Estimated Time:
1 hour

LESSON 3

Computer Protection

OBJECTIVES

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

- Protect computer hardware from theft and damage.
- Safeguard data.
- Identify environmental factors that can damage computers.
- Protect computers from power loss and fluctuation.
- Identify common computer hardware problems.

DATA FILES

You do not need data files to complete this lesson.

WORDS TO KNOW

backup
data theft
driver
encryption
humidity
ping
power spikes
surge suppressor
uninterruptible power supply (UPS)

Computers enhance our lives. They make our daily tasks much easier, our work more efficient, our learning more interesting and convenient, and even our game playing more exciting. As computers continue to play a central role in business and our personal lives, protecting computer systems and the information they hold has become increasingly important. This lesson examines how to protect computers and their data from typical dangers.

IC³ 1-1.2.1

Protecting Computer Hardware from Theft and Damage

Theft of and damage to computer equipment are serious problems that many organizations face. In addition to the capital loss of equipment and the related down time until it is replaced, losing sensitive and confidential information through theft or damage could have long-term consequences. One safeguard you can use to prevent theft in the workplace is to physically secure equipment, especially items such as notebook computers, handheld devices, cell phones, and other transportable devices. See **Figure 3–1**.

FIGURE 3–1 Preventing computer theft

ABOVE AND BEYOND

Another type of theft that is sometimes overlooked involves employees accessing a company's computer for personal use. Theft of computer time is a crime committed regularly on the job. Some companies use spyware to monitor employee personal use, though this practice has been challenged in court.

In addition, you can apply the following safeguards to help protect computer hardware from theft:

- If the equipment is located within an office or open lab, use security locks and/or tabs to secure the equipment to the desk or other furniture.
- Attach an alarm that will sound if the equipment is moved from its designated location.
- Mark all equipment with an identification tag or symbol that can be traced easily.
- Insure the equipment. Some insurance policies cover loss due to accidental damage, theft, vandalism, power surges, lightning strike, flood, fire, earthquake, and other natural disasters.
- Use a designated schedule to back up data to a separate system.

Safeguarding Data

In most instances, hardware can be replaced when it is stolen or damaged. Data, on the other hand, is a critical component of most businesses and is not easily replaced. Many companies protect their data with security devices such as firewalls and intrusion-detection devices. Data thieves, however, also steal laptops and servers. They then use the remote software on the stolen system to connect to the organization's network and bypass the company's security measures. In other instances, ***data theft*** can occur when older systems are discarded and the data is not completely deleted. The risk and severity of data theft is increasing due to four predominant factors:

VOCABULARY
data theft
encryption
backup

- The value of data stored on computers
- Massive amounts of confidential and private data being stored
- Increased use of laptops and other mobile devices outside of a secure network
- Increased proficiency of data hackers and thieves

Many businesses and organizations use data encryption to protect their data. ***Encryption*** is a secure process for keeping confidential information private. The data is scrambled mathematically with a password or a password key. The encryption process makes the data unreadable until it is decrypted.

Data Backup

Even saved data can be lost or corrupted by equipment failure, software viruses, hackers, fire or water damage, or power irregularities. Because data is so valuable, you must back up important files regularly. To back up files, you save them to removable disks or some other independent storage device that you can use to restore data in case the primary system becomes inaccessible. A hard disk crash (or failure) can result in a catastrophic loss of data if it occurs on a critical system and the files have not been backed up properly.

Backup procedures should place a priority on files that would be difficult or impossible to replace or reconstruct if they were lost, such as a company's financial statements, important projects, and works in progress. Large organizations have secure backup procedures that include a regular schedule for backing up designated files. They store the backup files off site so they will survive intact if the main system is destroyed either by natural disaster or by criminal acts. When flooding is a possibility, it is a good idea to locate computers above the first floor of a building.

ABOVE AND BEYOND

Data backup systems include disk and tape devices that make archive copies of important files and folders. You should back up data to storage media that can be removed and stored in a separate location from your computer.

Identifying Environmental Factors that Can Damage Computers

IC³ 1-1.2.2

Computers require the right balance of physical and environmental conditions to operate properly. As indicated previously, computer equipment and its data are subject to various types of hazards. These hazards include theft of hardware and data as well as damage caused by improper use. Environmental factors such as temperature, humidity, and electrical fields also can contribute to hardware and software damage. Organizations can prevent many of these conditions through proper planning and by providing employees with appropriate training on how to use and safeguard the equipment. As an employee, you should know how to protect computers from environmental risks.

