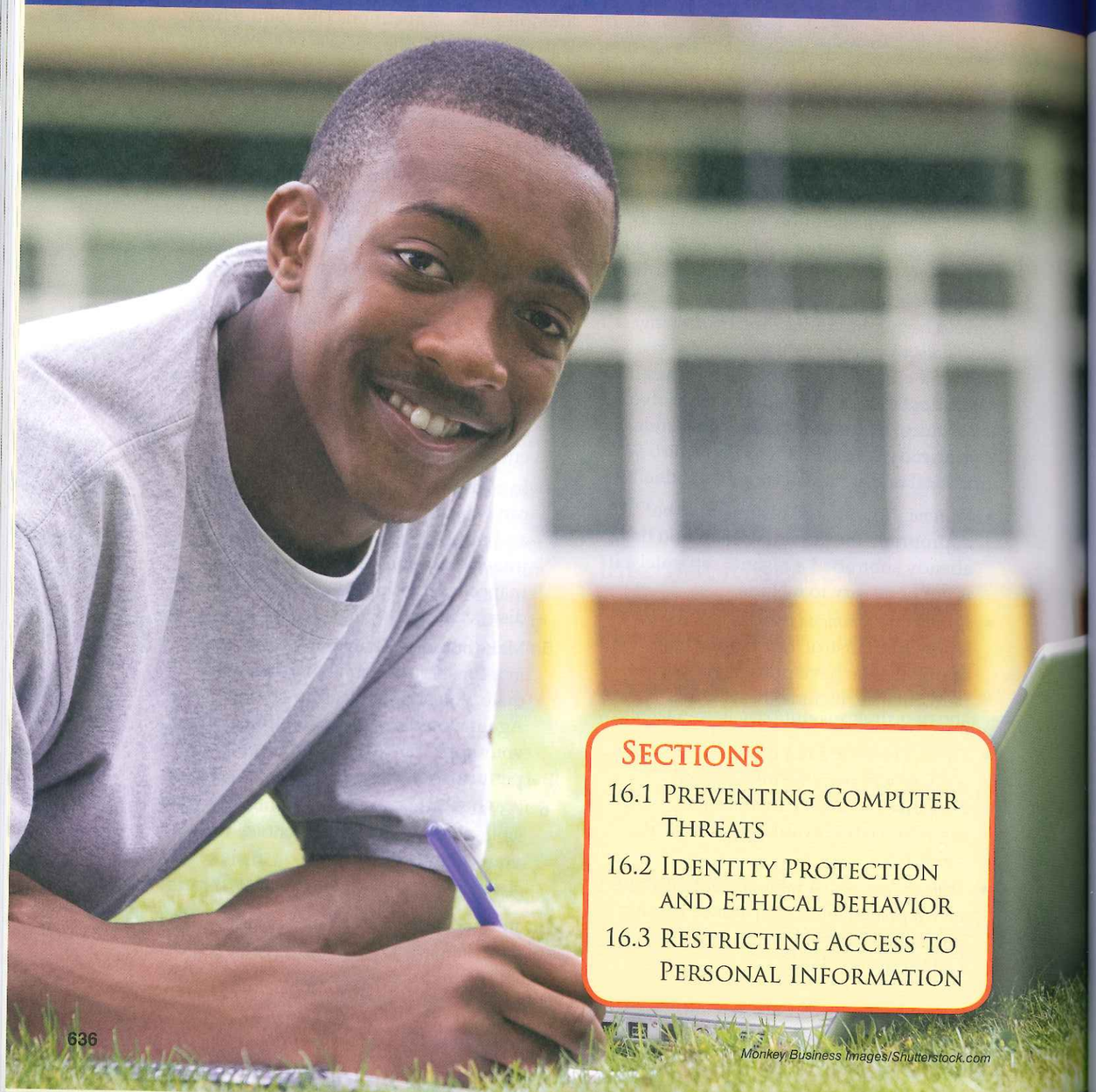
16 Security, Privacy, and Safety



Sections

Monkey Business Images/Shutterstock.com

Check Your IT IQ

Before you begin this chapter, see what you already know about information technology by scanning the QR code to take the chapter pretest. If you do not have a smartphone, visit www.g-wlearning.com.

The President of the United States has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation." Because of the threat, people who have advanced computer skills are in high demand to fill thousands of cybersecurity jobs. Recent estimates suggest that the demand for cybersecurity experts is growing at a rate twelve times that of the overall job market and more than three times the overall pace of IT jobs. Master and doctorate cybersecurity degrees are now being offered in programs known as "information assurance."

However, the job of improving computer security is ultimately the responsibility of each and every computer user, and especially those users who connect to a network or to the Internet. There will always be a struggle between those who try to crack into computer systems and files and those who need to protect those systems. Everybody should know how to use computers with confidence and relative safety. This chapter discusses how to prevent computer threats, how to protect personal data, and how to promote general safe practices for computer users.

College and Career Readiness

Reading Prep. Arrange a study session to read the chapter with a classmate. After you read each section independently, stop and tell each other what you think the main points are in the section. Continue with each section until you finish the chapter.

IC3 Certification Objectives

GS5

Computing Fundamentals

Domain 7.0 Security
- **Objective 7.1** Know credential management best practices
- **Objective 7.2** Know the basic threats to security of computers, data, and identity
- **Objective 7.3** Understand the implications of monitoring software (surveillance)
- **Objective 7.4** Understand connecting to secured vs. unsecured network (wired and wireless)
- **Objective 7.5** Know the use of and importance of antivirus software
- **Objective 7.6** Know the use of firewalls and basic settings
- **Objective 7.7** Know e-commerce interactions and best practices

Living Online

Domain 1.0 Internet (navigation)
- **Objective 1.1** Understand what the Internet is

GS4

Computing Fundamentals

Domain 3.0 Computer software and concepts
- **Objective 3.4** Software tools

Domain 4.0 Troubleshooting
- **Objective 4.1** Software

Living Online

Domain 2.0 Networking concepts
- **Objective 2.1** Internet connection

Domain 4.0 Digital citizenship
- **Objective 4.2** Legal and responsible use of computers

Domain 5.0 Safe computing
- **Objective 5.1** Secure online communication or activity

SECTION 16.1

PREVENTING COMPUTER THREATS

Essential Question

What impact do computer threats have on our economy?

Protection of digital data will continue to require a combination of technologically advanced hardware, frequently updated software programs, and safe practices and procedures. Not only do you need to have the equipment, applications, and cyber-protection programs, you need to know how to properly use these items. Ultimately, it is the individual computer user who is responsible for cybersecurity.

Users also need to ensure their cyber behavior helps, rather than hurts, their own cybersecurity. Regardless of the equipment and software, the actions of computer users are largely responsible for failures to protect computer data. When devices are recycled, care must be taken to remove all data. This section discusses how to prevent computer threats and how to protect stored data.

TERMS

adware
antivirus software
bot
cache
censorship
completely automated public Turing test to tell computers and humans apart (CAPTCHA)
computer virus
computer worm
cookies
data vandalism
hacking
malware
phishing
pop-up
ransomware
scareware
social engineering
spyware
Trojan horse

LEARNING GOALS

After completing this section, you will be able to:

- Identify types of computer threats.
- Discuss Internet security protocols.
- Explain how to protect stored data.

Computer Threats

There are many types of threats to computer systems and computer users. Malware most frequently finds its way into a computer as executable code hidden in another program. Often the computer user does not find out about the infection until long after a successful attack. Other threats come from phishing, data vandalism, cookies, and computer hacking.

