigilant of threats that may come from within the company.

Employers typically look for candidates with a bachelor's or advanced specialized associate's degree in information systems or computer science. Experience in this field or in network administration is usually required. IT security analysts should possess good communication and research skills, and be able to handle high-stress situations.

IT security analysts can expect to earn an annual salary of $62,000 to $101,000. Opportunities for advancement typically depend on experience. Demand for this position is expected to grow as malware, hackers, and other types of threats become more complex and prevalent. To learn about other careers in information technology, visit us at www.computing2014.com and enter the keyword **careers**.



Now that you have learned about privacy, security, and ethics, let me tell you about my career as an IT security analyst.

A LOOK TO THE FUTURE

The End of Anonymity

Do you enjoy the ability to interact with others on the web anonymously? Is there a sense of comfort knowing that you can express yourself freely without others knowing your identity? Anonymity has been a way of life on the Internet since the very beginning. However, various organizations, ranging from advertisers to governments, are questioning whether the Internet can continue like this. And based on the amount of information currently shared by people online, one wonders whether anonymity will be valued at all in the future.

There are many factors that are causing many to question the value of anonymity. First is the issue of harassment. Most forums and comment areas on websites allow users to post messages anonymously. Some individuals use this ability to write abusive or threatening comments. Many children and teenagers have been victims of online harassment, or cyberbullying, at some point in their lives. Others have been stalked online to the point where they have experienced psychological harm. Experts feel that if anonymous comments were disallowed, those same individuals would not be willing to write those types of messages, as their anonymity would be stripped. The other area where anonymity has become a problem is the legal field. Some anonymous web users have posted lies about individuals or businesses that have damaged the target's reputation. In the real world, those types of false and damaging comments could lead to lawsuits. For these reasons, many legislators are proposing laws aimed at discouraging the sort of anonymity that allows various online crimes to occur. In the future, it may even be a requirement to provide a real-world ID in order to use the Internet.

Many online companies are also fighting to end anonymity. This is because they make most of their money off targeted advertising. For these companies to deliver the proper advertisement to you, they need to know quite a bit about you and your online activities. By having a profile with your real name and interests, they can follow your activity throughout the web to get to know you better. At present, many advertisements you see online are for a product or service that does not interest you. In the future, every advertisement you see will interest you, as marketing companies develop a complete profile that lets them know everything about you. Now, many online businesses do aim to protect your privacy, but this is only with respect to what the public knows about you. When it comes to their advertising partners, they don't hide much because it is not in their interest to do so. Essentially, it is a trade-off for users, whether to give up some (or all) of your anonymity in return for targeted advertising.

Although many organizations are working toward ending or severely limiting anonymity, some would like to keep the Internet the way it is. Many civil rights groups and journalists support anonymity as a basic right. If you cannot be anonymous, then it would be difficult, for example, to post information that uncovers abuses in government or in a business. Some psychologists also support anonymity, stating that creating a separate online identity can be useful for personal development, allowing an individual to explore interests without leaving a record that is tied to his or her own life.

How do you feel about the possible end to anonymity? Do you agree that there will be less negativity on the web if everyone had to provide real names? Since advertisements pay for free services, will you at least tolerate future ads more if they contain something that interests you?

VISUAL SUMMARY

Privacy, Security, and Ethics

PRIVACY

Privacy concerns the collection and use of data about individuals. There are three primary privacy issues: **accuracy** (who is responsible to ensure data is correct), **property** (who owns data and rights to software), **access** (who controls access to data).

Large Databases

Large organizations are constantly compiling information about us. **Reverse directories** list telephone numbers followed by subscriber names. **Information resellers (information brokers)** collect and sell personal data. **Electronic profiles** are compiled from databases to provide highly detailed and personalized descriptions of individuals.

Identity theft is the illegal assumption of someone's identity for the purposes of economic gain. **Mistaken identity** occurs when an electronic profile of one person is switched with another. **The Freedom of Information Act** entitles individuals access to governmental records relating to them.

Private Networks

Many organizations monitor employee e-mail and computer files using special software called **employee-monitoring software**.

The Internet and the Web

Many people believe that, while using the web, little can be done to invade their privacy. This is called the **illusion of anonymity**.

PRIVACY

Information stored by browsers includes **history files** (record sites visited) and **temporary Internet files** or **browser cache** (contain website content and display instructions). **Cookies** store and track information. **Privacy mode (InPrivate Browsing; Private Browsing)** ensures that your browsing activity is not recorded.