The following sections describe environmental factors that are detrimental to computers and how you can control and contain some of these problems.

Temperature

Environmental conditions in a computer room or data center are critical to ensuring that a computer system runs properly and reliably and remains accessible to users. A temperature range of 68 to 75 degrees is optimal for system reliability. The general consensus is that you should not operate computer equipment in a room where the temperature exceeds 85 degrees. A separate thermostat can monitor temperature and humidity levels in a computer room (see **Figure 3–2**).

Courtesy of Sensatronics

FIGURE 3–2 Temperature control

Humidity

VOCABULARY
humidity

A high level of ***humidity*** can cause computers to short circuit, resulting in the loss of data and damage to hardware. Excessive humidity also can cause components to rust. For example, taking a cold notebook computer from an air-conditioned office into an automobile on a sunny day could create a thin film of condensation covering the entire interior of the laptop. Over time, the condensation can cause hardware problems. Consider the following humidity factors to protect your data and computers:

- For optimal performance, the relative humidity of the computer room should be above 20 percent and below the dew point (which depends on the ambient room temperature).
- Environments that require high reliability should have a humidity alarm that rings when the humidity is out of an acceptable range.
- Some equipment has special humidity restrictions. Generally this information is contained in the equipment manual.

Water Damage

Most computer centers contain some type of sprinkler system. If water sprinklers are activated, newer models of computers most likely will not be damaged, provided that the computer's power is turned off before the water starts to flow. Modern computer systems contain a cut-off device that is triggered if the sprinklers turn on. If the computer does suffer water damage, make sure it is completely dried out before you restore the power. Storage devices and printouts, however, can be damaged or destroyed by water. Other types of water damage may occur from flooding and broken pipes.

Magnetic Fields and Static Electricity

Magnetic fields and static electricity exist wherever electrical current flows. A single spark from static electricity can damage the internal electronics of a computer. Computer technicians have grounding protection on the floor and use a grounded strap on their wrists when they service computers. You should do the same if you need to open a computer case, such as to install a component. Grounding prevents damaging a computer with a static electrical spark. Computer rooms should also have tile floors and antistatic carpet to reduce static electricity.

Data on a hard drive is stored in small magnetic dots on the disk and is therefore sensitive to magnetic fields. To prevent losing data, do not store magnets directly on a computer.

Physical Damage

Most electronic devices can suffer damage from physical contact with other objects. You can prevent physical damage to desktop computers by arranging the equipment so it is stable on a desk or floor and cannot fall or be knocked over. Notebook computers are generally more costly than desktops with similar storage and processing capabilities. They are also more prone to physical wear and tear because they are portable. To help protect the computer and limit the extent of the damage, most portable systems are insulated with shock absorbing material. This reduces damage to internal components if the computer is dropped or subjected to impact with another object. You should take additional steps to prevent physical damage to portable computers by transporting devices with care, such as in padded cases.

Poor Maintenance

One of the best ways to cut down on computer repair is through preventive maintenance. Create a monthly maintenance schedule and follow it regularly to clean equipment and perform tasks to keep computer devices in good working order. For example, if you use a mechanical mouse, you need to remove the ball and clean it periodically. Poorly maintained printers can print pages that are smudged or otherwise difficult to read. Cable connections can be weakened by dust, preventing normal communication with a computer. Damaged cables in general can prevent peripheral devices from communicating with the computer. Lesson 4 covers computer maintenance in detail.

1-1.2.3

Protecting Computers from Power Loss and Fluctuation

One ever-present threat to a computer system is an electrical power failure. A computer needs electricity to operate in general and to store data in particular. An unexpected power outage, for example, can wipe out any data that has not been properly saved.

To safeguard computer systems against power outages, secure electric cords so that they cannot be disconnected accidentally. You also need to protect computers and other electronic devices from ***power spikes***, which are short, fast transfers of electrical voltage, current, or energy that can damage computer hardware and software. ***Surge suppressors*** (see **Figure 3–3**) plug into electric outlets and can protect against power spikes. Some lower end brands of surge suppressors wear out over time, however, and need to be monitored and replaced as necessary.

VOCABULARY

power spike

surge suppressor

uninterruptible power supply (UPS)

Courtesy of Monster Cable Products, Inc.

FIGURE 3–3 Surge suppressor

WARNING

Do not plug a laser printer into a UPS. Laser printers need a lot of power when they start a print job, and can damage a UPS or even components connected to it. Instead, plug your laser printer directly into a wall outlet or a surge suppressor.

