Chapter 5

Hacker's Heaven: Computer Threats

Overview

Movies might make hackers look glamorous, but in real life, they and other cybercriminals wreak havoc on people's computer systems, sometimes with the intention of committing crimes. In this chapter, you will become familiar with many types of malware used by hackers and cybercriminals, including viruses, Trojan horses, worms, spyware, and adware. The cyberspace junk mail called spam as well as hacker techniques called phishing, pharming, and using pop–ups are also discussed.

Key Terms

- Computer threats
- Hackers
- Cybercriminals
- Malware
- Viruses
- Trojan horses
- Worms
- Spyware
- Adware
- Spam
- Phishing
- Pharming
- Pop–up
- Zombie
- Bot
- Botnet

Hackers and Threats

Think about all the different ways we use computers. On any given day, we may type a paper, send email, check our bank account balance online, buy a gift for a friend on an e–commerce site, and perform any number of other digital activities. However, although computers are a daily part of our lives, we often don't think about potential dangers that can jeopardize them—and our identities.

Computer threats are potentially dangerous breaches of security that can cause harm to a computer. Once a computer's security has been breached, its software can be infected, its files can be corrupted, and private data stored on the computer can be stolen. Hackers are people who "hack," or break into, computer systems through unauthorized means. Hackers are also called cybercriminals, especially when they hack in order to commit financial crimes.

Not all computer threats are inflicted by hackers, though. Sometimes, computers pick up viruses online, so we have to be careful about the websites we visit and the content we download while surfing the Web. If a computer does become infected by viruses or is otherwise vulnerable, the consequences can be dire.

Malware

One of the most common types of computer threats is malware, which is ***mal***icious soft***ware*** that hackers or cybercriminals use to gain unauthorized access to computers, steal private information, or disrupt computer operations.

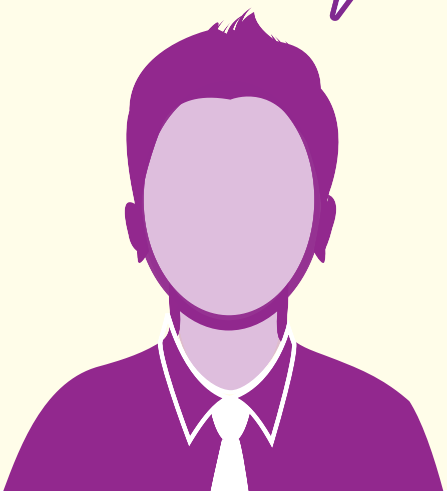
The most common malware attacks involve viruses, Trojan horses, worms, spyware, and adware. Each is discussed below:

1. Viruses are computer programs that replicate and are spread from one computer to another, typically through downloads or email attachments. Viruses attach themselves to existing computer programs and files. They can damage hardware, software, and files. Viruses require a human action (such as downloading a file or clicking on a link in an email) to spread.

Hackers are people who "hack," or break into, computer systems through unauthorized means.

Remember:

Once a computer's security has been breached, its software can be infected, its files can be corrupted, and private data can be stolen.



2 Trojan horses are files or programs that attach themselves to a computer for the purposes of hacking information or interrupting computer use. People often unwittingly download and install or run them on their computers, because they are attached to software or files that are legitimate or that look legitimate. While Trojan horses don't replicate or spread like viruses and worms, they can cause great harm to a host computer. Some Trojan horses grant a hacker remote access to a computer for a number of illicit activities, including stealing data, downloading files, and even crashing an operating system.

3 Worms are a type of virus. However, unlike viruses, they don't need a human action in order to spread. They are not attached to existing programs. Instead, they use computer networks to spread. They can do the same types of damage done by viruses. Often, worms use up bandwidth, slowing down or crashing servers or individual computers.