Spyware secretly records and reports Internet activities. **Computer monitoring software** (or **keystroke loggers**) are particularly dangerous. **Antispyware (spy removal programs)** detects and removes various privacy threats.

Online Identity

Many people post personal information and sometimes intimate details of their lives without considering the consequences. This creates an **online identity**. With the archiving and search features of the web, this identity is indefinitely available to anyone who cares to look for it.

Major Laws on Privacy

The **Gramm-Leach-Bliley Act** protects personal financial information; the **Health Insurance Portability and Accountability Act (HIPAA)** protects medical records; and the **Family Educational Rights and Privacy Act (FERPA)** restricts disclosure of educational records.

To be a competent end user, you need to be aware of the potential impact of technology on people. You need to be sensitive to and knowledgeable about personal privacy, organizational security, and ethics.

SECURITY

Computer **security** focuses on protecting information, hardware, and software from unauthorized use as well as preventing damage from intrusions, sabotage, and natural disasters. Someone who gains unauthorized access to computers that contain information about us is commonly known as a computer **hacker**. Not all hackers are intent on malicious actions and not all are criminals.

Cybercrime

Cybercrime (computer crime) is an illegal action involving special knowledge of computer technology.

- Malicious programs **(malware)** include **viruses** (the **Computer Fraud and Abuse Act** makes spreading a virus a federal offense), **worms**, and **Trojan horses. Zombies** are remotely controlled infected computers used for malicious purposes. A collection of zombie computers is known as a **botnet**, or **robot network**.
- **Denial of service (DoS) attack** is an attempt to shut down or stop a computer system or network. It floods a computer or network with requests for information and data.
- **Scams** are designed to trick individuals into spending their time and money with little or no return. Common **Internet scams** include identity theft, chain letters, auction fraud, vacation prizes, and advance fee loans. These are frequently coupled with **phishing** websites or e-mails.

SECURITY

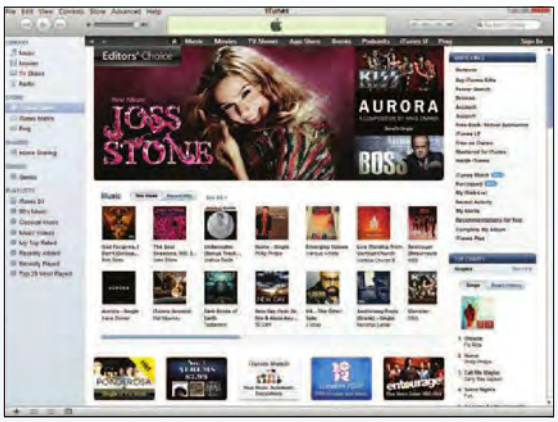
- Social networking risks include posting work-related criticisms and disclosure of personal information.
- **Cyberbullying** is the use of the Internet, cell phones, or other devices to send or post content intended to hurt or embarrass another person.
- **Rogue Wi-Fi hotspots** imitate legitimate hotspots to capture personal information.
- Theft takes many forms including stealing hardware, software, data, and computer time.
- Data manipulation involves changing data or leaving prank messages. **The Computer Fraud and Abuse Act** helps protect against data manipulation.

Measures to Protect Computer Security

There are numerous ways in which computer systems and data can be compromised and many ways to protect computer security. These measures include

- Access can be restricted through **biometric scanning** devices and **passwords** (secret words or phrases; **dictionary attacks** use thousands of words to attempt to gain access).
- **Encrypting** is coding information to make it unreadable except to those who have the **encryption key. Virtual private networks (VPNs)** encrypt connections between company networks and remote users. **WPA2 (Wi-Fi Protected Access)** is the most widely used wireless network encryption for home wireless networks.
- Anticipating disasters involves physical security, data security, and disaster recovery plans.
- Preventing data loss involves protecting data by screening job applicants, guarding passwords, and auditing and backing up data.

ETHICS



What do you suppose controls how computers can be used? You probably think first of laws. Of course, that is right, but technology is moving so fast that it is very difficult for our legal system to keep up. The essential element that controls how computers are used today is *ethics*.

Ethics are standards of moral conduct. **Computer ethics** are guidelines for the morally acceptable use of computers in our society. We are all entitled to ethical treatment. This includes the right to keep personal information, such as credit ratings and medical histories, from getting into unauthorized hands.