One option for preventing data loss due to power outages is to install an ***uninterruptible power supply (UPS)***. These electrical devices range from basic kits to more sophisticated models designed for desktop computers and networks. The UPS shown in **Figure 3–4** is designed for a single computer. A UPS contains a battery that temporarily provides power if the normal current is interrupted, and generally keeps a computer running for several minutes following a power outage. This additional time provides an opportunity for you to save data and to properly shut down the computer. Most UPS systems now also include a software component that shuts down the computer automatically. The two basic types of UPS systems are standby power systems (SPSs) and online UPS systems. An SPS monitors the electrical power and switches to battery power if it detects a power problem. Depending on the computer system, the switch to battery power can take less than one second. An online UPS constantly provides power, even when the system is using electrical power. In either case, you avoid momentary power lapses.

Courtesy of APC by Schneider Electric

FIGURE 3–4 Uninterruptible power supply

WARNING

If you travel outside of the United States with your computer, you might need a transformer to convert from one electrical system to another. Otherwise, you could seriously damage the electronics in your computer.

Identifying Common Computer Hardware Problems

1-1.2.4

Computer equipment and stored data are subject to computer hardware issues. Some common problems are a failed or "crashed" hard drive, damaged media, printer and monitor problems, loss of network or Internet connectivity, and general failure such as newly installed hardware not working. You can resolve or prevent many of these conditions by proper planning and by receiving appropriate training on how to use and protect the equipment. You can solve many problems on your own, while other problems may require the assistance of a professional.

The following sections provide an overview of common hardware problems and suggestions on how to troubleshoot and resolve them.

Crashed Hard Drive

Crashed hard drives generally are caused by software corruption or hardware defects. Hard drives can stop working if they become overheated, are dropped or shaken, become worn out, or are infected with a virus. Some suggestions to evaluate the condition of the drive are as follows:

- If a boot disk is available, use the disk to determine if the drive is readable. If so, back up the data and reformat the original disk.
- Several software solutions are available; these diagnostic and data recovery programs can locate and recover bad sectors.
- Use a data recovery service.

Damaged Media

Hard disks and other media eventually fail. Hard disks are mechanical devices with moving parts, and inevitably wear out. CDs and DVDs can be scratched, warped, or physically damaged in other ways. Tapes can be harmed by electromagnetic fields. Flash drives can also suffer physical damage, such as from unsafe removal, dust, lint, sun exposure, shock, or force.

Many people assume that information stored on damaged media, such as disks, tapes, or CDs, is unrecoverable. In many instances, however, you can recover the data. The first step is to locate the hardware and damaged media and move it to a secure environment. Secondly, inspect or test the media to determine what type and how much damage has occurred.

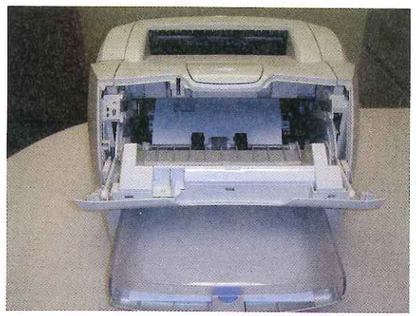
The type of damage determines the type of recovery method to use. If the media was damaged by water, do not restart the computer. This could cause a short if even small amounts of water are still in the computer. If the media is wet, do not dry it. Instead, place it in an airtight plastic bag to keep the media wet. If media such as hard disks get wet and then dry out, contaminants remain on the disks. The contaminants degrade the disk, causing it to lose data. If the media was damaged by fire and is still inside a melted computer case, leave it in the case if water or other elements were used to control the fire. The case should be opened by a professional. If the computer was dropped or otherwise physically harmed in some way, do not restart the computer. The read/write heads can be damaged or out of alignment.

Another option is to locate a disaster data recovery company with the knowledge, skills, and equipment necessary to recover data from the computer.

Printer Problems

Printer problems are a frequent problem. Generally, these problems are easily fixed.

Paper jams stop printers from printing a complete file when paper becomes trapped in the printer. Using the wrong type of paper can cause a printer jam, as can wrinkled or torn paper. If the rollers that feed the paper are worn or dirty, they might turn slowly or unevenly and cause a jam. When eliminating a paper jam, always pull the paper in the direction of the paper path. Pulling the paper backward can damage the printer (see **Figure 3–5**).