GS5 Computing Fundamentals 7.2.1, 7.2.2, 7.2.3, 7.3

GS4 Computing Fundamentals 4.1.3

Malware

Malware is software that intentionally performs actions to disrupt the operation of a computer system, collect private information, or otherwise harm the computer or user. The word *malware* comes from "malicious software," meaning software that intends to harm. Malware is a broad category of harmful software. Some threats falling under malware are:

- computer viruses;
- computer worms;
- Trojan horses;
- spyware;
- adware;
- scareware; and
- ransomware.

A **computer virus** consists of computer code carried in another program that can replicate itself in order to corrupt or otherwise harm either data files or the software used to process these files. A **computer worm** is similar to a virus. However, a worm is a standalone computer program that replicates itself in order to spread to other computers. A **Trojan horse** is a program that invites the user to run it while concealing malicious code that will be executed.

Spyware is software that secretly collects a user's data and behavior. Spyware may activate a webcam, log keystrokes, collect login passwords, collect bank and credit card information, monitor Internet habits, or create tailored pop-up ads. To avoid spyware, follow the security practices outlined in Figure 16-1. Spyware is most commonly used for advertising. When used in this manner, it is usually called adware.

Adware is software that creates advertisements designed to drive the user to another website. The other site may be useful, misleading, harmful, or just distracting. Adware is famous for using cookies to track user activity.

Scareware is software designed to cause enough anxiety so the computer user leaps at the chance to opt for a poor choice. An example is a message that warns the user of a virus infection and offers a free antivirus computer scan. However, the "scan" actually installs malicious software. Ransomware is similar to scareware. However, **ransomware** encrypts files or blocks the user's access to programs until the user pays to unlock them.

FYI

A malware attack may occur when the user downloads seemingly harmless data from the Internet or transfers files from a shared flash drive.

GS4 Living Online 5.1.2

Activity	Action and Reason
Pop-up dialog boxes	Do not click links within pop-up dialog boxes. Just clicking within the dialog box or a "close" button within the window may result in spyware being installed. Instead, close the pop-up dialog box by clicking on the standard close button (X) in the upper-right corner of the title bar.
Pop-up windows on websites	These are windows created using HTML or other website-formatting language. They can be recognized because they do not look like standard dialog boxes generated by the operating system. Often, all parts of a pop-up window, including what appears to be a standard close button (X), will activate spyware. Try pressing the [Esc] key to close the window or close the browser window.
Unexpected dialog boxes	Be suspicious of unexpected dialog boxes that ask whether you want to run a particular program or perform another type of task. Close the dialog box by clicking the standard close button (X) in the title bar.
Links offering antispyware software	These links may actually install the spyware it claims to be eliminating. Only install antispyware from the developer's website, not from a third-party site.

Goodheart-Willcox Publisher

Figure 16-1. Good practices for safe use of the Internet and the World Wide Web.

Social Engineering

GS5 Computing Fundamentals 7.2.4

Distributors of malware often rely on social engineering. **Social engineering** involves manipulative techniques designed to lure unwary computer users into launching an infected file or opening a link to an infected website. Social engineering comes in many forms, such as:

- invitation to open an attached love letter or a notice of a traffic ticket;
- e-mail that imitates technical messages issued by the user's e-mail server, perhaps suggesting that storage has been exceeded and must be reduced immediately;
- message that claims to have been sent from Microsoft, perhaps saying that the attachment contains a patch that will remove Windows vulnerabilities;
- offer to reveal scandalous information on a famous person or to expand on an exciting news story;
- bank notice asking the customer to confirm account numbers or access codes; and
- attractively named files that entice the user to download them.

Attractively named files may include names such as PasswordHacker.exe, MicrosoftCDKeyGenerator.exe, JobsPayingMillions.exe, PlayStationEmulator.exe, or FreeInternetAccess.exe. Since the offer is often for something unethical or illegal, victims may not report the incident to their company or organization or to a law enforcement agency. In such cases, the cybercriminal has used a form of social engineering to deter the victim from reporting the abuse.

Cookies

GS5 Computing Fundamentals 7.4.3.2
Living Online 1.1.3.2
GS4 Living Online 5.1.2

Cookies are small text files that websites put on the computer hard disk drive when a user visits the websites. These are used to identify users. Cookies are often used to prepare customized web pages for the user. On many e-commerce sites, cookies are required to keep track of items in the shopping cart. Many password-protected websites also require cookies to keep the user logged in.

Cookies are also used to target the user with advertisements. For example, a user may search the Internet for "green fudge recipes". The search engine places a cookie on the user's computer containing this information. Then, the user goes to a website for the daily news, and ads for green fudge show up in a sidebar. The news site has used the cookie from the search engine to target the ad to the user. By selling cookies, the search engine generates revenue. While this use of cookies is not a threat to the computer system, it does represent collecting information about the user.

Cache

GS5 Computing Fundamentals 7.4.3.2
Living Online 1.1.3.3

Speed of downloading material from the Internet is improved when frequently repeated material is temporarily stored on the computer's hard drive. The location of these files is called the **cache** (pronounced *cash*). For example, a company's logo may appear on each page of the website. Instead of having to download that image file each time a new page is displayed, the browser can retrieve it from the cache. Most browsers have controls that allow users to dictate how long a cached file is retained before it is deleted or downloaded again, called refreshing, from the website.

Cookies are also cached on the hard drive. As cookies may contain personally identifiable information, routinely clear (empty) the cache, especially when using a public computer. Even when not using a public computer, it is wise to clear the cache (browser history) and clear cookies on a regular basis, especially if other people also have access to the same machine. Clearing the cache can also fix pages that freeze or do not finish loading, pages containing old content, or online applications (like games) that do not respond. Since clearing the cache deletes cookies, this can fix sign-in problems and eliminate error messages about setting user cookies.

The process for clearing a cache or cookies varies greatly depending on which browser is being used. As an example of clearing the cache, here is how to do so for Microsoft Edge:

1. Launch Microsoft Edge, and click the **More actions** button.
2. Click **Settings** in the menu.
3. In the menu that appears, under **Clear browsing data**, click the **Choose what to clear** button.
4. In the menu that appears, check the **Cookies and saved data** and **Cached data and files** check boxes. There are other categories that can be cleared as well.

5. Click the **Clear** button in the menu. Wait until the message **All clear!** appears at the top of the menu.
6. Click the **More actions** button to close the menu.

The downside of clearing the cache is that saved user names and passwords will be deleted and must then be reentered. However, the upside is that browser will work more efficiently and privacy will be improved.

GS5 Living Online 1.1.3.9

Pop-ups

In terms of web browsing, a **pop-up** is a message or window that appears on top of or under the page you are viewing. Pop-ups that appear under the page are usually called *pop-unders*. Many pop-ups are considered spam and may be designed to transmit malware. There are third-party pop-up blockers, but all modern Internet browsers contain this feature already built in. The method for controlling the pop-up blocker is different in each browser, and each browser offers different options concerning the degree of pop-up protection. Here is how pop-ups can be controlled in Microsoft Edge:

1. Launch Microsoft Edge, and click the **More actions** button.
2. Click **Settings** in the menu.
3. In the menu that appears, click the **View advanced settings** button.
4. In the menu that appears, click the **Block pop-ups** button so it is on.
5. Click the **More actions** button to close the menu.