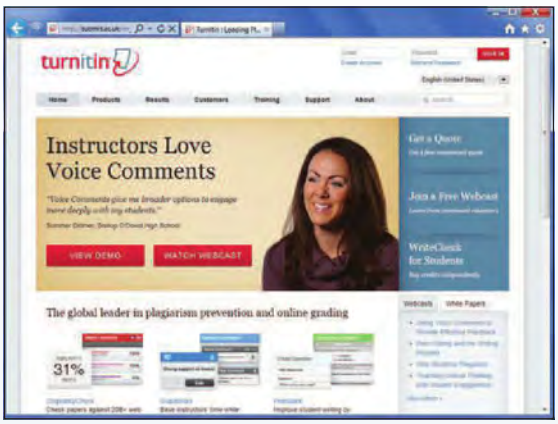
Copyright and Digital Rights Management

Copyright is a legal concept that gives content creators the right to control use and distribution of their work. Materials that can be copyrighted include paintings, books, music, films, and even video games.

Software piracy is the unauthorized copying and distribution of software. The software industry loses over $30 billion annually to software piracy. Two related topics are the Digital Millennium Copyright Act and digital rights management.

- **Digital Millennium Copyright Act** establishes the right of a program owner to make a backup copy of any program and disallows the creation of copies to be sold or given away. It is also illegal to download copyright-protected music and videos from the Internet.
- **Digital rights management (DRM)** is a collection of technologies designed to prevent copyright violations. Typically, DRM is used to (1) control the number of devices that can access a given file and (2) limit the kinds of devices that can access a file.

ETHICS



Today, many legal sources for digital media exist, including

- Television programs that can be watched online, often for free, on television-network-sponsored sites.
- Sites like Pandora that allow listeners to enjoy music at no cost.
- Online stores that legally sell music and video content. A pioneer in this area is Apple's iTunes Music Store.

Plagiarism

Plagiarism is the illegal and unethical representation of some other person's work and ideas as your own without giving credit to the original source. Examples of plagiarism include cutting and pasting web content into a report or paper.

Recognizing and catching **plagiarists** is relatively easy. For example, services such as **Turnitin** are dedicated to preventing Internet plagiarism. This service examines a paper's content and compares it to a wide range of known public electronic documents including web page content. Exact duplication or paraphrasing is readily identified.

CAREERS IN IT

IT security analysts are responsible for maintaining the security of a company's network, systems, and data. Employers look for candidates with a bachelor's or advanced specialized associate's degree in information systems or computer science and network experience. Salary range is $62,000 to $101,000.

KEY TERMS

access (243)
accuracy (243)
antispyware (249)
biometric scanning (255)
botnet (252)
browser cache (247)
computer crime (251)
computer ethics (263)
Computer Fraud and Abuse Act (251, 254)
computer monitoring software (249)
cookies (247)
copyright (263)
cracker (251)
cyberbullying (253)
cybercrime (251)
data security (260)
denial of service (DoS) attack (253)
dictionary attack (256)
Digital Millennium Copyright Act (263)
digital rights management (DRM) (263)
disaster recovery plan (260)
electronic profile (244)
employee-monitoring software (246)
encryption (256)
encryption key (259)
ethics (263)
Family Educational Rights and Privacy Act (FERPA) (250)
firewall (256)
first-party cookie (247)
Freedom of Information Act (246)
Gramm-Leach-Bliley Act (250)
hacker (251)
Health Insurance Portability and Accountability Act (HIPAA) (250)
history file (247)
http (hypertext transfer protocol) (260)
https (hypertext transfer protocol secure) (260)
identity theft (245)
illusion of anonymity (247)
information broker (244)
information reseller (244)
InPrivate Browsing (248)
Internet scam (253)
IT security analyst (265)
key (259)
keystroke loggers (249)
malware (251)
mistaken identity (246)
online identity (250)
password (256)
phishing (253)
physical security (260)
plagiarism (264)
plagiarist (264)
privacy (243)
privacy mode (248)
Private Browsing (248)
property (243)
reverse directory (243)
robot network (252)
rogue Wi-Fi hotspot (254)
scam (253)
security (251)
security suites (256)
software piracy (263)
spy removal program (249)
spyware (249)
temporary Internet file (247)
third-party cookie (248)
tracking cookies (248)
Trojan horse (252)
virtual private network (VPN) (260)
virus (251)
web bugs (249)
wireless network encryption (260)
worm (251)
WPA2 (Wi-Fi Protected Access 2) (260)
zombie (252)

To test your knowledge of these key terms with animated flash cards, visit us at www.computing2014.com and enter the keyword terms9. Or use the free *Computing Essentials 2014* app.