Courtesy of CLAS Computer Support Group/University of Connecticut

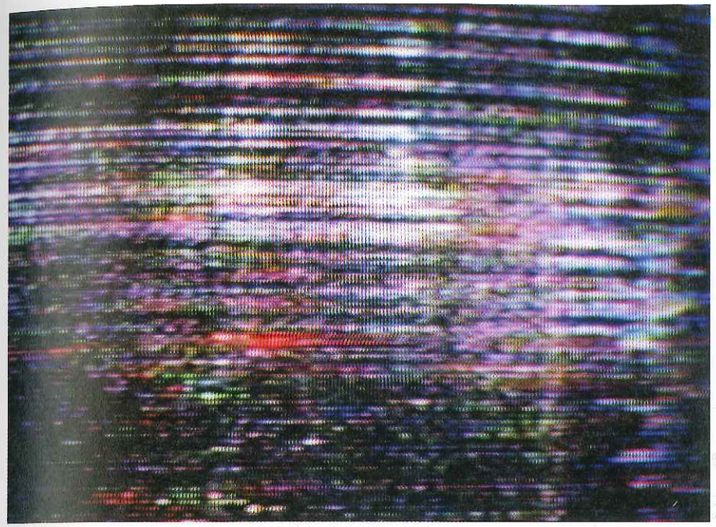
FIGURE 3–5 Paper jam

If ink or toner comes off the paper when touched, look for one of three possible causes. The printer's fuser assembly might be damaged and need to be replaced; the toner cartridge could be defective and need to be replaced; or some toner may have spilled into the printer. If toner has spilled, you need to clean it out of the printer with a dry cloth.

If the printed image is faded, this could indicate one of three conditions: the toner is low, the print density is set too low, or economy mode printing is turned on.

Display Problems

The hardware for your display consists of two elements: the monitor and the video card. It can be more difficult to determine the source of display problems than printer problems, for example, because more hardware is involved (see **Figure 3–6**).



© dubassy / Shutterstock.com

FIGURE 3–6 Video card problem

Consider the following factors as you troubleshoot a display problem:

- Check that the monitor power cord is plugged in and that the monitor cable is connected to the computer.
- Verify that the monitor is turned on and the display settings are correct.
- Update the video driver. The majority of display problems are caused by incorrect, corrupted, or missing video drivers. (See the following section for the definition of a driver.) You usually can upgrade the video driver when you update the operating system; otherwise, visit the Web site for the video driver manufacturer and look for instructions on updating the video driver.

Inoperable Hardware Devices

When a hardware device such as a printer or monitor does not work, it could be a software problem, an electrical problem, or a mechanical problem. A small program called a ***driver*** instructs the operating system on how to operate specific hardware. As mentioned in the previous section, most display problems are caused by missing or corrupted drivers. Other causes are incorrect installation of the software for the hardware device and hardware failure. Also check the following alternatives:

VOCABULARY
driver

- Check the power cord and verify that it is plugged in.
- Verify that the circuit breaker has not tripped.
- Make sure the electrical plug strip, the UPS, or the surge protector are turned on and working properly.

Loss of Network or Internet Connectivity

Local networks and the Internet provide valuable resources for organizations and individuals. Because people depend on these systems, losing connectivity means they cannot communicate or work effectively. Intermittent connectivity and time-out problems can result in poor network performance.

The following are common causes for connectivity problems:

- The network provider's system is not working properly.
- Network adapters and switch ports do not match.
- The network adapter is incompatible with the motherboard or other hardware components.

Some troubleshooting options are:

- Use the DOS ***ping*** command to test connectivity and isolate hardware problems and any mismatched configurations.
- Verify that other computers on the same network and those plugged into the same switch are also experiencing network connectivity problems.
- If you are using a router, restart the router.
- Check the computer's network card or board and verify it is using appropriate settings as indicated by the manufacturer.
- Try another network cable if you are working on a cabled network.
- If you are using a wireless router within a home, beware of signal interference from other home appliances. Common sources of interference are cordless phones, garage door openers, and microwave ovens. In densely populated areas, a wireless signal from one person's home network may interfere with a neighbor's home network.

VOCABULARY
ping

ABOVE AND BEYOND

Connecting computers to a network or the Internet creates opportunities for unauthorized access from outside the network. Software and hardware devices that safeguard a network and provide security from unauthorized entry are called firewalls.

The following Step-by-Step exercise shows you how to use the ping command.

Step-by-Step 3.1

1. Click the **Start** button on the taskbar, point to *All Programs*, click **Accessories**, and then click **Command Prompt**. The Command Prompt window appears, as shown in **Figure 3–7**.