Career Skills

Health and Safety Engineer

Health and safety engineers design systems and create procedures to keep people from injury or illness as a result of a manufacturing problem. They are also concerned with preventing property damage. Their concerns are potential damage from substances, machines, software, equipment, and other consumer products. They rely on IT for new research, report generation, and communications.

Phishing

Phishing is an attempt to get sensitive information by appearing as a harmless request. For example, a user may be told he or she has won a special prize or qualified for a no-cost introductory offer. The offer states all that is necessary is to fill out a survey. However, the survey requests sensitive information. Some information about a person that phishing scams commonly try to get includes:

- full name;
- employer's name;
- address;
- phone number;
- year of birth;
- credit card number; and
- Social Security number.

Once this information is in the hands of the phishers, it may be used to steal the person's identity or otherwise commit fraud.

Phishing also frequently comes in the form of phone fraud. This may begin with an unexpected phone call from a stranger who has a friendly voice and an appealing story. The same claims are made as in electronic phishing scams. Phone-based phishing scams often claim to be collecting for a natural disaster that is currently in the news. The sales pitch usually calls for an immediate decision. Never give out credit card details, your Social Security number, or banking information over the phone if you did

not make the call. Be cautious even if only asked for a mailing address or e-mail address. Doing so gives the scammer another way to target you.

FYI

Visit the consumer information section of the US Federal Trade Commission website (www.consumer.ftc.gov), and search for "phone scams" to find more information.

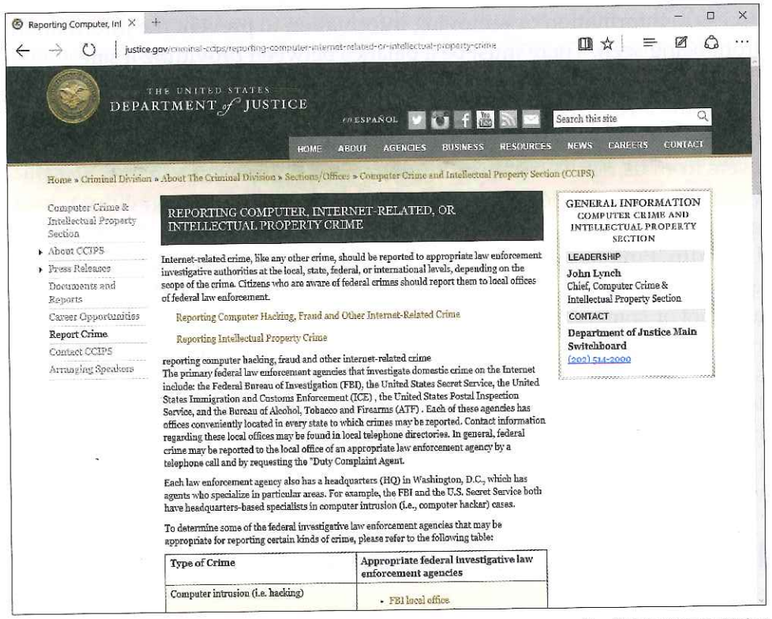
Data Vandalism

Data vandalism is the manipulation or destruction of data found in cyberspace. It is unethical and can be illegal, as shown in Figure 16-2. For example, a hacker may break into the school computer database and alter grades. Commercial competitors may engage in data vandalism, such as hacking a competing website to change the URLs for hyperlinks. Then, a customer who clicks a link for sports jackets, for example, instead may be sent to a page for sports shoes. That customer would quickly become frustrated and simply choose to shop at another online retailer. All of these examples demonstrate unethical uses of online resources.

Computer Hacking

Hacking is an activity by computer programmers to break into the e-mails, websites, computer systems, and files of other computer users. Hacking is often an unethical and illegal activity. However, there are legitimate hackers as well. Many companies hire hackers to find faults in their own computer systems. In this way, the faults can be fixed before they are exploited.

There are numerous ways hackers can discover a computer fault to exploit. For example, in many organizations, usernames and e-mail



Goodheart-Willcox Publisher

Figure 16-2. The Department of Justice maintains a website for reporting computer crimes, including hacking and data vandalism.

addresses are based on the name of the user. A hacker can try to find the person by searching social media. Once a person's name and place of work are known, the e-mail address can be guessed and verified with an online service. Then, other means can be used to crack the password to gain access to the system.

HANDS-ON EXAMPLE 16.1.1

CYBERSECURITY THREATS

The federal government and the White House have undertaken many cybersecurity policy initiatives. The White House website contains information about cybersecurity threats.

1. Launch a browser, and navigate to www.whitehouse.gov.
2. Using the website's search function, search for foreign policy cybersecurity.
3. Locate an article on foreign policy related to cybersecurity. Alternatively, directly navigate to the page www.whitehouse.gov/issues/foreign-policy/cybersecurity.
4. Read the article, and summarize the government's objectives.

GS5 Living Online 1.1.7

GS4 Living Online 4.2.1

Censorship

Many schools, companies, and organizations restrict the information that their members can access. While this is usually done to prevent computer threats by blocking certain websites and other electronic access, some people consider it censorship. **Censorship** is the act of limiting access to information or removing information to prevent the information from being seen. There must be a balance between providing a safe computing environment and allowing free access to information.

Some forms of censorship can be justified. For example, it is reasonable and legal for a school or company to prevent its computer users from using the organization's time and equipment to access certain websites. For example, online blogs, such as political chat rooms and genealogical web pages; social media sites, such as YouTube, Facebook, LinkedIn, Pinterest, and Twitter; shopping sites, such as Amazon and ebay; and sites with illegal or inappropriate images may all be blocked by a school or company. It is important for the organization to establish rules related to accessing online content to protect its reputation as well as the safety of its employees and equipment. Many organizations use software to filter content and automatically prevent access to specific sites or sites matching keywords. In addition, self-censorship is appropriate while using a computer that may be seen by others. Be aware that others may view content as offensive or politically incorrect even if you do not.

Internet Security Protocols

Internet protocols tell computers, modems, routers, and networks how to communicate with each other. Protocols also provide instructions

on how to verify and handle information being received and transmitted. Internet security protocols are especially important because they reduce or eliminate malicious uses of the Internet. There are several Internet protocols related to security.

However, no system, protocol, or technique can overcome lax behavior by computer users. For example, in 2014 a Russian website alerted the world to the fact that many people never bother to change the default password on video-surveillance cameras. To prove the point, the website streamed feeds from over 4,500 webcams around the world. Feeds for everything from baby bedroom monitors to hospital wards and business security systems were shown. This was possible simply because the users never changed the default passwords.

Green Tech

Recycle and Save

Many socially responsible companies work with the community to encourage participation in recycling efforts. Several companies have in-store recycling bins for customers to deposit used electronics and ink cartridges, compact fluorescent lightbulbs (CFLs), and plastic shopping bags. Some companies also offer incentives, such as gift cards, for recycling items in the store.

TCP/IP

The transmission control protocol (TCP) and the Internet protocol (IP) were the first networking protocols, as discussed in Chapter 13. TCP/IP provided end-to-end connectivity by specifying how data should be put into data packets, addressed, transmitted, routed, and received.

When TCP/IP was introduced during the 1980s, network or Internet security was not a serious issue. Thus, TCP/IP lacks basic mechanisms for security, such as source authentication and data encryption. Unfortunately, during the last 30 years, malicious individuals have developed techniques for misleading (spoofing) a computer concerning the real source of information. In general, this involves pretending that data are being sent from an IP address different from the actual address.

