 Estimated Time:
2 hours

LESSON 27

Communications and Collaboration

■ OBJECTIVES

Upon completion of this domain, you should be able to:

- Explore communication methods.
- Identify the advantages of electronic communication.
- Solve electronic communication problems.
- Protect against viruses and other security risks.
- Engage in professional and effective communications.
- Use other e-mail options.
- Follow guidelines for electronic communication.

■ DATA FILES

You do not need data files to complete this lesson.

■ WORDS TO KNOW

filtering
fraud
hoax
logic bomb
netiquette
phishing
pyramid scheme
RDF Summary
spam
tagging
teleconferencing
time bomb
Trojan horse
urban legend
virus
worm

In Lesson 26, you learned about e-mail. In this lesson, you expand your knowledge of e-mail and learn about other electronic communication methods, the appropriate use of each method, and the advantages and disadvantages associated with them.



Exploring Communication Methods

When you work with computers to communicate, you can use a variety of electronic communication methods. In most instances, people with whom you are corresponding and the topic of the correspondence determine which communication method to select. Electronic mail (e-mail), which was discussed in detail in Lesson 26, is best used in the following situations:

- When the correspondence might require a paper trail
- When the correspondence covers multiple points
- When the correspondence needs to be accessed frequently

Instant messaging (or texting), also introduced in Lesson 26, is best used when correspondence needs to be accessed in real time. Each person can send and receive messages from a computer, cell phone, or other mobile device (see Figure 27-1).

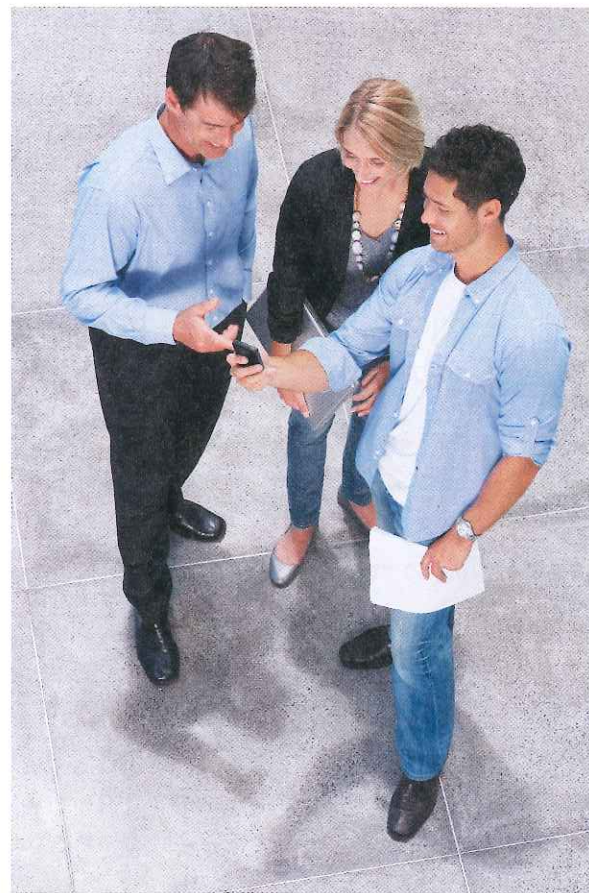


FIGURE 27-1 Text messaging

Teleconferencing uses a telecommunications system to serve groups, permitting the live exchange and sharing of information between two or more people. Generally the communication medium is a telephone line. This communication method has expanded into video conferencing, which adds two-way video transmissions to the two-way audio of phone calls, and Web conferencing, which allows groups of people to communicate with each other online.

Syndication (Really Simple Syndication, or RSS), also known as Rich Site Summary and **RDF Summary**, are formats originally developed to syndicate news articles electronically. This communication method is now widely used to share the contents of blogs.

In some instances, a combination of the preceding communication methods may be used, especially for group collaboration. For example, a group of people who live in different parts of the country may be enrolled in an online class. This group can use e-mail, instant messaging, and teleconferencing to communicate about a class project. They could also use a blog to post project updates and social networks to keep in touch with each other.

Identifying the Advantages of Electronic Communication

Electronic communication offers many advantages over other types of communication. The communication is not restricted to a specific place and time, allowing people to communicate from remote locations using computers and cell phones. When you communicate electronically, you can use text and graphics, making it easy to forward and route messages. You can also use more than one type of correspondence, including one to one, one to many, and many to many. In one-to-one communication, one sender communicates with one receiver. E-mail is an example of one-to-one communication. One-to-many communication involves a sender communicating with many receivers. An e-mail message sent from one person to a group is an example of one-to-many communication, as is posting files on an FTP site and using Telnet. Many-to-many communication such as file sharing, blogs, wikis, and tagging enable people to both contribute and receive information. **Tagging** is used in blogs and other informational sites to simplify the search process. In a many-to-many example, a group might use a discussion board where everyone can post information and read all of the postings.

VOCABULARY

teleconferencing

RDF Summary

tagging



Using collaborative communication tools, you can engage in all three types of correspondence. Collaborative software allows you to use live voice, full-motion video, and interactive desktop sharing between yourself and one other person or an unlimited number of people (see **Figure 27-2**).



All participants can communicate with one another

FIGURE 27-2 Collaborative communication

Electronic communication also fosters community building by connecting members of a group who share the same general interest. The community could be connected by a social media site, blog, mailing list, message board, or other type of electronic communication, which allows them to exchange information and organize their efforts to meet a goal.

Another advantage is online document sharing, which allows users to create and edit documents online while collaborating in real time with other users. Google Docs is an example of online document sharing.

Other advantages of electronic communication follow:

- Speed is almost instantaneous, which means increased accessibility and enhanced interaction.
- Cost is minimal or even free in some instances. E-mail, for example, is a service that is part of most networked computers. Price remains the same whether you send and receive a hundred messages or a thousand messages. Based on the device that is being used, instant messaging is a free service or has a minimal fee. Teleconferencing, on the other hand, generally involves a fee for the host. However, using this service can eliminate travel expenses for people who would otherwise need to meet in person.
- Access is available from various devices such as computers and cell telephones.
- Forwarding and routing of messages can be accomplished in an instant. Using e-mail software, you can click the message, select the address of the individual to whom it is to be forwarded, and then click the Forward button.

Routing is the process of selecting paths in a network along which to send network traffic. It can be an automatic or an individual process. For example, a network administrator might receive a message that a server is going to be offline for a specific time. The administrator can then route this message to everyone who would be affected.

Like many companies, Microsoft hosts blogs to communicate with customers. In the following Step-by-Step exercise, you visit a Microsoft blog for Windows users.

Step-by-Step 27.1

1. Click the **Internet Explorer** button on the taskbar (or start Internet Explorer the way you usually do).
2. In the Address bar, type **http://windowsteamblog.com** and then press **Enter** to display the home page for Windows blogs (see **Figure 27-3**). Blogs change regularly, so the content displayed on your screen will differ from the figures.



FIGURE 27-3 Windows blogs home page

3. Point to the *Blogs +* button, and then click **Blogging Windows** to display the most recent post for the Blogging Windows blog (see **Figure 27-4**).