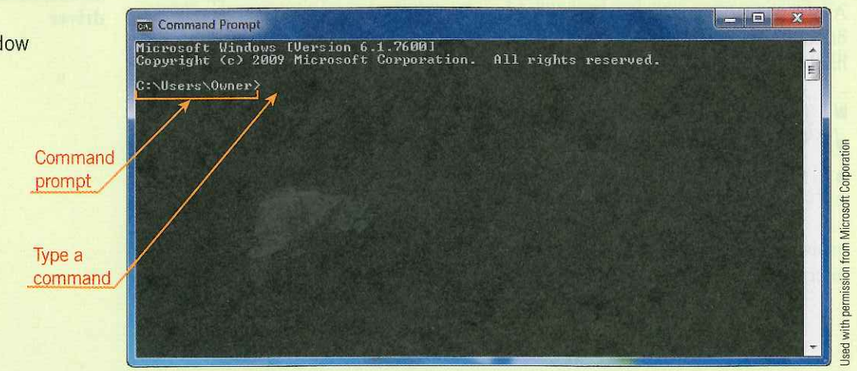


FIGURE 3–7
Command Prompt window

2. At the command prompt (such as C:\), type **ping *Web site address of your school or another Web site address*** and then press the **Enter** key.

   The results include a series of replies, which indicates the connection is working (see **Figure 3–8**). The time shows the speed of the connection. Your specific results will be different from those in **Figure 3–8**.

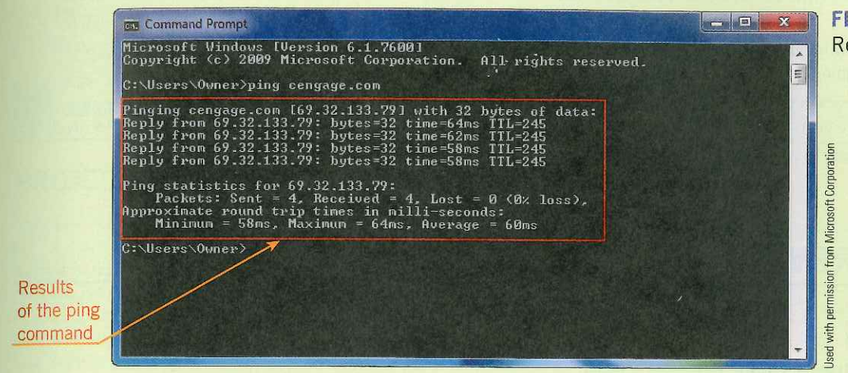


FIGURE 3–8
Replies to ping command

If a "timed out" error instead of a reply is displayed, there is a breakdown somewhere between your computer and the site to which you are attempting to connect.

3. Close the Command Prompt window.

ETHICS IN TECHNOLOGY

The Golden Rule of Computer Ethics

You probably heard the Golden Rule when you were in elementary school: "Do unto others as you would have them do unto you." The Golden Rule applies to computer ethics, too. Would you appreciate it if someone used their computer to cause you financial harm or to ruin your reputation? Of course not, and you should extend the same courtesy to other people. Don't give in to the urge to snoop around in other people's files or interfere with their work by accessing and changing data in files. You wouldn't want someone to mess with your hard work or private files, would you? And if you had spent a few months creating a great computer game, how would you feel if all your friends started passing copies of the game around to all their friends, without even giving you credit for the program, not to mention cheating you out of any potential profit for your work?

If you do write computer programs, think about the social consequences of the programs you write. Don't copy software illegally, and don't take other people's intellectual property and use it as your own. Just because something is posted on the Web does not mean it is "free" for anyone to use. Use your computer in ways that show consideration of and respect for other people, their property, and their resources. Many organizations create a use policy that outlines acceptable behavior for using the organization's computers, including ethical behavior.

SUMMARY

In this lesson, you learned:

- Computer equipment needs to be protected from theft and damage.
- Data should be backed up frequently and consistently to avoid losing important information.
- The right balance of physical and environmental conditions are required for computers to operate properly.
- High humidity, water, and electric/magnetic fields can damage computer equipment.
- Preventive maintenance reduces equipment repair needs.
- Electrical power failure can destroy data and equipment.
- Surge suppressors can protect against power spikes.
- Computer systems are vulnerable to problems such as a crashed hard disk, damaged media, printer and display problems, inoperable hardware devices, and loss of network and Internet connectivity.