Security precautions and protocols must thus be added to TCP/IP to combat sniffing and denial of service attacks. *Sniffing* is eavesdropping that traps packets of information. A *denial of service attack* floods a service with so much traffic that the server slows down or shuts down. Most such vulnerabilities can be combated by installing the newest updates to security software and by properly configuring network applications and router settings.

SSH

A particularly important Internet security protocol is the SSH. The secure shell (SSH) is a network protocol that secures data communication and remote command execution. It is used to authenticate the client and server machines and to establish a secure channel between them. Within the SSH are three protocols: TLP, UAP, and CP.

The transport layer protocol (TLP) authenticates the server to the client and establishes a channel that the client deems secure. The user authentication protocol (UAP) authenticates the client to the server. It does this by verifying user names and passwords are matched and valid. The connection protocol (CP) distributes the secure channel into several logical channels. The CP is not really a security protocol, but is necessary.

HTTPS

Another very important Internet security protocol is the secure hypertext transfer protocol. The secure hypertext transfer protocol (HTTPS) secures communication over computer networks. It is widely used on the Internet to provide secure connections. HTTPS provides the user with authentication of a website and web server. In effect, the user's data can only be read by the website. HTTPS is actually the layering of other protocols to prevent various forms of wiretapping. Wiretapping is called *man-in-the-middle attacks.*

Other Protocols

There are also protocols for routers, fiber-optic channels, Bluetooth communication, and Yahoo Messenger:

- file transfer protocol (FTP)
- secure file transfer protocol (SFTP)
- simple mail transfer protocol (SMTP)
- hypertext transfer protocol (HTTP)
- secure socket layer protocol (SSL)
- Internet message access protocol (IMAP)
- bitcoin protocol

Over the past 25 years, experts have created many Internet protocols. Almost all of these play a role denying unauthorized access to computers and the data they contain. These protocols have greatly reduced hacking of computer systems and databases, virus transmission, and online identity theft. However, these protocols have not eliminated all threats.

FYI

The Turing test, named after pioneering computer scientist Alan Turing, measures how closely a computer can imitate the intelligence of a human.

Security Measures

Unethical Internet users may create computer programs to make massive robot-like attacks on poorly protected systems. Sometimes these attacks are done to create free e-mail accounts and send spam advertisements. Other times these attacks are for massive downloading from multimedia websites. These cyber attacks typically use web robots. A web robot, called a **bot**, is a software application that automatically performs Internet-based activities.

One common defense against bot attacks is called CAPTCHA. A **completely automated public Turing test to tell computers and humans apart (CAPTCHA)** is a brief online test to determine whether the request for access comes from a computer or a human. A common form of CAPTCHA requires the user to enter the letters and numbers shown in a distorted screen image. The image is often composed of swirled letters or blurred photos, as shown in Figure 16-3. This test is effective because humans can recognize the variety in the forms of letters and numbers, but computers cannot. This is also true for differing colors and shades. Humans can also see logical groups or segments of letters and numbers, regardless of vertical or horizontal spacing.

Goodheart-Willcox Publisher

Figure 16-3. A common CAPTCHA is a phrase composed of swirled letters. Most people can read the phrase shown here as Dog Tail, but it would be very hard for a computer program to decipher this.

Protecting Stored Data

The easiest way to protect information from corruption is by backing up those files in other locations. The cost of large-capacity external drives has plummeted in recent years. A reliable 2 TB portable hard drive costs less than $100. This is enough capacity to store all important, irreplaceable files from several laptop and desktop computers. Even a movie buff can store a collection of 150 or more Blu-ray movies on an external 4 TB drive. This size of drive costs only around $150.

Many computer users choose cloud-based options for backups. Services such as iCloud, Egnyte, and Dropbox are all file-storage solutions. They allow easy access via a web browser. Using a cloud-based service removes possible losses due to computer thefts, virus infections, fires, floods, and similar problems. Users can feel secure knowing that massive off-site computers with their own backup systems will retain the files.

FYI

The cost for 20 GB of cloud storage for an individual computer user is approximately $12 per month. The cost to back up the files of a small office with 1 TB of cloud storage is about $8 per employee per month.

Removing Data from Discarded Devices

GS4 Living Online 5.1.2

The needs of a computer user will eventually exceed the capability of his or her machine. Old electronic equipment should be recycled. In many states, it is required by law. To find recycling programs, use a search engine and use a search phrase such as "computer recycling."

Data should be cleared from any computer equipment before it is recycled. Storage devices should be "wiped" to ensure all personal files are completely erased. This will protect the data from identity thieves. Using the operating system's procedures, file access can be denied. However, the file content may still be accessible to a hacker.

A very safe approach to removing data is to repeatedly overwrite the drive. Repartition the hard drive, and then overwrite all space on the drive at least three times. Alternatively, free disk-wipe software, also called data-sanitization software, can be downloaded from the Internet. The same approach can be used with a portable flash drive.

FYI

The only sure way to remove data from a drive is to degauss it, which means to demagnetize it.

Huguette Roe/Shutterstock.com

Figure 16-4. This machine is crushing and shredding a hard drive, which will completely destroy the data on the drive.

For the most sensitive data, mechanical destruction of the drive is the best solution. There are several ways to mechanically destroy a drive. One method is to shred or chop it into small pieces, as shown in Figure 16-4. Other methods include punching holes in the drive or burning it at an extremely high temperature.

Defending Against Cyber Attacks

In the rapidly changing world of cyber attacks, it is a very good idea to run cyber-defense software. Cyber-defense software, usually called **antivirus software**, detects and removes malicious software from a computer. Most also actively prevent infections. Many companies offer cyber-defense software. Some are for-purchase and some are offered as freeware or open-source software.

GS5 Computing Fundamentals
7.5.1, 7.5.2

Some antivirus software always monitors for viruses, which is known as *real-time protection*. With some software, however, a scan must be manually started. If the antivirus software detects a virus, it should be removed as quickly as possible. Most antivirus software will remove the virus as soon as it is detected. In some cases, however, the user must manually tell the software to remove any virus that is found. This added step has the advantage of being able to tell the software that a particular file or program is safe, but this should be done only if you are certain the file is not infected. A file that antivirus software thinks is infected when, in fact, it is not is called a *false positive*.

If for any reason a virus cannot be removed, it will be quarantined. This means the virus is isolated from the rest of the files on a computer. Once in quarantine, the virus cannot infect anything else. This is especially helpful if a critical file, such as a registry file, is infected.

Cyber threats rapidly evolve. Therefore, the software must be regularly updated. In most cases, the software will check for updates at a set interval, such as once a day or once a week. In this way, the software can quickly respond to new threats.

FYI

Cyber-defense software may be called antivirus, antimalware, or antispyware software. It may be known by other names as well.

Hands-On Example: 16.1.2

Computer Viruses

Computer viruses have been around for decades. Some viruses target a specific operating system, while others seek to exploit a fault in a general protocol.

1. Launch a browser, and navigate to Wikipedia.
2. Using the search function, enter the search phrase antivirus software.

Hands-On Example 16.1.2 (continued)

3. Read the section of the article entitled Identification Methods.
4. What are the five basic methods of identifying viruses?
5. Read the section of the article entitled Issues of Concern.
6. Summarize the issues of concern.
7. Search Wikipedia for the phrase computer virus, and open the article of the same name.
8. Read the section of the article entitled "Recovery Strategies and Methods."
9. Summarize the various basic processes that can be used to remove a virus.