4 Spyware is malware that collects information without the knowledge of the computer user. Often, it is attached to software or files (such as music files) that a user wants, and it is downloaded along with the desired files. Spyware is similar to Trojan horses. It can track and record keystrokes, so it captures items such as Internet searches, log–in information, passwords, bank account information, and other private data. Most spyware is used for illegal purposes, but some uses of spyware are legitimate. For example, some companies intentionally install spyware on shared business computers to monitor employee computer use.

5 Adware is advertising software intended to make money for the creator of the advertisement. Often, adware comes bundled with free software (or freeware). The price of getting the freeware for free is having to view the ads. (Many freeware programs also have an ad–free version available—but you must pay for it.) While not all adware is malicious, it can sometimes come with spyware, which allows the creator to "spy" on user activity. When you log into your email account, for instance, and see advertisements relevant to your recent Web searches, this is an example of spyware and adware at work.

The term *Trojan horse* can be traced back to the story of the Trojan War in Greek mythology. It refers to a giant hollow wooden horse in which Greek warriors hid in order to sneak into the city of Troy.
The term *Trojan horse* has come to mean a sneaky way to get into a guarded place in order to do mischief or harm.

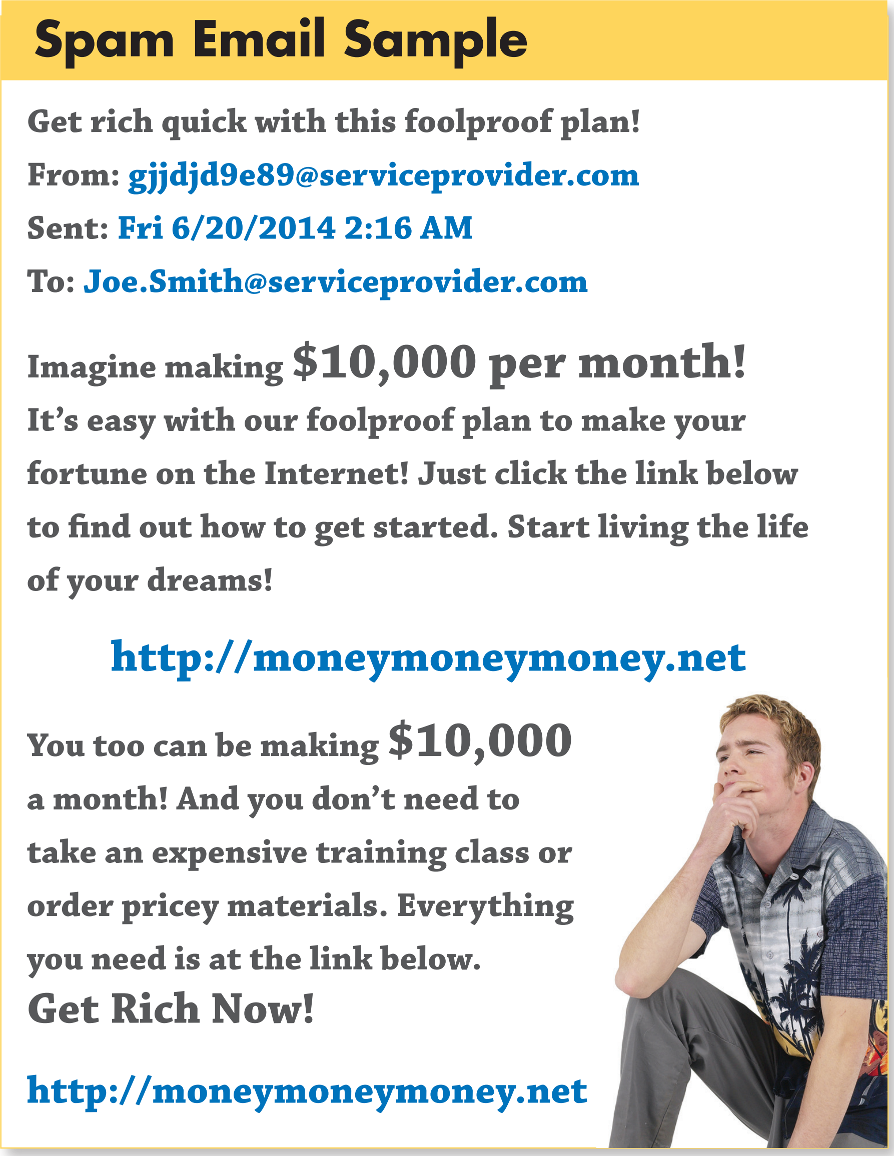
All About Spam

Have you ever heard the phrase *junk mail*? Just as our mail carrier delivers junk mail to the mailbox at our home, we can also receive junk mail in our email inbox. Usually, that junk mail is spam. Spam is unsolicited messages sent to a large group of people. Spam is most commonly sent by email, although it can also find us through instant messages, search engines, and mobile phones, too.