MULTIPLE CHOICE

Circle the letter of the correct answer.

1. The three primary privacy issues are accuracy, property, and:
   a. access
   b. ethics
   c. ownership
   d. security

2. To get the name, address, and other details about a person using only his or her telephone number, you could use a:
   a. third-party cookie
   b. keystroke logger
   c. reverse directory
   d. worm

3. Browsers store the locations of sites visited in a:
   a. history file
   b. menu
   c. tool bar
   d. firewall

4. The browser mode that ensures your browsing activity is not recorded.
   a. detect
   b. insert
   c. privacy
   d. sleep

5. The information that people voluntarily post in social networking sites, blogs, and photo- and video-sharing sites is used to create their:
   a. access approval
   b. firewall
   c. online identity
   d. phish

6. Computer criminals who create and distribute malicious programs.
   a. antispies
   b. crackers
   c. cyber traders
   d. identity thieves

7. Programs that come into a computer system disguised as something else are called:
   a. Trojan horses
   b. viruses
   c. web bugs
   d. zombies

8. The use of the Internet, cell phones, or other devices to send or post content intended to hurt or embarrass another person is known as:
   a. cyberbullying
   b. online harassment
   c. social media discrimination
   d. unethical communication

9. Special hardware and software used to control access to a corporation's private network is known as a(n):
   a. antivirus program
   b. communication gate
   c. firewall
   d. spyware removal program

10. To prevent copyright violations, corporations often use:
    a. ACT
    b. DRM
    c. VPN
    d. WPA2

For an interactive multiple-choice practice test, visit us at www.computing2014.com and enter the keyword multiple9. Or use the free *Computing Essentials 2014* app.

MATCHING

Match each numbered item with the most closely related lettered item. Write your answers in the spaces provided.

a. accuracy
b. biometric
c. cookies
d. encryption
e. information brokers
f. malware
g. phishing
h. plagiarism
i. spyware
j. zombies

___ **1.** Privacy concern that relates to the responsibility to ensure correct data collection.
___ **2.** Individuals who collect and sell personal data.
___ **3.** Small data files deposited on your hard disk from websites you have visited.
___ **4.** Wide range of programs that secretly record and report an individual's activities on the Internet.
___ **5.** Malicious programs that damage or disrupt a computer system.
___ **6.** Infected computers that can be remotely controlled.
___ **7.** Used by scammers to trick Internet users with official-looking websites.
___ **8.** A type of scanning device such as fingerprint and iris (eye) scanner.
___ **9.** Process of coding information to make it unreadable except to those who have a key.
___ **10.** An ethical issue relating to using another person's work and ideas as your own without giving credit to the original source.

For an interactive matching practice test, visit our website at www.computing2014.com and enter the keyword matching9. Or use the free *Computing Essentials 2014* app.

OPEN-ENDED

On a separate sheet of paper, respond to each question or statement.

1. Define privacy, and discuss the impact of large databases, private networks, the Internet, and the web.
2. Define and discuss online identity and the major privacy laws.
3. Define security. Define computer crime and the impact of malicious programs, including viruses, worms, Trojan horses, and zombies, as well as cyberbullying, denial of service attacks, Internet scams, social networking risks, rogue Wi-Fi hotspots, theft, data manipulation, and other hazards.
4. Discuss ways to protect computer security including restricting access, encrypting data, anticipating disasters, and preventing data loss.
5. Define ethics, and describe copyright law and plagiarism.

DISCUSSION

Respond to each of the following questions.

1 Making IT Work for You: SECURITY SUITES

Do you currently have software that protects you and your computer from various types of threats? Review the Making IT Work for You: Security Suites on pages 257 and 258 and then respond to the following: (a) Do you have a security suite installed on your computer? If so, which one do you have and describe its functionality. If you do not, have you ever experienced any security or virus issues? (b) Does your Internet service provider offer a security suite or antivirus with your subscription? If so, which one(s) does it offer? If it does not, contact your ISP and ask its advice on how to protect your computer. What was its advice? (c) Find an article that reviews current security suites. (*PCWorld, CNET*, and *PCMag* are good places to start.) List three products that earned the highest marks, and document your source(s). (d) Based on your experience and research, do you plan on using a security suite in the future? If so, which one and why that one? If you do not plan to use a security suite, why not? (e) Do you think free security suites are as effective as those that must be purchased? Discuss.