16.1 Section Review

Check Your Understanding

1. How is a computer worm different from a computer virus?
2. When is hacking legitimate?
3. What does the HTTPS protocol do?
4. What is the purpose of a CAPTCHA?
5. What does it mean to quarantine a virus?

IC3 Certification Practice

The following question is a sample of the types of questions presented on the IC3 exam.

1. Which of the following is software that secretly collects a user's data and behavior?
   A. computer virus
   B. spyware
   C. scareware
   D. hacking

Build Your Vocabulary

As you progress through this course, develop a personal IT glossary. This will help you build your vocabulary and prepare you for a career. Write a definition for each of the following terms and add it to your IT glossary.

adware
antivirus software
bot
cache
censorship
completely automated public Turing test to tell computers and humans apart (CAPTCHA)
computer virus
computer worm
cookies
data vandalism
hacking
malware
phishing
pop-up
ransomware
scareware
social engineering
spyware
Trojan horse

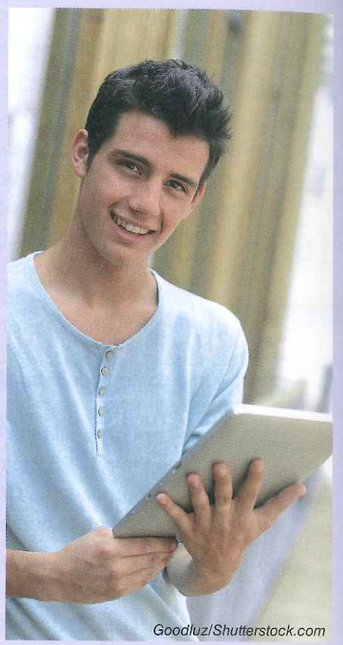
SECTION 16.2

IDENTITY PROTECTION AND ETHICAL BEHAVIOR

Essential Question

How does your ethical behavior online affect others in society?

Millions of people fall victim to fraud each year. In fact, the Federal Trade Commission (FTC) estimates that as many as nine million Americans have their identities stolen each year. The impact can be financially and emotionally devastating. Victims have to spend countless hours and dollars trying to correct the damage.



Goodluz/Shutterstock.com

Computer users should protect their identities when visiting websites. Know what information is being collected, by whom, and how it will be used. Websites track visitors as they navigate through cyberspace. Most legitimate websites include a privacy statement, typically found at the bottom of the home page. This statement should detail the type of information the site collects about its visitors and how users can control the information that is being gathered.

LEARNING GOALS

After completing this section, you will be able to:

- List precautions for protecting your identity on the Internet.
- Explain ways to protect your identity in e-mail communication.
- Describe ethical behavior in cyberspace.

TERMS

e-mail filters
ethics
identity theft
online piracy
pharming

Identity Protection on the Internet

Identity theft is an illegal act that involves stealing someone's personal information and using that information to commit theft or fraud. Identity theft is rampant on the Internet. This results in millions of lost dollars each day. Most credit card companies will compensate victims of online fraud. However, the victim still pays a huge price in time and aggravation. Here are steps each Internet user should take:

- Never click any links in unsolicited e-mail.
- Do not set social media profiles to public.
- Immediately delete messages from suspicious senders.
- Fill in only required fields in online forms and consider using an alternate spelling of your name.
- Carefully inspect the terms of service for websites.
- Be sure to understand the purpose of any check box relating to sharing your information.
- Ensure that the lock symbol is shown in your browser's status bar and look to see that the URL begins with https, indicating that a secure connection is being used.
- Use software that color-codes websites as to their security risk, known as secure-search software.

GS4 Living Online 5.1.1

Ethics

Bypassing Security

Computer users and network administrators take steps to ensure the security of their computers. Trying to bypass security measures is unethical and, in many cases, illegal. Breaking into a computer or network should be viewed as no different from breaking into a house or business.

LAN, WAN, and VPN Security

The primary goals of network security are availability, confidentiality, and integrity. But how much security can a user expect from a LAN, WAN, or VPN? All are generally secure. Security for LANs and WANs is generally very strong. However, much of the security depends on the network administrator, plus the hardware and software security resources. The network administrator must maintain server firewalls and access-control lists to prevent unauthorized access. He or she must also require appropriate credentials to access network resources. He or she must ensure all sensitive network traffic is encrypted. This makes it extremely difficult for a hacker to decipher any captured network traffic.

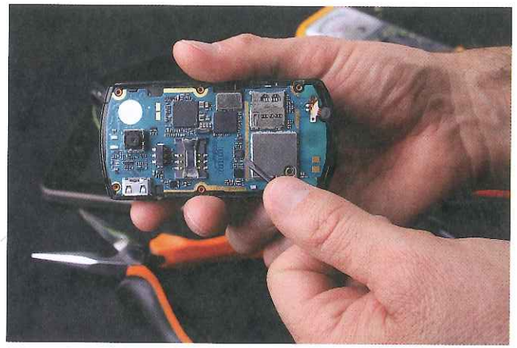
The best security system for portable or remote use is a VPN card. VPN software encrypts the data, inserts it into an IP packet for Internet compatibility, and sends it through a special tunnel. The packet is then decrypted at the other end of the tunnel. Several tunneling protocols are available: IP security (IPsec), point-to-point tunneling protocol (PPTP), and layer 2 tunneling protocol (L2TP). This increased security allows remote users to very securely transmit e-mail.

Wireless Network Protection

GS4 Living Online 2.1.3

Wireless networks are not as secure as the traditional wired networks. However, the risk on a wireless network can be minimized by enabling encryption, changing the default password, changing the service set identifier (SSID) name of the network, turning off SSID broadcasting, and using the MAC filtering feature. The MAC filtering feature allows you

to designate and restrict which computers can connect to the wireless network. Be aware that devices using wireless networks are just as vulnerable to viruses and hackers as wired devices. Only download applications from trusted sources.



mickyso/Shutterstock.com

Figure 16-5. At its heart, a smartphone is just a computer.

Security Risks with Audio and Video Applications

All smartphones are computers, as shown in Figure 16-5. They are increasingly targets of cyber attacks. Hackers seek ways to exploit weaknesses related to text messaging via SMS. Denial of service is a common attack. Hackers can also attach virus-infected image files or ring tones that are transmitted via MMS. When these files are opened, they infect the smartphone. The virus is also forwarded to everyone in the address book.

Videoconferencing and VoIP transmissions can also be hacked. Most often, these hacks have been denial of service attacks. Hackers have also developed viruses that stop the stream of video packets and freeze the screen image. Even real-time videos being transmitted from cell phones to other computers can carry viruses. Programs have been developed to detect virus infections in near-real-time audio and video streams. These antivirus programs can detect viruses in any streaming files, such as MP3 audio files. The development of the real-time streaming protocol (RTSP) made the transmission of video and audio data more efficient and secure.

HANDS-ON EXAMPLE 16.2.1

IDENTITY THEFT

Identity theft is a real online problem. However, identity theft is not limited to online activities. The Federal Trade Commission (FTC) provides information on how to protect yourself from identity theft and what to do if you are a victim.

1. Launch a browser, and navigate to www.consumer.ftc.gov, which is the Federal Trade Commission consumer website.
2. Using the search function, enter the search phrase identify theft.
3. Locate the link for the featured information title Identity Theft. Alternately, directly navigate to www.consumer.ftc.gov/features/feature-0014-identity-theft.
4. Read the information.
5. What are the three steps to take if you have been the victim of identity theft?
6. Click the link for How to Keep Your Information Secure.
7. Read about how to keep your online information and your devices secure.