Spam can look like many different things, but the messages usually make offers that sound too good to be true or that seek to sell recipients a product or service. Spam could be an email telling you that you've won the lottery, a coupon for a new product, or a link to a get–rich–quick scheme. See **Figure 5.1** for an example of a spam email.

Spam can contain many different types of messages.

Figure 5.1



Spam Email Sample

Get rich quick with this foolproof plan!

From: gjjdjd9e89@serviceprovider.com

Sent: Fri 6/20/2014 2:16 AM

To: Joe.Smith@serviceprovider.com

Imagine making $10,000 per month!
It's easy with our foolproof plan to make your fortune on the Internet! Just click the link below to find out how to get started. Start living the life of your dreams!

http://moneymoneymoney.net

You too can be making $10,000 a month! And you don't need to take an expensive training class or order pricey materials. Everything you need is at the link below.
Get Rich Now!

http://moneymoneymoney.net

Phishing, Pharming, and Pop–Ups

Besides malware, hackers also use phishing, pharming, and pop–ups to gain access to private information. Each is discussed below:

Phishing

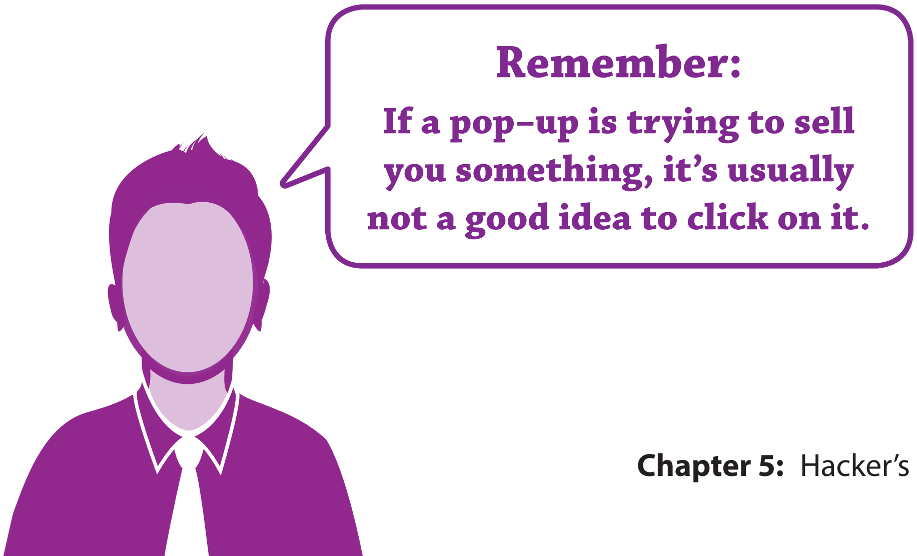
As discussed in Chapter 4, email phishing occurs when thieves send out emails that "fish" for users' private information. Sometimes cybercriminals pose as representatives of legitimate companies, or link users to phony websites that mimic the look of legitimate websites, in order to trick users into providing private information, such as Social Security numbers or passwords.

Pharming

Pharming is a tricky tactic that hackers or cybercriminals use to secretly redirect users to a different website from the one they think they are visiting. Users might think that they are visiting a bank's website, for instance, when really they are being redirected to a phony website that looks almost exactly like the real thing. When they enter their banking account password on this phony website, it is stolen, which can have severe financial repercussions for the users.

