Chapter 6

Homeland Security: Computer Protection

Overview

Firewalls? Antivirus software? If these words are unfamiliar to you, then your computer is at risk. In this chapter, you will learn how to use security methods and critical thinking skills to protect your computer from threats posed by hackers and cybercriminals. A discussion of the importance of backing up your computer and updating your security methods regularly is included.

Key Terms

- Computer protection
- Firewall
- Antivirus software
- Updates
- Backing up

Fact!

Did You Know?

In 2012, 40% of households in the United States were affected by viruses, and nearly 24 million households were hit with heavy spam.

Source: *Statistic Brain*

What Is Computer Protection?

In Chapter 5, you learned about different computer threats that you might encounter when you're online. But how do you protect yourself from malware, spam, and phishing? Computer protection means using a combination of methods to safeguard your computer's information from theft and other harmful attacks, such as corrupted files and malware.

Security Methods

In order to protect your personal information and to ensure your computer stays free of malicious software, you should obtain two very important security features: a firewall and antivirus software.

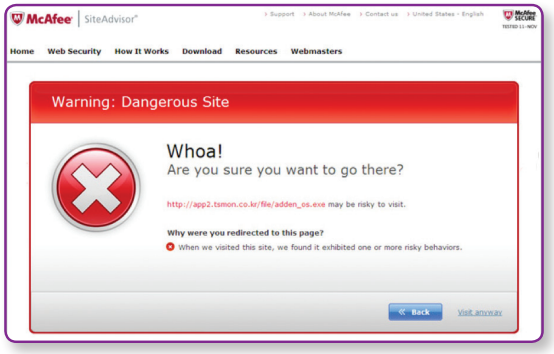
1 Firewalls

Think of a firewall as a guard who protects a gate. It stands between your computer's network and the Internet, helping to protect your computer from unauthorized access to your network. Just like a guard, a firewall decides what to let in and what to keep out. Firewalls make it more difficult for hackers to break down your computer's "gate" with malware and tap into your computer's network. For example, most schools use a firewall to protect students from visiting inappropriate websites and from receiving harmful emails, such as spam.

A good way to understand the function of a firewall is to imagine it as a literal wall that surrounds your computer, protecting it from harm.

2 Antivirus Software

Antivirus software acts like a detective, searching for and removing any malware. It also prevents malware from attaching to your computer in the first place and keeps viruses, worms, and Trojan horses safely away from your files and applications. Many new computers come with antivirus software trials, with the option to purchase the software after the trial date ends.



Antivirus software acts like a detective, searching for and removing any malware.

Shields of Protection

Making sure firewalls and antivirus software are in place is a great first step toward protecting your computer from potentially dangerous threats. But there's even more you can do to ensure your computer is safe from hazardous malware. **To build a strong shield of protection, remember these four Ps: *protect*, *prevent*, *prepare*, and *perceive*.**

1 Protect

Safeguarding your computer means putting into action the best available tools to secure and protect it from malicious attacks. **Listed below are security methods that you should use regularly:**

- **Firewall:** Make sure your computer has a firewall and that it is turned on to keep hackers out of your network.
- **Antivirus software:** Use antivirus software and keep it up to date so that viruses can't corrupt your files or software.
- **Operating system:** Keep your operating system updated, because updates will offer the latest security protection.
- **Downloads:** Be careful what you download, transfer, or save from the Internet. You never know what might be hiding in an attachment from someone you don't know or in software that can be downloaded for free.

Fact!

Did You Know?

In 2000, a 16–year–old resident of Miami, Florida, became the first juvenile to be sentenced for a federal computer crime after hacking into NASA's computer system.

Source: *IT Security*

2 Prevent

Preparing for the worst may seem unnecessary, but by taking a few precautionary steps, you can make certain your computer is well shielded if malware tries to attack:

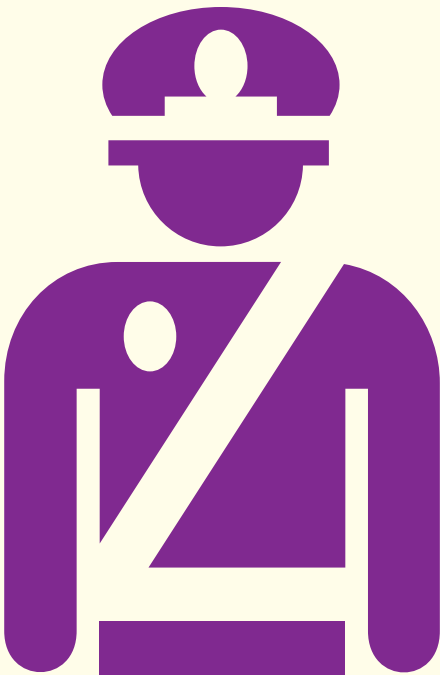
- **Backing up:** Backing up your files means making copies of the data that is on your computer. By duplicating files and important computer software programs, you ensure that you will always have a copy of everything that is on your computer in case it ever becomes infected with malware. There are many different tools available to assist people in backing up their files, from external hard drives to online storage. After you research which back–up method is right for you, you can select one that can protect your important files.
- **Turn off:** This tip is often overlooked, but it is a surefire way to keep hackers at bay. When you are finished using a computer, turn it off. When you turn a computer off, you cut off its connection to potential dangers.