E-commerce Security

GS5 Computing Fundamentals 7.7.1, 7.7.2

GS4 Living Online 5.1.1

E-commerce is buying and selling products or services over electronic systems such as the Internet. E-commerce involves electronic funds transfers, online transaction processing, Internet-based marketing, electronic-data interchanges, inventory-management systems, and automated data-collection systems. Online retail sales in the United States now account for hundreds of billions of dollars each year. Recent figures estimate that over 70 percent of Americans have made online purchases. This explosion of e-commerce has led to a new generation of associated cybersecurity threats.

Privacy and data security are major concerns for both consumers and e-commerce businesses. Due to cybercriminals, millions of stolen credit- and debit-card numbers have been posted on the Internet. A major study by LexisNexis found that the value of merchant losses each year due to fraud exceeds the value of consumer losses from fraud by more than 20 times. However, consumers in the United States engaging in e-commerce are victims of fraud for billions of dollars each year.

Companies assess the risk of e-commerce transactions, often on each individual purchase. Checks include seeing whether the telephone number provided by the purchaser matches the ZIP code where the item is to be shipped and whether the IP address of the computer used to place the order is in that same region. Such instant risk analyses will also check whether the order is for a large number of high-value items, which could be fraud. The analysis will also look at the shipping address of the order. An order shipped to an unusual or foreign address also could be a possible sign of fraud. All of these checks are done through software.

Today, every e-commerce system must address the following key issues:

- privacy
- integrity
- authentication
- nonrepudiation
- protection from denial of service (DoS) attacks

Information exchanged during a transaction must be kept private at all times. Even after the transaction is complete, the information must be kept from unauthorized parties. The integrity of the information must be guaranteed by making sure no information has been altered. The information must be authenticated. This is done by forcing both parties to prove their identities. Nonrepudiation is proving that exchanged information has indeed been received. By preventing DoS attacks, the information will be available to the intended users.

Merchants assume the bulk of the risk of e-commerce. However, customers also have a responsibility to help out. Start by always providing accurate information on the online order form. When creating an account, provide the answer to the security question that would be difficult to predict. Remember, social media sites can be used to gather personal information about you, such as your pet's name. Reduce your

Internet profile. If you do so, it will be harder for cybercriminals to find information about you.

Frequently check your bank and credit card statements for fraudulent charges. If you find any fraudulent charges, *immediately* contact your bank and cancel your credit card. Never use a debit card for an online purchase. A credit card offers protection, but a cybercriminal with your debit card information can drain your bank account. Once the money is gone, it is very hard to get it back.

An alternative to using a credit card is to use a merchant service. PayPal is an example, but there are others. With a merchant service, you provide your financial information once to the service, then the service conducts the transactions. Your bank account and credit card information is never exposed to the merchant. Credit card companies also offer a similar service through single-use credit card numbers. The number is linked to your credit card, but it is good for only one purchase. In some cases, you can even specify which merchant the number is good for and for how much.

Maintain a healthy skepticism about the authenticity of e-commerce websites. Do not just click a link that says it will go to a legitimate site. Manually enter the actual URL address into the browser's address bar. If suspicious about a link to a company, look up the company directly using a search engine. Finally, just because the site shows an "official" or "verified" logo does not mean it is a legitimate site.

Be extra suspicious of foreign sites. If the IP address is in Russia or Nigeria, for example, investigate the site further before providing any information. Also look for the top-level domain. Websites based in many countries must use that country's top-level domain, such as .ru for Russia or .cy for Cypress.

Avoid sites that consist of very few web pages and offer only general descriptions of products and service. Sites that appear to have been quickly created may not be legitimate. Also be wary of websites that seem to have bugs. Programming issues may be a sign of an amateur who is unable to properly protect data.

Be suspicious of websites containing offers that are just too good to be true. For example, if major retail sites offer a sleeping bag for $75, a site offering the same sleeping bag for $15, including shipping, should raise a warning. Major retailer sites are generally trustworthy, but for smaller independent e-commerce sites, be sure to do your research before placing an order.

Always look for the HTTPS protocol in the browser's address bar before entering personal data. This indicates the site is secure. Also, most browsers will provide a visual indication, such as a lock icon, that the site is secured.

GS5 Computing Fundamentals 7.1.1

Identity Protection in E-mail

Users can take precautions to protect their personal e-mail accounts. One method is to create a "junk mail" account that you use whenever you need to enter an e-mail address in a form. This can often be done

as part of the e-mail provider's service. If not, use one of the many free e-mail services. This reserves the primary e-mail address for personal or professional e-mail. Junk mail, including spam and phishing scams, is more likely to stay out of the primary e-mail. Additionally, any mail received in the junk account can simply be deleted. Because the mail is never read, security is enhanced.

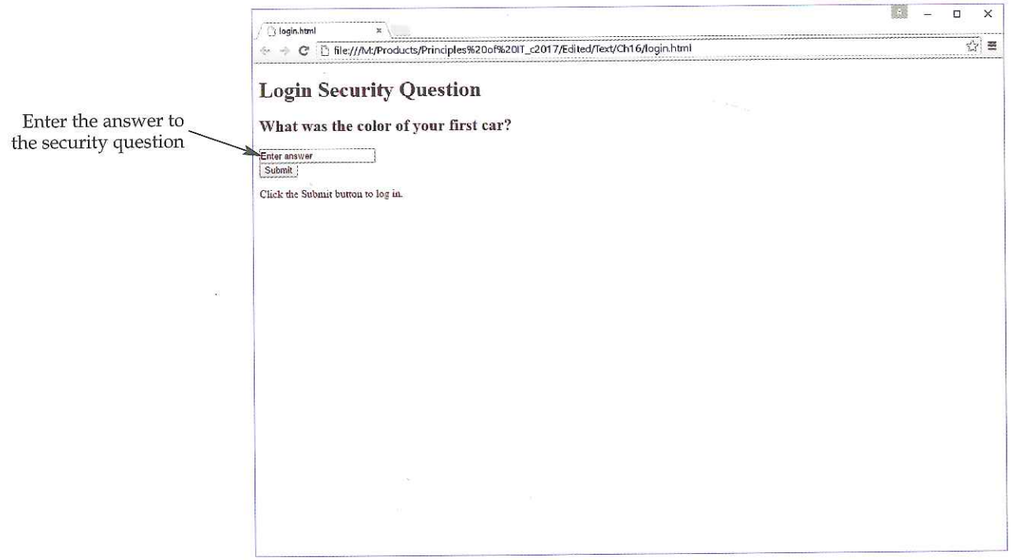
FYI

Avoid setting up auto replies on your personal accounts as this will confirm the e-mail account is valid and active.

Consider creating a username that is misleading or does not reveal personal information. The name GolfSmith6503 may be good if the person does *not* play golf, is *not* named Smith, and does *not* have the number 6503 as a street address or partial phone or Social Security number. For a person named Smith who plays golf and was born June 5, 2003, this is a poor choice for a username.

Periodically check the filter and forwarding functions for each e-mail account. Hackers can enter an account and establish a rule to forward e-mail messages to an address. If you see forwarded mail that you did not forward, the e-mail account has probably been hacked. If you find your e-mail has been hacked, immediately change your password, and then perform a scan with your antivirus software.

If provided, take advantage of the option to create a specific security key. A security key is often a question that must be answered to gain access, as shown in Figure 16-6. For example, the question may ask for your pet's name or the name of your favorite grade school teacher. Some providers allow users to create their own security questions. Some providers also allow selection of a sign-in seal or a favorite color as the security key. Questions that ask for a mother's maiden name or your birthplace are poor security keys. Do not use the same questions and answers for different accounts.