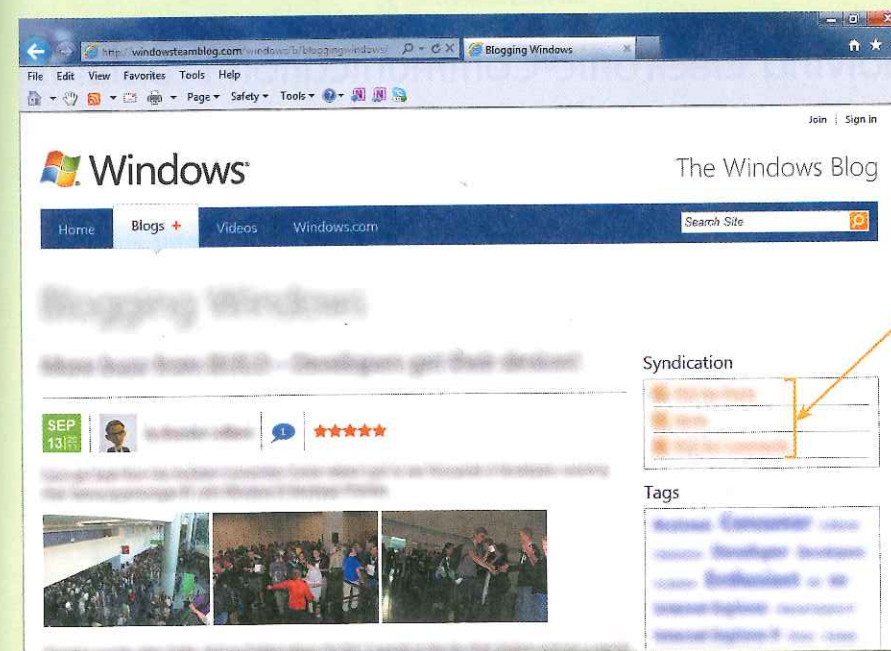
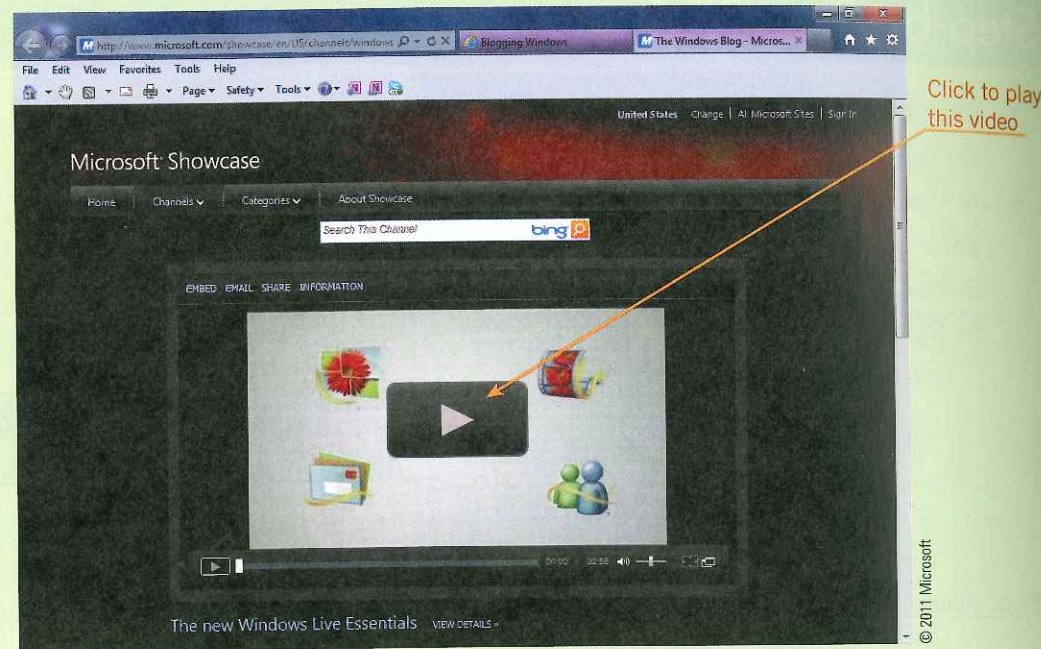


FIGURE 27-4 Post for the Blogging Windows blog

4. Scroll down to find a post that interests you. Use your word-processing program to write a summary of the post.

- Return to the top of the page and then click the **Videos** button to display a showcase of Windows videos (see **Figure 27-5**).

FIGURE 27-5
Showcase of Windows videos



- Watch a video of your choice, and then return to your word-processing document. Add a summary of the video you watched. Save your document as **Windows_blog** and submit it to your instructor.
- Close the Internet Explorer window.




Solving Electronic Communication Problems

Similar to other electronic technologies, electronic communication is not without problems. Windows 7, however, contains troubleshooting tools to help you identify and resolve computer communication problems.

Lost Internet Connection

Most electronic communication involves being connected to the Internet. You can then exchange e-mail messages, use Web conferencing software, or visit a collaboration Web site. Losing your Internet connection can be frustrating, especially if you are in the middle of an online conference or uploading important data for others to use. Depending on the problem, you may need to contact your ISP. However, you may be able to repair the problem with the Internet Connections troubleshooter. The following Step-by-Step exercise illustrates how to use this tool.

Step-by-Step 27.2

- Click the **Start** button  on the taskbar, and then click **Control Panel** to display the Control Panel Home window.
- Click **Network and Internet** to display the Network and Internet window (see **Figure 27-6**).

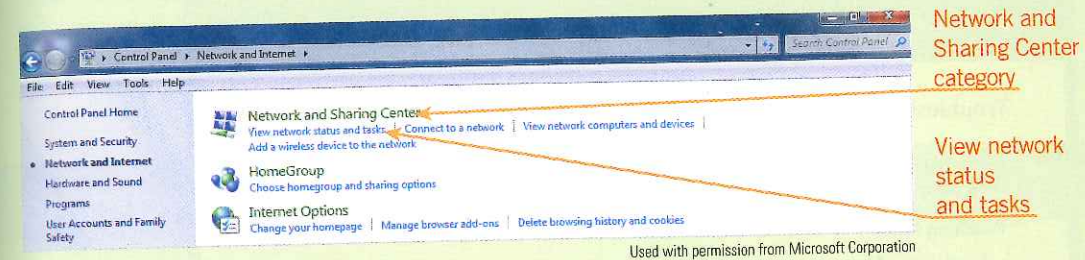


FIGURE 27-6
Network and Internet window

- Click **View network status and tasks** to display the Network and Sharing Center window (see **Figure 27-7**).