3 Prepare

The best way to protect your computer is to stay informed about the latest computer security methods and to update your security programs regularly:

- **Keep current:** Stay informed about new computer security methods. As technology evolves, so do security methods. If appropriate, add new programs to your list of defenses or replace old programs with new, more effective ones.
- **Watch for updates:** Always check for updates to all security products, software programs, and operating systems. Technology changes quickly, and updates allow you to receive the latest and most thorough protection.
- **Report it:** If you do experience something suspicious, be sure to report it to your Internet service provider. Reporting it not only helps you, but it could also help prevent malware from spreading to other users too.

Remember:
To build a strong shield of protection, use the four Ps—*protect*, *prevent*, *prepare*, and *perceive*.



4 Perceive

Not only does it help to be knowledgeable about the latest computer security programs, but it also pays to use your instincts whenever you encounter uncertain situations:

- **Critical thinking:** We encounter many different things on the Web, from advertisements to social networking sites. In any online situation, using critical thinking skills to assess potential dangers is one way to avoid vulnerability. When you visit sites on the Web, watch for warning signs that might indicate the presence of malware or other computer threats. Think about how certain actions can jeopardize your safety when surfing the Web, and exercise good judgment.
- **Evaluate:** Always evaluate online encounters and use common sense before acting. For example, if you receive an email that looks like it might be part of a phishing scheme, evaluate it carefully before you decide whether to open it. There are many threats lurking on the Web, but by evaluating each encounter we face, we can make thoughtful decisions to protect ourselves.

What Else Can I Do to Protect Myself?

Using common sense and good judgment while surfing the Web is important, but so are our actions. We can accidentally create windows for malware or hackers to get in if we're not careful about protecting our information and accounts. **Ways to minimize risk are listed below:**

- Always **password–protect** your wireless network.
- **Change your passwords** often, and make sure they are unique.
- Always remember to **log out** of accounts when using a public computer.

If you forget to log out of your personal accounts while using a public computer, the next person to use the computer will have access to your accounts.▼

Make a Protection Plan

The best approach to protecting yourself and your computer is to take action before anything bad happens. If you wait until your computer is infected with malware, your files or software could become corrupted before you can fix the problem. Be proactive: Outline a security plan that ensures your computer will be protected even if a threat does appear.

When you're making a plan to protect your computer, ask yourself the questions shown in **Figure 6.1**.

Figure 6.1

Am I Prepared?

- ❑ Do I have a firewall?
- ❑ Do I have antivirus software?
- ❑ Do I back up files?
- ❑ Do I check for updates regularly?
- ❑ Do I turn off the computer when I'm finished?
- ❑ Do I use unique passwords?
- ❑ Do I change passwords frequently (at least every few months)?
- ❑ Do I exercise good judgment while using the Internet?
- ❑ Do I stay up to date with new security methods?
- ❑ Do I evaluate situations with critical thinking before acting?
- ❑ Do I report suspicious activities?
- ❑ Do I follow good downloading practices?

Be Prepared:
Having backups of your important files and software will ensure that you will be able to restore your system after a malware infection.

Chapter 6 Assessment

What Do You Think?

Create a cyber protection plan for your computer by writing a three–to five–paragraph response to the questions below:

1. What security measures do you currently practice?
2. What security measures should you take to protect yourself? Why?
3. If you have a computer at home, does it have a firewall? How would you describe its effectiveness?
4. If you have a computer at home, does it have antivirus software? How would you describe its effectiveness?

Challenge: What Would You Do?

In this chapter, you learned about how to protect your computer from various threats. Now, apply what you have learned. Read the scenario below and write one paragraph explaining what you would do if faced with a similar situation. Use examples from the chapter to justify your reasoning.

Scenario:

Colin gets an email message with a subject line reading "Awesome Pictures!" He's been waiting for his friend to send pictures from a concert they went to last week, so he opens the email without checking who sent it, assuming it must be from his friend. The email contains a link telling him to click on it to view pictures. The link takes him to a website selling TVs at discount rates, and pop–ups start flooding his screen. The pop–ups advertise high–resolution TVs. Colin tries to exit out of the windows, but more keep popping up.

What should Colin have done differently in this case? What would you do if you received a similar email?