Goodheart-Willcox Publisher

Figure 16-6. A common security key is a question that you have to answer.

Pharming is another way your identity can be stolen. In **pharming**, a virus or other malware infects the computer and takes control of your web browser. Then, when you enter the URL of a legitimate website, you are taken to a fake website that looks like the real website. Any information that you think you are entering on a legitimate website is instead stolen.

E-mail Awareness

Avoid downloading programs and files from unknown sources or from sources that appear to be suspicious. What makes a source suspicious? There are precautions you can take to help recognize suspicious e-mail.

Check Questionable Messages

E-mail addresses that appear to have been computer-generated should be questioned. For example, an e-mail from 67ghvv786@gmall.com is suspicious for two reasons. First, the information before the at sign (@) is just letters and numbers. This could be computer-generated. Second, the domain name after the at sign appears at a glance to be from Gmail. However, looking closely, the domain is gmall.com, *not* gmail.com. Using a domain that is very close to a well-known domain is a common way scammers try to fool people.

Be Wary of Attachments from Unknown Sources

Always be suspicious of attachments from sources you do not recognize. Never open an attached file unless you know and trust the source. Opening an attachment may launch malware. Do not rely on your antivirus software to stop the malware. Rather, be safe and do not open the attachment.

Do Not Click Links in E-mail

Offering links in an e-mail for online shopping is one of the oldest ways hackers use to carry out scams. Messages that offer sales are suspicious. If the offer appears to be from a legitimate source, open a browser and manually navigate to the site claiming to offer the sale. Then, manually search for the sale. Shop only at sites that are known and trusted. When entering payment details, make sure the URL for the page is secure. A secure URL begins with https instead of http. Also, most Internet browsers display a lock or other icon somewhere in the browser window to indicate a secure connection. After completing the order, sign out of the site or close the browser.

FYI

Never use a debit card for online purchases because it does not offer as much protection against fraud as a credit card.

Every few months hundreds of people succumb to an e-mail hoax related to Microsoft patches. The phony e-mail includes a fake or stolen Microsoft logo, fake return address, and phony links. Microsoft *never* sends out patches or updates by e-mail. There are no exceptions. Similar scams involve messages designed to look like a bank trying to update its customers or a firm trying to contact lottery winners. Never follow the links in these e-mails. If you think your bank may be trying to contact you, manually contact the bank yourself. Mention the e-mail so the bank can alert other customers to the scam.

Stay Alert for Phishing Attempts

GS4 Living Online 5.1.1

Ignore unsolicited e-mail that asks for personal information. These are likely phishing scams. Phishing is an attempt to get you to provide information that can be used to break into accounts and steal your identity. Phishing scams usually ask for personal information such as your address, SSN, and phone number. This information can be used to gain access to financial accounts and your online presence.

Never reply to an e-mail asking you to "verify your information" or to "confirm your user ID and password." The most common form of phishing is e-mail pretending to be from a bank, governmental agency, or legitimate retailer or organization. For example, a cyber criminal sends an e-mail that appears to be from Facebook. The e-mail states there has been unusual activity on your account and asks you to verify your username and password. However, when you enter the information, it is stolen. Your Facebook account is then hacked, and the criminal uses information found there to locate even more information about you elsewhere.

FYI

Visit the website www.fraud.org run by the National Consumers League for more information on identity theft.

E-mail Filters

GS4 Living Online 4.2.2

E-mail filters, also called rules, are used to automatically route incoming e-mail to a specified inbox folder, as shown in Figure 16-7. A filter is especially useful to send e-mail from an address known to be spam to the Trash or Junk Mail folder. However, filters can also be used to automatically send e-mail to folders based on project names, friend names, or hobbies. Most e-mail clients allow many filters or rules to be created.

One drawback to e-mail filters is that a filter may incorrectly identify incoming mail. A legitimate message may be sent directly to the Trash or Junk Mail folder without being seen by the user. Another drawback is that the user may overlook the information if it is automatically routed to another folder. However, most e-mail clients indicate how many unread messages are in each folder.

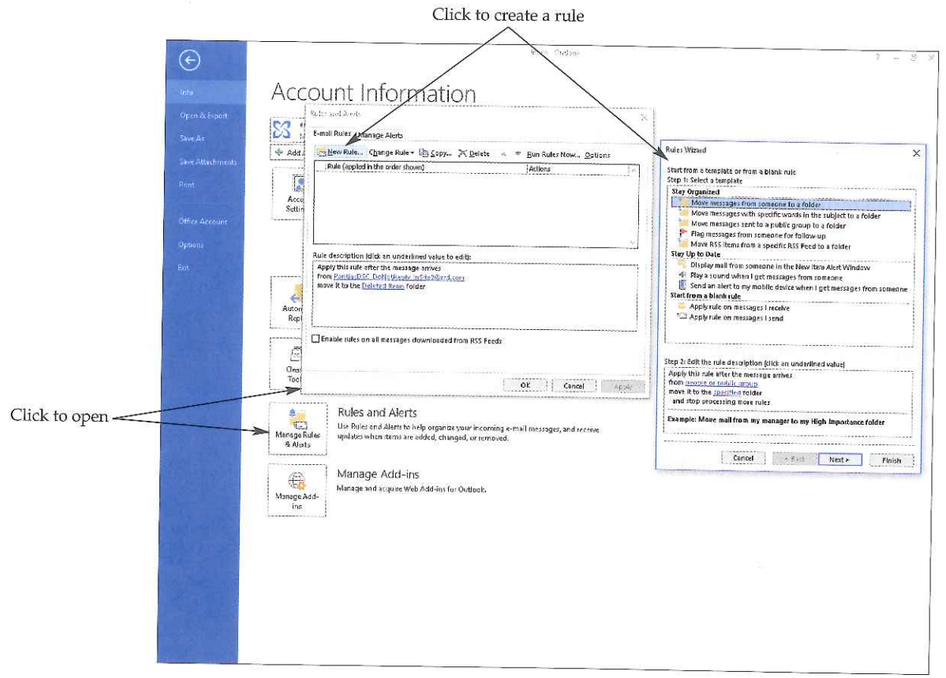
E-mail Account Piracy and Protection

Some hackers focus on taking control of e-mail accounts. Once an account is hacked, it is used to send spam to the entire e-mail directory. If anybody replies to the spam, the hacker can then take control over that account, sending spam from it. How can a user prevent an e-mail account from being pirated? There are several precautions to take.

Before replying to an e-mail, verify the address. Look at the properties of the sender's name. This is usually done by hovering the cursor over the sender's name or right-clicking on the name and selecting **Properties** or **Message Options** in the shortcut menu. Make sure the e-mail address is correct. A common trick is to make an e-mail look like it came from a legitimate source, but the address is actually a scammer.

FYI

There is much information on the Internet concerning e-mail authentication.