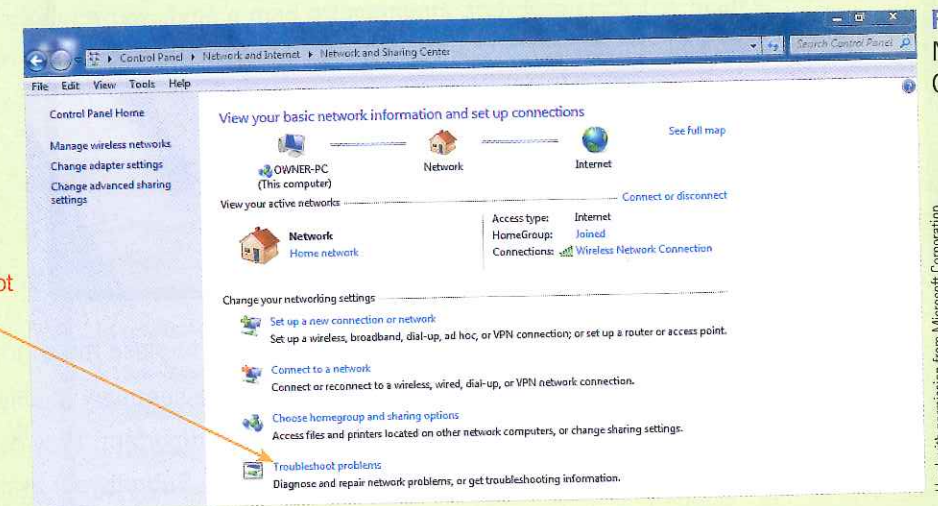
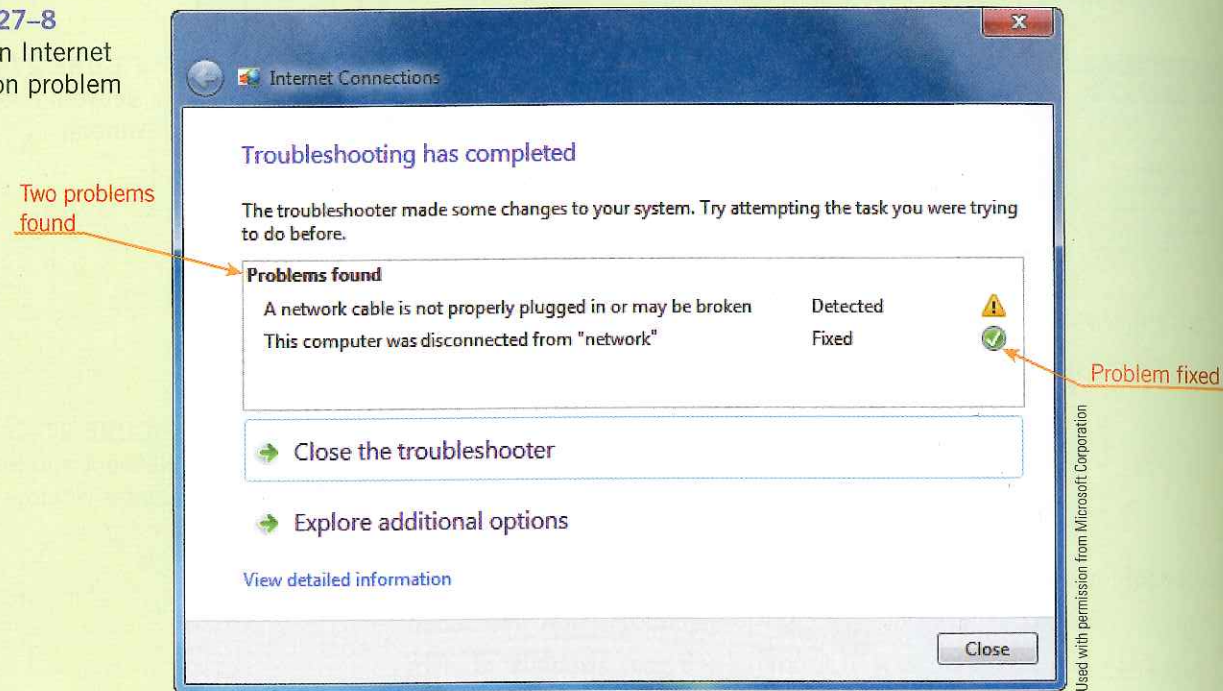


FIGURE 27-7
Network and Sharing Center window

- In the Change your networking settings section, click **Troubleshoot problems** to display a list of network troubleshooters.
- Click **Internet Connections** to open the Internet Connections dialog box.

- Click the **Next** button to start the troubleshooter. When the Internet Connections dialog box opens, click **Troubleshoot my connection to the Internet**. Windows scans your network devices and software. If it finds a problem, it tries to correct it. In any case, Windows reports the results of the scan, as shown in **Figure 27-8**. Your results will differ.

FIGURE 27-8
Solving an Internet connection problem



- Click the **Close** button or the **Cancel** button to close the window.
- Use your word-processing program to write a summary of why you think the Internet Connections troubleshooter is important. Provide an example of when and how you would use this tool. Submit your assignment to your instructor.
- Close the Network and Internet window.

E-Mail Software Problems

A failure in e-mail software to send or receive messages can result from various problems. Your service provider's connection could be down. If your connection to the Internet is still available, then checking your service provider's Web site could provide answers to your problem. Make sure your computer is connected to the Internet to isolate the problem to your e-mail service or software. Often, waiting a few minutes and then trying to send or receive messages results in success.

QUICK TIP

You can send an open Microsoft Office document without closing the file. Click the File tab, click Save & Send, and then click Send Using E-mail to send the document. You might perform this shortcut during a conference call to share an open document with participants.

Problems with Downloading and Viewing E-Mail Attachments

If you are unable to download or view an e-mail attachment, the size of the attachment might be the problem. Some e-mail programs limit attachment size and the number of attached files. If the message or attachment appears to contain harmful software (also known as malware), your antivirus software or e-mail program could be blocking the message. A third issue could relate to the sender and the type of e-mail—advertising, pornographic materials, or other unrecognizable documents, which also may be blocked by your e-mail program.

Windows Help provides suggestions on why you cannot view an attachment. In Step-by-Step 27.3, you access and review this Help information.

Step-by-Step 27.3

- Click the **Start** button on the taskbar, and then click **Help and Support** to display the Windows Help and Support window.
- In the Search box, type **e-mail attachments** and then click the **Search** button to display a list of Help topics related to the search text (see **Figure 27-9**).

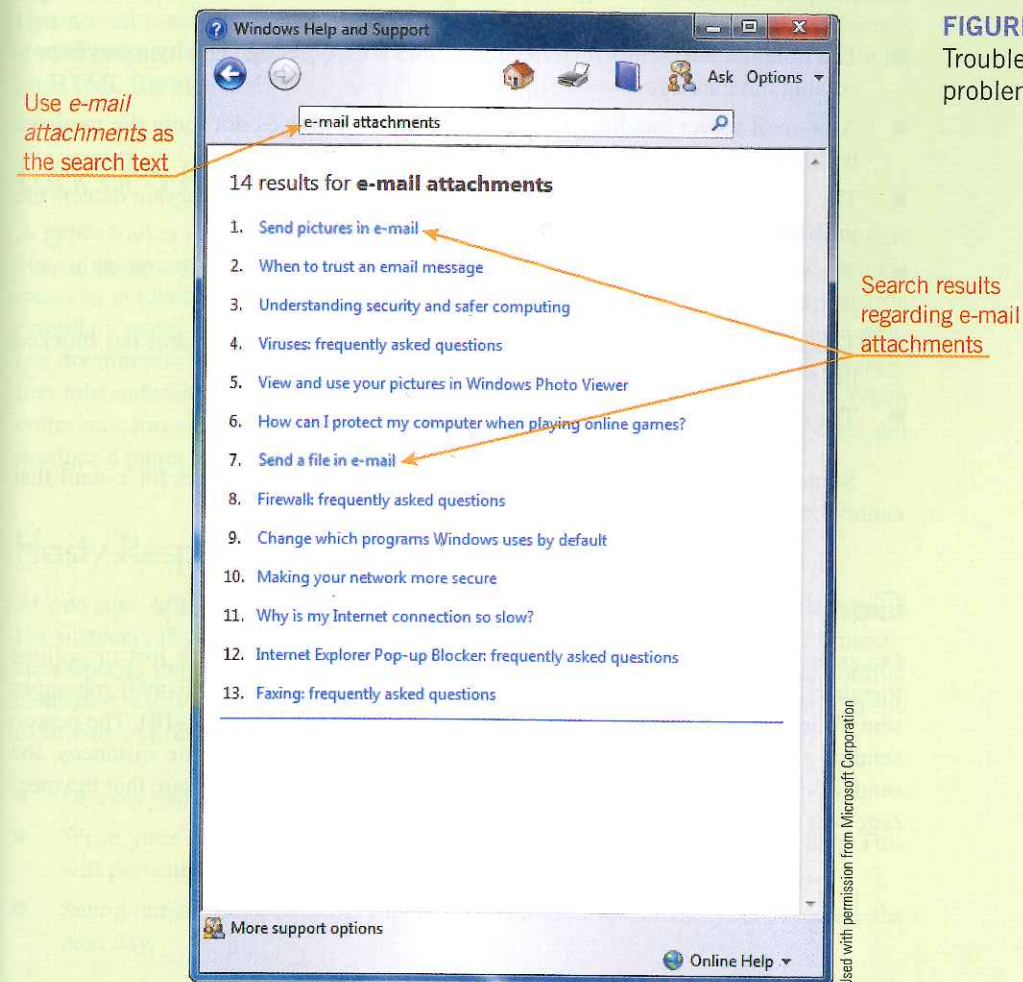



FIGURE 27-9
Troubleshooting attachment problems

3. Review the list of results. Two of the topics are directly related to e-mail attachments. Click the **Send pictures in e-mail** link and then read the topic, focusing in particular on the troubleshooting notes at the end of the topic.
4. Click the **Back** button  to return to the search results. Click the **Send a file in e-mail** link and then read the topic, focusing again on the troubleshooting notes at the end of the topic.
5. Use your word-processing program to explain what you should do before sending pictures as e-mail attachments. Also explain what types of files some e-mail programs block and what you can do if you have trouble sending these files.
6. Close the Windows Help and Support window.
7. Submit your word-processing document to your instructor.