LESSON REVIEW

TRUE / FALSE

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

T F **1.** One ever-present threat to a computer system is an electrical power failure.

T F **2.** Power spikes are short, fast transfers of electrical voltage, current, or energy.

T F **3.** Crashed hard drives generally are caused by software corruption or hardware defects.

T F **4.** Data theft is decreasing.

T F **5.** The hardware for your display consists of four elements: the monitor, the video card, the controls, and the UPS key.

MULTIPLE CHOICE

Select the best response for the following statements.

1. Generally, a _____ keeps a computer running for several minutes following a power outage.
   A. driver C. backup
   B. spike D. UPS
2. Computer technicians use grounding protection when they service computers to prevent damage from _____ .
   A. condensation C. power surges
   B. high temperatures D. static electricity
3. _____ can protect against power spikes.
   A. Surge suppressors C. Undamaged media
   B. Video drivers D. Network connections
4. A high level of _____ can cause computers to short circuit.
   A. smoke C. dust
   B. humidity D. alarms
5. Most display problems are caused by missing or corrupted _____ .
   A. surge suppressors C. drivers
   B. network connections D. storage media

FILL IN THE BLANK

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

1. One of the best ways to cut down on computer repair is through _____ .
2. Notebook computers generally are more costly than _____ _____ .
3. _____ should be performed on a regular basis for files that would be difficult or impossible to replace.
4. The _____ on a mechanical mouse should be cleaned periodically.
5. Using the wrong type of paper or using wrinkled or torn paper in a printer can cause a _____ .

PROJECTS

PROJECT 3–1

IC³ 1-1.2.2

Your instructor has assigned you to a team responsible for maintaining the school's computer lab. As you learned in this lesson, static electricity can damage computer components. Using the Internet or other resources, research the types of damage static electricity can cause in computers. Also research how to avoid static electricity when you are working in a computer's case, such as installing an expansion board. Complete the following:

1. Use word-processing software to write a one-page report summarizing your research.
2. Be sure to identify the types of damage static electricity can cause and explain how to avoid static electricity.
3. Submit the document to your instructor as requested.

PROJECT 3–2

Your instructor has asked you to draft an acceptable use policy for the school's computer lab. Complete the following:

1. Write a statement that describes appropriate and inappropriate behavior and acceptable and unacceptable use of equipment.
2. Share your statement with your classmates.

PROJECT 3–3

Computer crimes are responsible for the loss of millions of dollars to businesses and individual computer users. Some crimes result in more loss than others. Complete the following:

1. Use the Internet and other resources to locate information on lost revenue and other costs due to computer crimes in the last year and for two previous years. Some search terms that may be helpful are "computer crimes," "computer crime costs," "hackers," "viruses," "data loss," and "software piracy."
2. Use a spreadsheet program to prepare the data, organizing it according to the type of crime, if necessary. Use formulas that will add the totals of each type of crime, if necessary. Use a chart to compare each year's data.
3. Submit the document to your instructor as requested.

TEAMWORK PROJECT

IC³ 1-1.2.1 1-1.2.2 1-1.2.3 1-1.2.4

Working with one or two partners, research three of the hardware and software issues and problems discussed in this lesson. Find information on the Internet that describes each issue and recommends how to troubleshoot the problem to determine its cause. Create a presentation describing the three problems and possible solutions. Share your team's presentation with your class.

CRITICAL THINKING

Use the Internet and other resources to identify early security measures that were used to protect computers and computer data. Describe how these measures counteracted the intrusions made on the computers. Then, visit the Web sites of some companies that now make computer security devices, such as us.kensington.com and www.computersecurity.com. Describe how and why these devices are different. Write a report of your findings.

ONLINE DISCOVERY

Protecting a home network is just as important as protecting a business or company network. An unsecured home network is as vulnerable to unauthorized use and intrusion as networks within small and large organizations. Security measures help prevent unauthorized users from accessing a home network system. Research this issue and then create a document explaining at least three ways you can protect your home network.

JOB SKILLS

Your supervisor has assigned you responsibility for maintaining the company's computer lab. Assume that the lab has 30 networked computers, a server, 2 color inkjet printers, 3 laser printers, and a scanner. Hardware and software needs to be updated and maintained on a regular schedule. As part of this job, one of your tasks is to create a maintenance schedule for the equipment. Use the Internet for research as necessary. Complete the following:

1. Use a spreadsheet program or word-processing software and create a schedule listing required maintenance.
2. Record how often maintenance is scheduled.
3. Submit the document to your instructor as requested.