Goodheart-Willcox Publisher

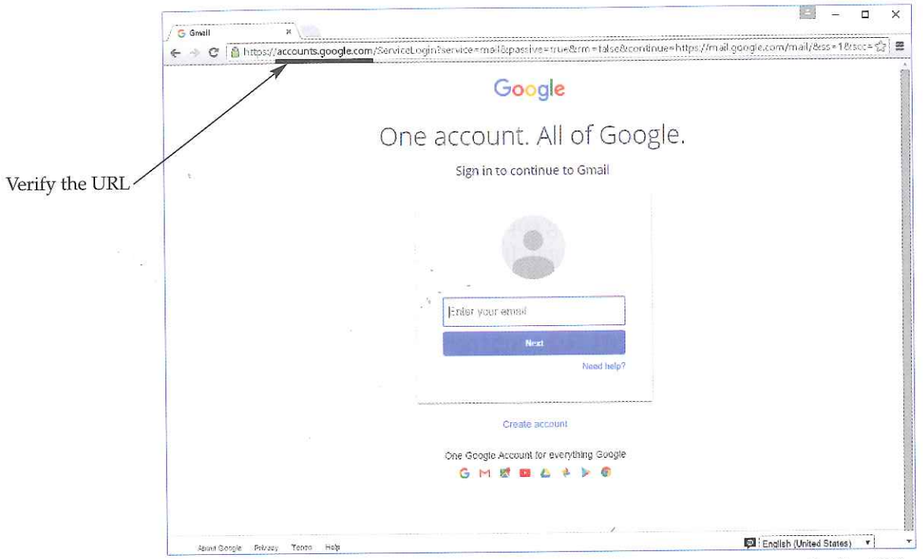
Figure 16-7. In Microsoft Outlook, rules can be set up to automatically route incoming mail to a specific folder.

Check whether the e-mail was authenticated by the sending domain. This is usually done by right-clicking on the e-mail message and selecting **Properties** or **Message Options** in the shortcut menu. Check that the domain in the properties matches the domain shown as the e-mail address. The reply will be sent to the domain given in the properties, regardless of what is actually displayed as the e-mail address.

If using web-based mail, make sure the URL on the sign-in page is correct, as shown in Figure 16-8. For example, when logging into Gmail, does the URL actually end with google.com? Does the Yahoo Mail URL actually end with yahoo.com? If the URL is not correct, do not log in.

If anything is suspicious, contact the organization from which the message appears to have been sent. Do not reply to the message or use any links within it. Instead, visit the official website of the company in question, and find the correct contact address.

Take action quickly if you mistakenly entered personal information in a fake e-mail message. Copy the message header and the entire text of the message, and e-mail it to the Federal Trade Commission at spam@uce.gov. If you entered credit card or bank account numbers, immediately call the financial institution. If you think you are the victim of identity theft, contact local law enforcement.



Goodheart-Willcox Publisher

Figure 16-8. If using web-based e-mail, make sure the URL on the sign-in page is correct. Here, the URL is for Google, which is correct.

Ethical Behavior in Cyberspace

Ethics are the principles of what is right and wrong that help people make decisions. Ethical actions are those actions in which the user applies ethics and moral behavior. Acting ethically means doing what most individuals and social groups believe to be morally correct and good for society. This is more than following specific rules and laws. It means doing the right thing, even when nobody is watching. Cyberbullying, which is discussed in Chapter 15, is an example of unethical behavior in cyberspace. There are legal and ethical responsibilities for everything you do online.

Legal Responsibilities

As described in Chapter 8, intellectual property is something that comes from a person's mind, such as an idea, invention, or process. The World Intellectual Property Organization (www.wipo.org) defines intellectual property as "creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names, and images used in commerce." Laws protect individuals from unauthorized and unethical use of intellectual property. As discussed in Chapter 8, copyrights, patents, and trademarks protect intellectual property. These are most often enforced by national courts. The United Nations Commission on International Trade Law provides international support.

All software comes with a licensing agreement or terms of use, as described in Chapter 8. Websites that you must join, such as Facebook and Twitter, also have terms of use, sometimes called *terms of service.* This

FYI

If you check the box that says you agree to the terms, you are legally bound by them, even if you never read the document. Always read and understand the terms before agreeing to them.

legal document explains acceptable uses of the software, if the software can be copied or installed on multiple devices, and if the code or part of it can be reused. In the case of a website, the document will also explain what can be posted or shared. It is illegal to violate this agreement. Punishment may include a fine, imprisonment, or both.

Be careful on sites that share files of music, movies, games, and software. The material on these sites may be protected by copyrights. Downloading copyrighted material without permission of the copyright holder is illegal. It is theft and called **online piracy**. Online piracy is no different than walking into a store and stealing a DVD or CD.

Ethical Responsibilities

Ethical use of the Internet involves not breaking the law. It also involves respecting the intellectual property of others. As discussed in Chapter 8, plagiarism is claiming another person's material as your own, which is both unethical and illegal. If you *copy* the work of others without permission, even if you credit the source, you are committing plagiarism. However, it is entirely ethical to use the Internet while creating an original mixture of ideas. While doing this, be sure to cite known sources for all major and unusual ideas.

Copying whole sentences and paragraphs and using them as your own without attribution is unethical. However, consulting articles can be an effective first step while researching a subject. Articles can provide a general introduction to the topic. The See Also and References sections at the end of the article can also provide other sources of information.

Just as the Internet has made it easy to find information, it has made discovering plagiarism easy. There are many resources that can be used to check for plagiarism. Some of these are free, while others must be purchased. These resources make it easy for teachers and others to quickly find out if written material has been plagiarized.

GS4 Living Online 5.1.1

Be Social Media Savvy

Make sure your social networking profiles are set to private. Sites such as Facebook and Twitter should not be allowed to display any information that can be used to identify you. Check the security settings for each account. Be careful what information you post online. Do not over-share information. There are unethical cyber surfers who troll the Internet looking for personal data to steal and sell to others. Even if a photo appears innocent, it may contain, for example, the name of your school. If you use this as part of your password, you have given hackers a hint.

Configure all of your social media accounts to control your status, who can gain access to what information, who can post, and who can share account information with others. The methods for making these security settings differ by site. Use a search engine or the site's search function to find out how to change security settings.

HANDS-ON EXAMPLE 16.2.2

SOCIAL MEDIA SECURITY

Before signing up for a social media account, be sure to investigate its privacy policy. It should be easy to find this information even without logging in.

1. Launch a browser, and navigate to Facebook.
2. Click the **Privacy** link at the bottom of the page.
3. Read the information on the page. It explains Facebook's policies on how information is received, posted, and shared; how cookies are used; and what information is seen by web surfers.
4. What steps are necessary to delete information about yourself?
5. Navigate to LinkedIn.
6. Click the **Privacy Policy** link at the bottom of the page.
7. Read the information on the page. It explains LinkedIn's policies on how information is collected and saved; how information may be posted, shared, and restricted; and how account holders may access, correct, and delete information.
8. What steps are necessary to delete information?

16.2 SECTION REVIEW

CHECK YOUR UNDERSTANDING

1. What are two indications in a browser that a secure connection is being used?
2. List four precautions you can implement to provide safety for e-mail.
3. What does an e-mail filter or rule do?
4. Which type of legal document explains acceptable uses of the software?
5. What unethical behavior is shown by copying someone else's work and claiming it as your own?

IC3 CERTIFICATION PRACTICE

The following question is a sample of the types of questions presented on the IC3 exam.

1. Which of the following is a safe practice when using web-based mail?
   A. Use only a public Internet provider.
   B. Allow the browser to save your password.
   C. Make sure the URL on the sign-in page is correct.
   D. Look for the secure icon on the web page.

BUILD YOUR VOCABULARY

As you progress through this course, develop a personal IT glossary. This will help you build your vocabulary and prepare you for a career. Write a definition for each of the following terms and add it to your IT glossary.

e-mail filters
ethics
identity theft
online piracy
pharming