Delivery Failure

E-mail delivery failure refers to a returned or “bounced” e-mail. This can happen for a number of reasons, including the following:

- The e-mail address was mistyped or is otherwise unrecognized by a server processing the message.
- An e-mail server handling the message is busy and does not route the message within a specified amount of time.
- The e-mail attachment may contain malware. The receiving program detects the problem and will not accept the message.
- The receiver has a spam-filtering program. Based on the e-mail content or subject, the program may identify the message as spam.
- The sender is known and the person to whom the message is sent has blocked the sender.
- The recipient’s mailbox is full.

Some e-mail programs return delivery failure (bounce) notices for e-mail that cannot be delivered. Others do not provide this service.

Garbled Messages/No Guaranteed Delivery

Occasionally, e-mail and other transmissions over the Internet are lost or spliced together. This occurs most often when Internet traffic is heavy. E-mail messages sent in rich text format (RTF) are garbled frequently (see **Figure 27-10**). The person sending the message should change the format to HTML. In some instances, the sender does not receive a notification of delivery failure and is unaware that the message was not delivered properly.

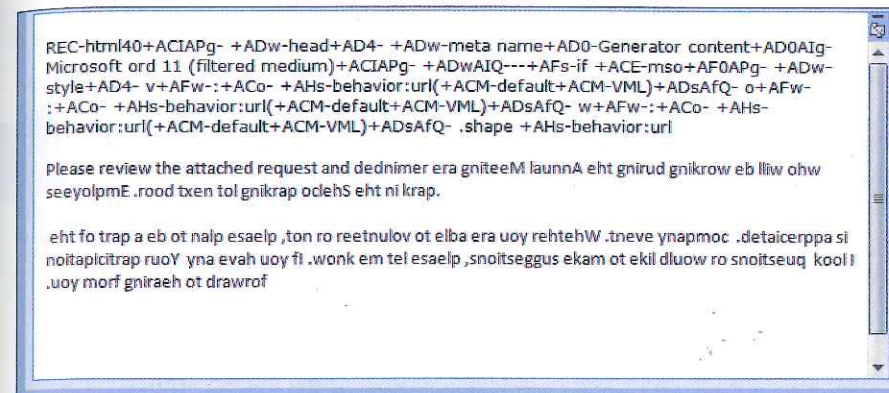


FIGURE 27-10 Garbled message

Lost Formatting

Microsoft Outlook and other e-mail programs provide at least two formatting options: HTML (Hypertext Markup Language) and Plain Text. Many programs also provide RTF formatting. HTML provides formatting options such as multiple fonts, bold text, colored headings, graphics, and links to Web sites. To use HTML when creating a message in Microsoft Outlook, click the Format Text tab in a New Message window, and then click the HTML button in the Format group. To format a message as plain text, click the Plain Text button in the Format group. Keep in mind that not all e-mail programs support HTML-formatted messages. If the recipient’s e-mail program does not support HTML, the message is displayed as plain text with an HTML file attached.

Lack of a Paper Trail

A paper trail is a written record, history, or collection of evidence created by a person or organization in the course of activities. Paper trails have been used in legal cases as evidence, for example. E-mail and other electronically stored information provide a paper or electronic trail similar to that of traditional mail and other written documents. Other types of electronic communication such as instant messaging, teleconferencing, and online conferences might not provide a paper trail. When communication needs to be documented, electronic communication that does not produce a paper or electronic trail could create problems.

Hasty Responses

At one time or another, everyone has sent an e-mail that they wanted to take back. For instance, if you receive an e-mail message that makes you angry, your immediate response may be to send a quick reply. This action could accelerate the conflict instead of resolving it. To avoid sending a message you later may regret, consider the following options:

- Discuss your response with someone else.
- Write your message, but do not include the e-mail address in the To line. This will prevent an accidental sending of the message.
- Save your message overnight as a draft and then reevaluate your response the next day.

Professional and Informal Communication

With the advent of online communication formats, the boundary between professional and informal communication has blurred. Computer technology has provided the tools to make composing messages easier and faster. The fast-paced media used for electronic communication demand a writing style that is clear and concise without sacrificing speed. This often results in informal messages that include abbreviations and conversational language. When writing professional communications, however, you should be more formal, taking time to compose sentences and paragraphs.

Volume of E-Mail Replies

Communications *netiquette*, a combination of the words net and etiquette, refers to good manners and proper behaviors when communicating through electronic media. Because most e-mail users report that their biggest problem is not spam but too much e-mail, keep the following netiquette guidelines in mind when replying to an e-mail message:

- **Reply to senders:** You have received an e-mail message and now you want to send a reply to the user. Click the Reply button, type your message, and then click the Send button. Verify, however, that your reply is necessary; do not send responses that do not apply to the original message.
- **Use Reply All only when necessary:** Reply All is another e-mail option. If you receive a message that also was sent to or copied to other recipients, for example, clicking the Reply All button sends your reply message to the sender and the other recipients. If the reply message does not apply to the other recipients, use Reply rather than Reply All to reduce the volume of e-mail replies.
- **Use Cc and Bcc sparingly:** Two other options are Cc and Bcc. Both options send copies of the message to other recipients. Use the Cc option only if someone needs to know about the information in the e-mail but does not need to respond. Use the Bcc for the same reason with someone whose address should not appear in the delivered e-mail message.

Junk Mail (Spam)

Just as you might receive unsolicited advertisements, flyers, and catalogs in your regular mail, you most likely receive junk e-mail, also called *spam*, in your e-mail inbox. This type of message might include advertisements, fraudulent schemes, pornography, or other illegitimate offers. This method of advertising is very inexpensive, and it is not uncommon for most people to receive numerous spam messages.

To help prevent spam:

- Use caution in giving out your e-mail address. Do not publish it online, on a Web site, in newsgroups, or in other public areas on the Internet.
- Check a Web site's privacy statement before you provide your e-mail address. Verify that it does not permit the sharing of your e-mail address with other companies.
- Never reply to a junk e-mail message. Once you reply, the sender will know that your e-mail address is valid. More than likely, you will receive even more junk e-mail, and the sender may also sell your e-mail address to others.
- Microsoft Outlook includes a junk e-mail filter that is turned on by default. The protection level is set to low and identifies only the more obvious junk e-mail messages. The program analyzes the content of your messages and moves suspicious messages to a special junk e-mail folder. You can then view and delete them. If a junk e-mail message is received in your inbox, you can specify that future messages from the sender are moved automatically to the junk e-mail folder.


VOCABULARY

netiquette

spam

In the following Step-by-Step exercise, you examine junk e-mail options in Microsoft Outlook.

Step-by-Step 27.4

1. Click the **Start** button  on the taskbar, point to *All Programs*, click **Microsoft Office**, and then click **Microsoft Outlook 2010**.
2. Click the **Junk** button in the Delete group on the Home tab, and then click **Junk E-mail Options** to display the Junk E-mail Options dialog box, shown in **Figure 27-11**.