Extension Activities

Activity 1 Multiple Choice

Read the questions below. Use what you have learned in this chapter to help you choose the correct answer.

1. How many households in the United States are affected by computer viruses?
   - **A.** 10%
   - **B.** 55%
   - **C.** 40%

2. What does antivirus software do?
   - **A.** It automatically changes passwords on computer accounts every few months.
   - **B.** It searches for, removes, and prevents malicious software from attaching itself to a computer's files.
   - **C.** It backs up computer data and files.

3. What should you do if you come across something suspicious online?
   - **A.** Report it to your Internet service provider.
   - **B.** Click on it to see what it is.
   - **C.** Email it to a friend so he or she can help you decide.

4. Which of the following will NOT help you protect your computer?
   - **A.** Turn off your computer after using it.
   - **B.** Install updates regularly.
   - **C.** Keep passwords the same so you can remember them.

5. Which of the following is an action that will **best** help you safeguard your computer?
   - **A.** Don't use the Internet so that malware cannot damage your computer.
   - **B.** Put into action the best available tools to protect the computer from malicious attacks.
   - **C.** Wait until your computer is attacked and then install malware protection.

Activity 2 Short Answer

Write a one– or two–sentence response to each of the prompts below.

1. Explain the concept of computer protection.
2. Describe the four Ps of protection.
3. Identify the difference between firewalls and antivirus software.
4. Explain why it is important to use critical thinking skills while surfing the Web.
5. Explain why it is important to back up your computer.

Activity 3 Security Protection

Using what you have learned in this chapter, match each security measure with its correct definition.

1. Computer protection
2. Antivirus software
3. Firewall
4. Backing up
5. Passwords
6. Updates

A. To make a copy of files, software, and other data on a computer

B. A combination of methods used to safeguard and protect a computer's information from theft and other harmful attacks, such as corrupted files and malware

C. Items we should change often, keep unique, and assign to our wireless network

D. A security method that searches for and removes malicious software

E. A prevention method that keeps all software, computer programs, and operating systems current

F. A security method that acts like a guard and is used to protect computer networks from unauthorized access

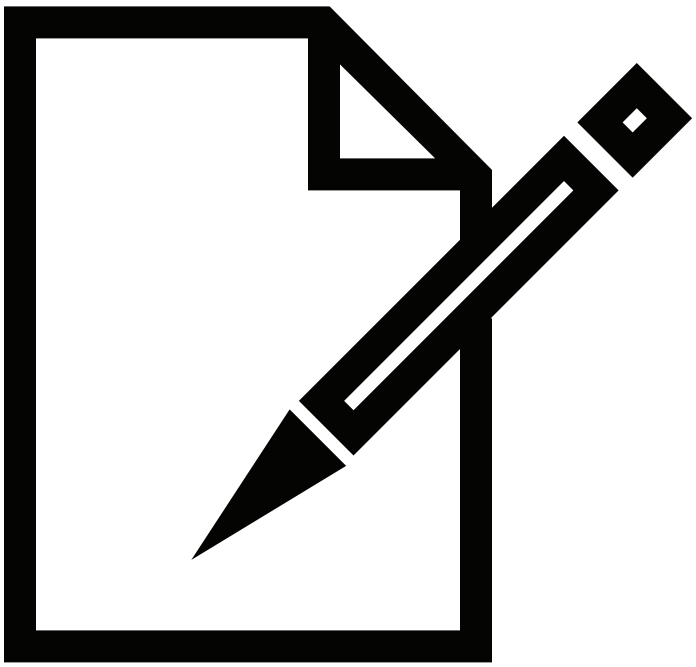
continued

Extension Activities

Activity 4 Letter of Advice

Imagine you have a friend who is buying a computer for the first time. Write him a three–paragraph letter of advice explaining what tools and techniques he can use to ensure his computer is well protected. In your letter, address the following questions:

1. What security methods are available, and which ones should your friend use?
2. What are the four Ps of protection, and why should your friend follow them?
3. How does a protection plan prevent malicious attacks?



Hands-On

Create a Board Game

Working with a small group of classmates, design a board game that incorporates the information you learned in both Chapters 5 and 6. Your game should include the following:

- Malware threats to computers, such as viruses, Trojan horses, worms, spyware, and adware
- Other threats to computers, such as phishing, pharming, and pop–ups
- Methods of protecting your computer from harm, such as firewalls, antivirus software, and updates

You might consider shaping elements of the game around what happens to computers when they do fall victim to malware and other computer threats:

- Zombies
- Bots
- Botnets

Consider what materials you want to use to create your game. You could:

- Use poster board to make all the elements of the game.
- Bring in materials from home to use instead.
- Use a software application to create the game.

After all groups have created their board games, groups should play one another's games.