2 Making IT Work for You: CLOUD-BASED BACKUP

Do you remember to make frequent backups of your irreplaceable data files, such as photos and documents? Review the Making IT Work for You: Cloud-Based Backup on pages 261 and 262 and then respond to the following: (a) How do you currently back up your important files? How often do you create these backups? (b) Have you ever used Carbonite or a similar cloud-based service? If so, which service have you used, and what do you typically use it for? If you have not used Carbonite or a similar service, describe how and why you might use one. (c) If you do not have a Carbonite account, set up a free one. Did you find the Carbonite software easy to set up and use? Briefly describe your opinion of the process. (d) Do you see yourself signing up for a paid, yearly subscription to a service such as Carbonite? Why or why not?

3 Explorations: PRIVACY MONITORS

Did you know that several organizations actively monitor privacy-related issues? Review the Explorations box on page 247 and then respond to the following: (a) What are the nature and goal of this organization? (b) Find and briefly explain one privacy issue related to cloud computing. Do you agree with this organization's concerns? Why or why not? (c) Find and briefly explain one privacy issue related to social networking. Do you agree with this organization's concerns? Why or why not? (d) Overall, do you believe that these organizations are valuable when it comes to privacy and the Internet? Why or why not?

4 Explorations: PASSWORDS

To learn more about creating strong passwords, review the Explorations box on page 256. Then respond to the following: (a) What are the problems with using passwords such as "internet" or "computer"? (b) Does the password strength improve if you add two digits, such as in "computer99"? Do any weaknesses remain in such a password? (c) Using some of the tips you have discovered, create a password that will not result in any warnings (do not use any of your actual, current passwords). What was this password? How long will it take to break such a password?

5 Ethics: SOCIAL NETWORKING

Social networking companies are often criticized for having misleading or confusing policies regarding the sharing of personal information. Review the Ethics box on page 253 and then answer the following: (a) Which social network(s) do you currently use? Do you feel that you fully understand how your posts and photos are shared on the network? Support your answer with a few examples. (b) Do you believe that social networks act unethically when they share information with advertisers? Why or why not? (c) Suppose that a high school teacher shares photos of her Halloween party, in which she is having alcoholic drinks with her social networking friends. Somehow, the school board obtains these photos and decides to suspend her. Is this ethical? Does this violate her right to act as she wishes on her own time? Why or why not? (d) In late 2009, Facebook's privacy settings underwent a major change in which each user's name, picture, and basic information appeared in Google search results and was visible to the entire Internet by default. Are there any ethical concerns here? Or by joining Facebook, does one waive the right to privacy? What do you think? Defend your position.

6 Ethics: PLAGIARISM

Some argue that when writing a paper using research from the Internet, it is difficult to draw a distinction between using information found on a website and plagiarizing its content. Many schools use special software to help professors make this distinction. Review the Ethics box on page 264 and then respond to the following: (a) Do you think it is ethical for instructors to employ a program that checks for plagiarism? Why or why not? (b) Do you think it is ethical for students or any individuals to copy all or part of a web page's content and then present the information as his or her original work? Why or why not? (c) How would you distinguish between using the web for research and plagiarizing web content? Be as specific as possible. (d) Does your school have a policy specifically regarding plagiarism of web content? If yes, what is the policy? If not, what would you suggest would be an appropriate policy?

7 Environment: DEPARTMENT OF DEFENSE

Did you know that the U.S. Department of Defense considers certain environmental issues to be potential threats to national security? Review the Environment box on page 251 and then respond to the following: (a) What are the two environmental research programs sponsored by the Department of Defense? (b) Why do you feel that environmental issues could be threats to national security? (c) Do you feel that the U.S. government should spend money on these types of research programs? Why or why not?

8 Environment: ENVIRONMENTAL ETHICS AND IT

Many technology companies and IT professionals are already taking their responsibility to the environment very seriously. Review the Environment box on page 263 and then respond to the following: (a) Do you feel that IT professionals should receive training or education in environmental issues? Why or why not? (b) Can a person be considered unethical if failing to consider the environment in any decisions? Discuss your response. (c) Do you feel that governments should create laws that govern the energy consumption of computers and other electronic devices? Why or why not? (d) Using a search engine, find the website of the Energy Star program. Which government agencies are responsible for this program? What environmental benefits has this program already given us?