Review the options
on these tabs

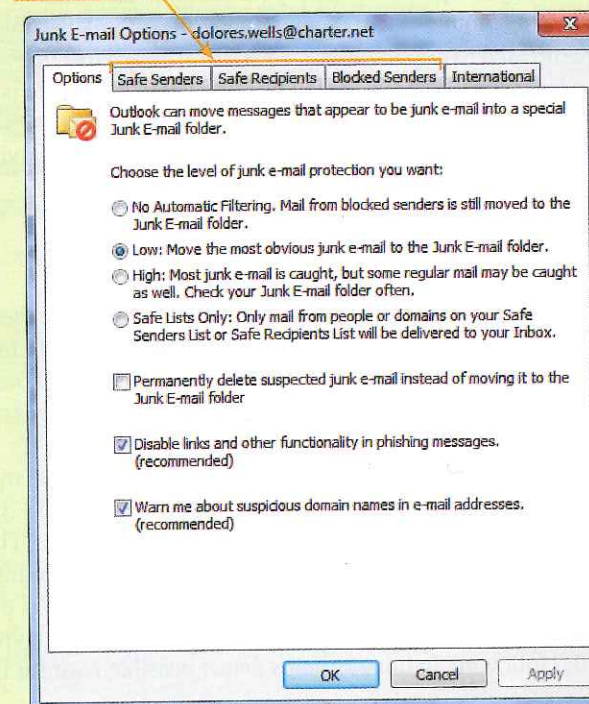


FIGURE 27-11
Junk E-mail Options dialog box

3. Review the settings on the Options tab, and then click the **Safe Senders**, **Safe Recipients**, and **Blocked Senders** tabs.
4. Use your word-processing program and write a summary of the information contained on each of the four tabs (Options, Safe Senders, Safe Recipients, and Blocked Senders). Submit the summary document to your instructor.
5. Close all open windows.

VOCABULARY

fraud
phishing
pyramid scheme
hoax
urban legend

Fraud, Hoaxes, and Other False Information

Electronic *fraud*, such as e-mail fraud, is a computer crime that involves the manipulation of a computer or computer data to dishonestly obtain money, property, information, or other things of value, or to cause loss. The U.S. Secret Service reports that hundreds of millions of dollars are lost annually due to fraudulent activities.

E-Mail Fraud

E-mail messages are often used for fraudulent activities. Beware of messages you receive from e-mail addresses or senders you do not recognize. In many instances, the messages are well-written and appear to be legitimate. Typically, the messages request money for one reason or another. Unless you know the reason to be true, do not send a response to a message that requests money or personal information. Common fraudulent types of messages include *phishing*, which are personal information scams. This type of message appears to come from a legitimate source, such as your bank. The message asks that you update or verify your personal information. However, the information is used to commit identity theft. If you click a link in a phishing e-mail message, you are directed to a spoofed site, one that disguises its URL so it looks like you are visiting a legitimate Web site. Being misdirected to a fake site is called spoofing. *Pyramid schemes* are an illicit business model where profits are based on the investor's ability to recruit other people who are enrolled to make payments to their recruiters. Generally, neither a product nor a service is delivered.

Hoaxes

A *hoax* is an attempt to deceive an audience into believing that something false is real. Sometimes a hoax takes the form of a practical joke with a humorous intent; other times, it is an attempt to defraud and mislead. Many e-mail hoaxes appear to be warnings about potential viruses, a type of malware, but actually contain a virus themselves.

Perhaps one of the most well-known media hoaxes—one that many consider the single greatest of all time—occurred on Halloween eve in 1938. Orson Welles shocked the nation with his Mercury Theater radio broadcast titled “The War of the Worlds.” Despite repeated announcements before and during the program, many listeners believed that invaders from Mars were attacking the world.

It is not always easy to spot an e-mail or chain letter containing a virus, but looking for some of the following hallmarks helps detect possible harmful files:

- The e-mail is a warning message about a virus.
- The message might be very wordy, contain all capital letters, or include dozens of exclamation marks.
- The message urges you to share information with everyone you know.
- The message appears credible because it describes the virus in technical terms.
- The message comes with an attachment, and you do not know who it is from.


If you identify any of these characteristics, it is wise to delete the e-mail immediately. Also, use antivirus software to scan e-mail messages, and keep the software updated.

In the twenty-first century, hoaxes, along with urban legends, myths, and chain letters, grow and flourish through the Internet. *Urban legends* are stories that at one time could have been partially true but have grown from constant retelling into a mythical yarn. Much of this false information is harmless; however, many urban legends are passed along in electronic chain letters, which can have viruses attached to the message. The Web site *liutilities.com* provides articles on computer topics, including virus myths and hoaxes. You visit this site in Step-by-Step 27.5.

ABOVE AND BEYOND

The first known computer crime, electronic embezzlement, was committed in 1958.

Step-by-Step 27.5

1. Click the **Internet Explorer** button  on the taskbar (or start Internet Explorer the way you usually do).
2. Type **www.liutilities.com/articles/computer-virus-myths-hoaxes** in the Address text box, and then press **Enter** to display the liutilities.com Web site, shown in **Figure 27-12**.

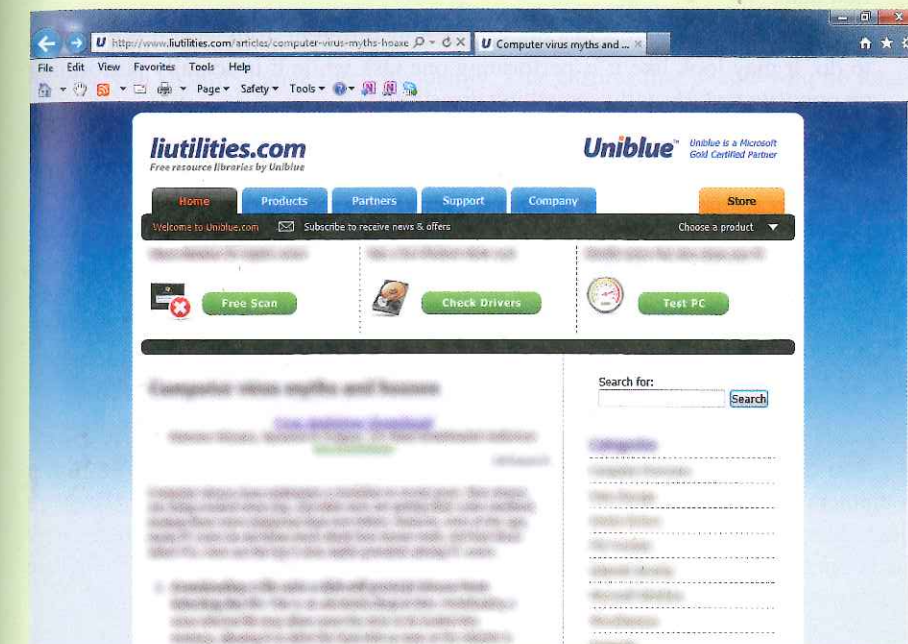


FIGURE 27-12
Computer virus myths and hoaxes article

3. Review the article, and then follow your instructor's directions to either print a copy or write a paragraph summarizing the six myths described on this Web page.
4. Close Internet Explorer.

Protecting Against Viruses and Other Security Risks

In an information-driven world, people and organizations must manage and protect against risks such as viruses, which are spread through electronic communications.

Viruses

A *virus* is a program that has been written, usually by a hacker, to corrupt data on a computer. The virus is attached to a file such as a program file, a document, or an e-mail message, and spreads from one file to another when the program is executed.

VOCABULARY

virus

A virus can cause major damage to a computer's data or it can do something as minor as display messages on your screen. Descriptions of different types of viruses follow:

VOCABULARY

- worm
- time bomb
- logic bomb
- Trojan horse

- A **worm** makes many copies of itself, consuming system resources so that the computer slows down or actually halts tasks. Worms don't have to attach themselves to other files.
- A **time bomb** is a virus that does not cause its damage until a certain date or until the system has been launched a certain number of times.
- A **logic bomb** is a virus triggered by the appearance or disappearance of specified data.
- A **Trojan horse** is a virus that does something different from what it is expected to do. It may look like it is performing one task while it is actually performing an opposite task (usually something disastrous).

To protect your computer against virus damage, try the following methods:

- Use antivirus software. This software should always be running on your computer and should be updated regularly.
- Be careful when opening e-mail attachments. It is a good idea to save attached files to disk before opening them so you can scan them.
- Do not access files copied from USB drives or other media, or those that are downloaded from the Internet without scanning them first.

You can prevent a virus from infecting your computer and spreading to other computers by diligently scanning files that you did not create to make sure they are clean. Many programs have a built-in virus scan feature that is activated when a new file is opened; in other cases, you can use an antivirus program to scan a file before opening it. **Figure 27-13** shows how a virus can spread.

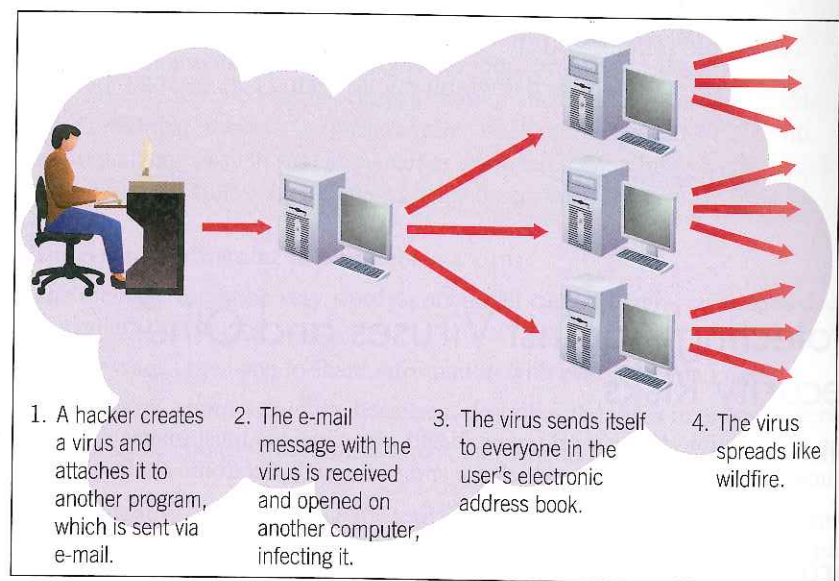


FIGURE 27-13 How a virus can spread

General Security Risks

Computer security can keep hardware, software, and data safe from harm or destruction. Some risks to computers are natural causes, some are accidents, and some are intentional. You cannot always detect that your computer is the object of a crime or intrusion. You should therefore install and use safeguards for each type of risk. It is your responsibility to protect your data.

The best way to protect data is to effectively control access to it. If unauthorized people gain access to data, they may obtain valuable information. Companies often establish password-protected locations on hard drives and networks so that designated users can use certain files but not others. Web sites also require passwords to access accounts or make transactions. For your personal computer, you can set a password to log on to the computer or to specific parts of it. To maintain secure passwords, you should change them frequently. This ensures that people who no longer need access cannot log on.

Other security measures include using the following:

- Electronic identification cards that provide access to designated areas within a building or department. See **Figure 27-14**.



FIGURE 27-14 Using an electronic identification card

- A firewall, which is an integrated security system that prevents unauthorized electronic access to a network computer system while permitting outward communication.
- Antivirus software to protect data on your computer.

Organizations must plan for security before they need it rather than handling breaches in security as they occur. For example, any company that handles sensitive information or needs to protect its data should take the following precautions:

- Institute a selective hiring process that includes careful screening of potential employees. Do not keep employees on who refuse to follow security rules. This measure will prevent internal theft or sabotage.
- Regularly back up data and store it offsite.

QUICK TIP

You can create secure passwords that are easy for you alone to remember. String together the first letter of a line from a song or poem, for example, to create a password such as **IlmhiSF!**, so you only need to remember "I left my heart in San Francisco." Add a punctuation mark at the end. A password like this is difficult for someone to guess.

- Employ biometric security measures, which examine a fingerprint, handprint, voice pattern, or the iris or retina of the eye, as shown in **Figure 27–15**. These images must match the entry that was originally stored in the system for an employee to gain access to a secure area. This method of security is usually employed when high-level security is required.



AP Photo/Ric Field

FIGURE 27–15 Biometric security measures

Another common security concern on the Internet is credit card information. Effective encryption technologies help keep credit card numbers secure, but you can add security by following simple precautions. For example, purchase from Web sites that you know are reputable and trustworthy. Read and understand the company's privacy and consumer-protection policy before you buy. Verify that any credit card information is transmitted in a secured, encrypted mode.



3-2.3.4

Engaging in Professional and Effective Communications

Electronic communications, as previously discussed, are available in a variety of formats—e-mail, instant messaging, teleconferencing, social networks, and so on. The level of formality and informality is based on the type of communication.

Statistics indicate that e-mail is the most popular of all Internet activities and that more than 90 percent of adult Internet users send or read e-mail. When used in the workplace for business communications, certain rules of etiquette and formality should be applied similar to those used in other business communications. The following list discusses elements of professionalism as applied to electronic communications:

- The content, tone, and format of the message should be appropriate for its audience. Writing for a business or professional audience is different from writing for a personal or social audience. When composing a business message, assume that your audience has limited time and most likely will skim the contents to find the main idea. The content should be clear and the message should not contain spelling or other errors.

- Personal and social messages can be less formal. They should, however, be checked for spelling and punctuation errors. The purpose should be clearly stated. Avoid using sarcasm or too much humor unless the message is to someone you know very well.
- Select a communication method that suits the purpose of the message. For example, is the purpose of a message to invite someone to dinner or to submit a proposal? As with knowing the audience, knowing the purpose helps you craft the content, tone, and format. Instant messaging should be short and to the point. An e-mail message can contain more information.
- Respond to messages quickly. The type of message often dictates response time. For example, if a customer needs immediate assistance or has a complaint, you should reply within 30 minutes to 2–3 hours. If a student needs assistance on how to upload an assignment for his online class, the response time should be within 5–10 hours. Other nonemergency responses should be made within 24 hours.
- Messages should be concise and to the point. Ideally, the recipient should not have to scroll past one page to read the message. If the message is longer than that, consider moving the message content into a document and attaching it to the message.
- Include one subject per e-mail message. The subject line should describe the message content using short, direct text.
- The purpose of the message and its recipients should determine the level of formality. Adding elements such as emoticons, abbreviations, jokes, and other informal elements are appropriate for some audiences but not others. Business correspondence, for example, should be more formal than social correspondence. Even social correspondence can range from formal to informal.
- Repeating information and including material from previous e-mail messages is another consideration. Verify that you are not duplicating something that was sent previously. Also check that the recipient was not previously sent a copy of any attachments that you are adding.

Using Other E-Mail Options

In addition to the e-mail options discussed previously, other alternatives are available. The ability to send and receive e-mail attachments and other supplemental information is of great benefit and often a timesaver, though it does introduce a security risk.

- Recall that an attachment is a file that is sent along with an e-mail message. More than one file can be attached to the same message, and the files do not need to be of the same type. When recipients receive the message, they can open or save the attached file.
- Most e-mail services have a limit on the size of the message, including attachments. The size, based on the server settings, can be anywhere from 30 MB up to 2 GB or more. Some services, however, now support delivery of files of unlimited size.
- Some e-mail services set security on certain types of files, such as executable programs (.exe extensions), so they are rejected. In other instances, company security policies for e-mail might reject all attachments.

QUICK TIP

Another often-used rule of netiquette is to not use all upper-case letters in a message. This is considered the equivalent of shouting.



3-2.3.5

QUICK TIP

Most e-mail programs let you assign a priority to a message, such as high or low. For example, when you are creating a message in Microsoft Outlook, you can click the High Importance button or the Low Importance button to indicate the message priority to your recipients. High priority messages appear in the Inbox with a red exclamation mark.

- When creating an e-mail, you can add a hyperlink to the message rather than attaching a file. With this format, the recipient can click the link rather than opening an attachment. There are two ways to add hyperlinks to an e-mail message. One way is to type the Web site address. Most e-mail programs recognize the text as a Web site address and convert it to a hyperlink. The second method is to attach the Web site address to a word or a phrase in the message. This makes the word or phrase the hyperlinked text. You can embed hyperlinks only in e-mail messages created in the HTML format. The recipient of the message must also use a program that can display hyperlinks.
- Some e-mail readers cannot display embedded graphics or animation. Generally, this happens if the e-mail program reader is set to text only.
- Viruses and other similar threats can be delivered as e-mail attachments. Protecting a system requires a number of security tools. Nearly all e-mail programs provide security settings, phishing filters, and anti-spam tools. Other protective tools and procedures include firewalls, encryption, antivirus tools, spam filters, and user education (see Figure 27-16).

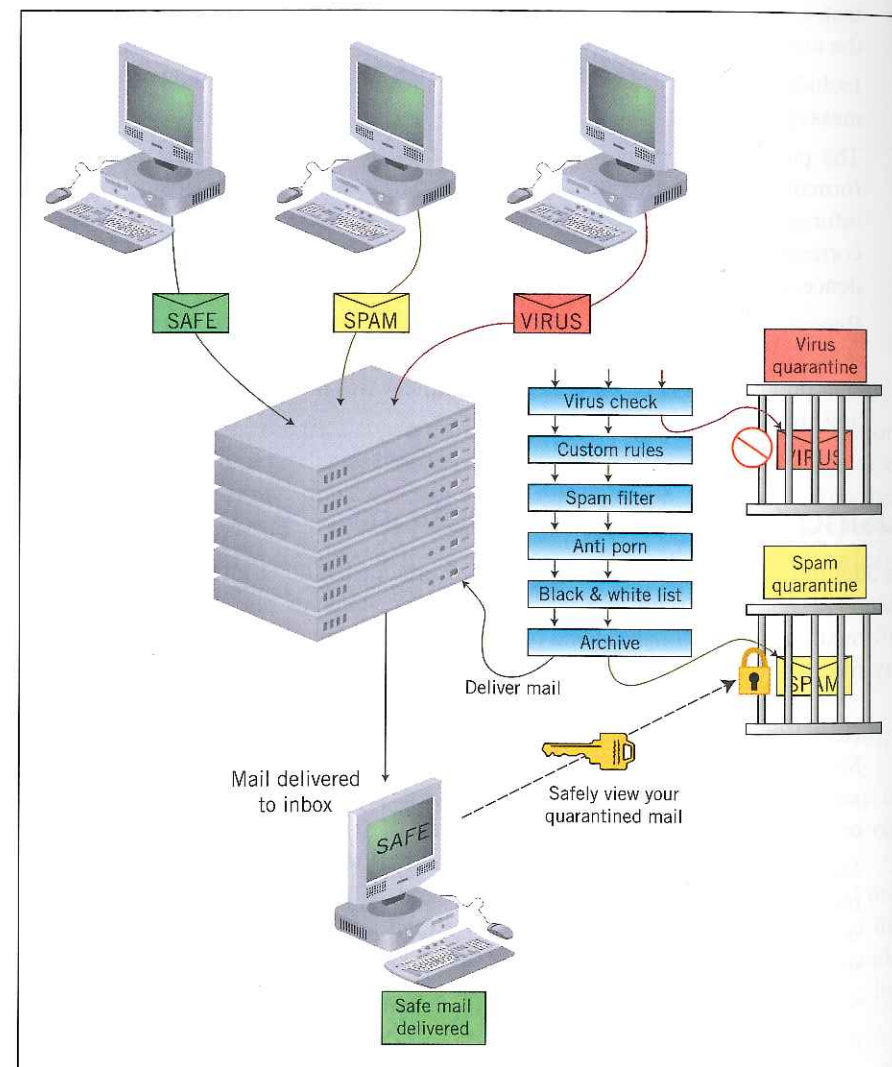


FIGURE 27-16 Controlling viruses and spam



Controlling Unsolicited E-Mail

E-mail filtering allows you to define rules to manage incoming e-mail. Filters automatically sort your incoming messages according to the rules you set up. You can filter your incoming e-mail messages to do the following:

- Sort incoming messages into folders
- Automatically tag messages
- Forward messages
- Discard messages

For example, you could define a filter rule to identify mail coming from your immediate supervisor and move it to a folder called "From My Boss" or to automatically move messages from a specific address to the Deleted Items folder.

Filtering Mail by Mail Servers

E-mail spam, or junk mail, was discussed earlier in this lesson. Spam has plagued users since the beginning of the Internet. Spam is an inexpensive way for people to market products and services, but a recent study by Nucleus Research, Inc., estimates that spam costs U.S. businesses more than \$71 billion per year in lost productivity.

Although some spam still will get through, you can use a number of techniques to reduce the amount that finds its way to your inbox. In the past few years, the amount of spam received by most users has decreased because of *filtering*, which processes some e-mail but not others. E-mail servers are the computers that send and receive e-mail. They are usually set up to catch obvious spam and remove it before it is transferred to users. See Figure 27-17. Administrators can also define rules on the e-mail server to filter e-mail that might contain viruses or offensive language, for example.

VOCABULARY

filtering

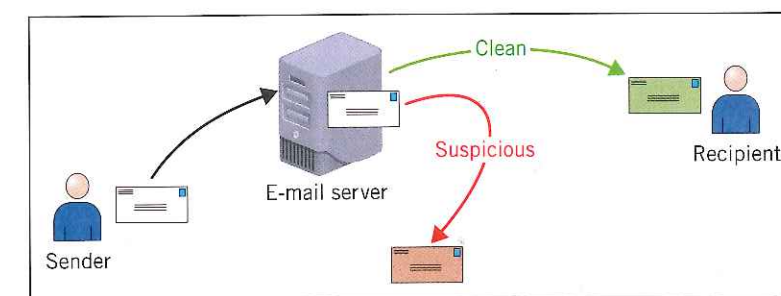


FIGURE 27-17 Filtering e-mail

Another preventive measure is to avoid posting your e-mail address in a public place. Marketers use database matching to obtain e-mail addresses. For example, the marketer has a database that contains names, addresses, and telephone numbers. They pay to have their database matched against another database that contains e-mail addresses to gather entries that include names, address, phone numbers, and e-mail addresses.



Following Guidelines for Electronic Communication

Most companies, institutions, government agencies, and other businesses and groups have guidelines for the use of electronic communications. The following is a checklist of guidelines, as discussed throughout this lesson:

- Check all incoming e-mail messages and attachments for viruses. It is critical that you use an antivirus program and update it on a regular basis.
- Review e-mail, instant messages, and other electronic communications prior to sending to make sure your communication is appropriate for its audience.
- Review and apply the rules of netiquette, company or school policies, cultural issues, and other guidelines.
- Verify that your e-mail program includes a feature that encrypts messages. Encrypting an e-mail message requires that you obtain a digital signature from a commercial digital ID group such as GlobalSign or VeriSign.
- Back up and archive correspondence on a regular basis.
- Understand the sensitive nature of data and of the rules related to sending data electronically.
- Be aware that electronic communications can leave an “electronic trail.” Messages left on public sites such as blogs, message boards, or posts to social networking sites can be publicly and even permanently accessible.
- When using computers at schools or other organizations for electronic communications, follow the organization’s guidelines for electronic communications.

ETHICS IN TECHNOLOGY

Physical Security

E-mail and attachments often contain information valuable to people and organizations, such as records of decisions, internal documents, and upcoming plans. Users should take steps to protect this information, including securing computer hardware and other equipment. It is generally fairly easy for an unauthorized person to access systems by removing them from a valid user’s desk.

Computers and their devices should be kept in a secure place. Only a limited number of people should have access. A list of authorized users should be kept up to date. Some organizations have security guards or equipment to monitor computer rooms and control entry.

Remember that limited access means less opportunity for computer equipment or data to be stolen. Alternative methods for getting into a computer room should not be available. This includes hidden spare keys in an unsecured place.

Some organizations have taken computer safety a step further by securing equipment physically to desks and tables. This might seem like overkill, but it does help them protect their investment and their data.

SUMMARY

In this lesson, you learned:

- Teleconferencing uses a telecommunications system to serve groups, permitting the live exchange and sharing of information between two or more people.
- Syndication (Really Simple Syndication or RSS), also known as Rich Site Summary and RDF Summary, are formats originally developed to facilitate the syndication of news articles.
- Electronic communication offers many advantages over other types of communication. For example, the communication is not restricted to a specific place and time. Secondly, in most instances, it uses text and graphics rather than voice. These tools also provide for different types of correspondence such as one to one, one to many, or many to many.
- Typical communication problems include failing to connect to the Internet or to your e-mail server. Being unable to download or view an e-mail attachment could be due to the size of the attachment, a virus in the message, the sender, or the type of e-mail.
- Communications netiquette, a combination of the words *net* and *etiquette*, refers to good manners and proper behaviors when communicating through electronic media.
- Fraud is a computer crime that involves manipulating a computer or computer data to dishonestly obtain money, property, or other things of value or to cause loss.
- A virus is a program that has been written, usually by a hacker, to corrupt data on a computer. The virus is attached to a file and then spreads from one file to another once the program is started.
- Computer security can keep hardware, software, and data safe from harm or destruction. The best way to protect data is to effectively control access to it.

LESSON REVIEW

TRUE / FALSE

Circle T if the statement is true or F if the statement is false.

- T F 1. Electronic communication offers many advantages over other types of communication.
- T F 2. If you cannot download or view an e-mail attachment, the size of the attachment could be the problem.
- T F 3. Personal and social messages should be formal.
- T F 4. A time bomb is a virus that does not cause any damage.
- T F 5. A hoax is an attempt to deceive an audience into believing that something false is real.

MULTIPLE CHOICE

Select the best response for the following statements:

- It is not always easy to spot an e-mail or chain letter containing a(n) _____.
 - virus
 - picture
 - instant message
 - paragraph of text
- Phishing is a type of e-mail _____.
 - listing
 - controller
 - fraud
 - hardware
- Most companies, institutions, government agencies, and other businesses and groups have guidelines for the use of electronic _____.
 - worms
 - filtering
 - communications
 - policies
- Viruses and other similar threats can be delivered as e-mail _____.
 - attachments
 - spam
 - servers
 - hyperlinks
- A(n) _____ can corrupt data.
 - RDF Summary
 - urban legend
 - attachment
 - virus

FILL IN THE BLANK

Complete the following sentences by writing the correct word or words in the blanks provided:

- _____ refers to good manners and proper behaviors when communicating through electronic media.
- E-mail delivery _____ refers to a returned or "bounced" e-mail.
- For e-mail messages, the _____ format provides formatting options such as multiple fonts, text, colored headings, graphics, and links to Web sites.
- An e-mail message sent from one person to a group is an example of one-to-_____ communication.
- _____ uses a telecommunications system to serve groups.

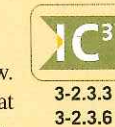
PROJECTS

PROJECT 27-1



Wikipedia.org describes e-mail filtering as the "processing of e-mail to organize it according to specified criteria." Access the Web page at http://en.wikipedia.org/wiki/E-mail_filtering and review the information. Then use your word-processing program to provide an overview of this article. As part of the overview, explain why people use e-mail filtering (motivation), how they use e-mail filtering (methods), and how they can configure it (customization).

PROJECT 27-3



Junk mail, also known as spam, has continued to grow. The Federal Trade Commission's Web site, located at www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt063.shtm, contains information on how to opt out of receiving unsolicited mail. Access this Web page and review the information it contains. Then describe the process you would use to opt out of receiving unsolicited e-mail. Describe what process someone could use if they did not have Internet access.

CRITICAL THINKING

Several free e-mail services are available online. The Web site located at http://email.about.com/od/free-mailreviews/tp/free_e-mail.htm provides an overview of the top 16 free e-mail services. Access this site and use your word-processing program to answer the following:

- How many services are listed? (Hint: The Web site information is contained on two pages; don't forget to click the Next link.)

PROJECT 27-2



Using the Internet or other resources, research the history of instant messaging. Then answer the following questions:

- In what year did instant messaging become popular?
- What is a chat room and how does it work?
- What is ICQ as related to instant messaging?
- When did AOL adopt instant messaging?
- How does instant messaging software know when one of your contacts is online?
- Name three popular instant messaging providers.
- Is instant messaging a secure technology?

TEAMWORK PROJECT



Some countries have laws against spam. Your Internet service provider may try to block spam before it reaches your mailbox. However, you may still be inconvenienced by junk e-mail.

Working with a partner, research spam to learn more about what it is used for, how marketers get addresses, how effective spam is, and ways you can stop spam. You and your teammate should each select one of the two positions—pro spam (how effective it is and what it is meant to do) or against spam (it is a nuisance or problem that you want to stop before it reaches your e-mail inbox). Write a brief summary of your findings and compare them with your partner. At the end of your report, answer the following questions with your partner: Is spam ever useful? Should there be laws to restrict spam? Do you think you can block all spam from reaching your inbox?

- Assume you are looking for a free e-mail service. Answer the following questions:

- Which service would you select? Why?
- Which service would be your second choice? Why?
- Which services use the Google approach to e-mail?
- Which services offer POP or IMAP access, and which allow you to download messages to any e-mail program?

Select three of the services that you consider less popular. Review each of the three services you selected and list the pros and cons for each service.

ONLINE DISCOVERY

Google Docs is a Web site where you can create and share your work online. Complete the following:

1. In a Web browser, visit the Google home page at *www.google.com*.
2. Click the more link in the bar at the top of the Web page, and then click Documents.
3. Read the description of Google Docs, and then create an account and sign in. If you already have an account, sign in.
4. Create a Google document that explains what you can do with Google Docs. Enter your name in the document, and then save the document.

5. Click the Share button on the Google Docs toolbar to open the Sharing settings dialog box. Click the Add people text box, and then enter the e-mail address of your instructor.




6. Click the Paste the item itself into the e-mail check box, make sure the Notify people via email box is checked, and then click the Share & save button.
7. Click the Done button, and then close the browser.

JOB SKILLS

Many work projects in all fields involve collaborating with others. Even if you work in the same location, this collaboration often uses a form of electronic communication. On your own or working with

a partner, brainstorm the types of skills and abilities someone needs to collaborate effectively. Select the top three skills and list them in a word-processing document. Briefly describe each skill.



 Estimated Time:
1 hour

LESSON 28

Using the Internet and the World Wide Web

OBJECTIVES

Upon completion of this lesson, you should be able to:

- Explore the Internet and the Web.
- Define Internet terminology.
- Connect to the Internet.
- Understand browser basics.
- Select Web browser settings.
- Identify browser issues.

DATA FILES

You do not need data files to complete this lesson.

WORDS TO KNOW

ActiveX
 cookie
 digital certificate
 domain
 File Transfer Protocol (FTP)
 geographic imaging
 home page
 Hypertext Markup Language (HTML)
 Hypertext Transfer Protocol (HTTP)
 Internet Protocol (IP) address
 Internet service provider (ISP)
 podcast
 portal
 Secure Sockets Layer (SSL)
 social networking site
 Uniform Resource Locator (URL)
 Web 2.0
 Web app
 Web cache
 wiki