Pop–Ups

Some cybercriminals use pop–up messages, which can pop up, seemingly out of nowhere, while a user is surfing the Web. Pop–ups, which are usually advertisements, are part of phishing schemes to entice recipients to click on a link. Not all pop–ups are dangerous, because some websites use pop–up messages to display important information or to perform specific tasks. But if a pop–up is trying to sell you something, it's usually not a good idea to click on it.



Remember:

If a pop–up is trying to sell you something, it's usually not a good idea to click on it.

Fact!

Did You Know?

In late 2013, the FBI's Internet Crime Complaint Center received multiple reports of a scheme dubbed "CryptoLocker." In this scheme, when a computer user opens an infected email attachment, a virus encrypts files on the computer. Then, a pop–up informs the user that data on the computer has been encrypted and the only way to remove the encryption is to pay a ransom of $300 to $700.

Source: *Pew Internet and American Life Project*

Fact!

Did You Know?

After hijacking White House computers in 1999, a 19–year–old hacker was sentenced to 15 months in federal prison, $36,240 in fines, and restricted computer use for at least three years.

Source: *ABC News*

What Happens After an Attack?

If a computer becomes infected with any type of malware, there can be multiple dangers with which to contend. When hackers or cybercriminals contaminate a computer, they can turn the computer into a zombie. Zombie computers have been infected by a bot, a program that automatically performs tasks on the Internet without its owner's knowledge. Hackers run bots on zombie computers to transmit malware to other computers, forming a network called a botnet, which can include computers in many countries. In the midst of a botnet, unsuspecting users are inadvertently helping criminals spread malware, send spam, and conduct attacks meant to crash targeted websites.

Even if a computer isn't part of a botnet, if it is infected by malware, multiple symptoms may appear. **A few of the most common problems are listed below:**

- Computer crashes
- Computer slowdowns
- Corrupted files
- Frozen applications
- Stolen private information

> When hackers or cybercriminals contaminate a computer, they can turn the computer into a zombie.

Chapter 5 Assessment

What Do You Think?

Write a two–paragraph reflection about your experiences with computer threats. Think about the different threats that exist and ask yourself if you or someone you know has ever experienced the situations below:

1. Seen a pop–up
2. Clicked on a link in an email from an unfamiliar sender
3. Received spam email

Your paragraphs should answer the following questions:

1. What are the potential dangers posed by malware?
2. What threats should you watch out for when surfing the Web?

Challenge: What Would You Do?

In this chapter, you learned about computer threats and how they can harm your computer. Now, apply what you have learned. Read the scenarios below and write a paragraph for each, explaining what you would do if faced with a similar situation. Use examples from the chapter to justify your reasoning.

1 You are surfing the Web when suddenly, a pop–up appears on your screen. “Free Money!” reads the pop–up’s giant headline. Text in the pop–up promises $25 to anyone who convinces a friend to sign up for a service. All you have to do is click on the pop–up for more details.

What would you do? Why?

2 One day, you receive an email from an unfamiliar email address. The subject line reads “email upgrade.” The email states that your service provider needs information in order to upgrade your account. The email asks you to click “reply” and send your user name, password, Social Security number, and date of birth. If you don’t, the email states, your email account will be immediately deactivated.

What would you do? Why?

Extension Activities

Activity 1 True or False

Using the information from this chapter, determine whether each statement is true or false.

1. Hackers use only emails to gain access to unauthorized computers.
2. Spyware allows hackers to view and track user actions on a computer.
3. Computer crashes, corrupted files, and identity theft are all caused by computer threats.
4. A worm is a type of computer virus that uses computer networks to spread.
5. If a pop–up asks you to click on a link, you should click on it.

Activity 2 Key Terms

For each term, write a definition in your own words.

Hacker	Malware	Spam
Trojan horse	Worm	Bot

Hands-On

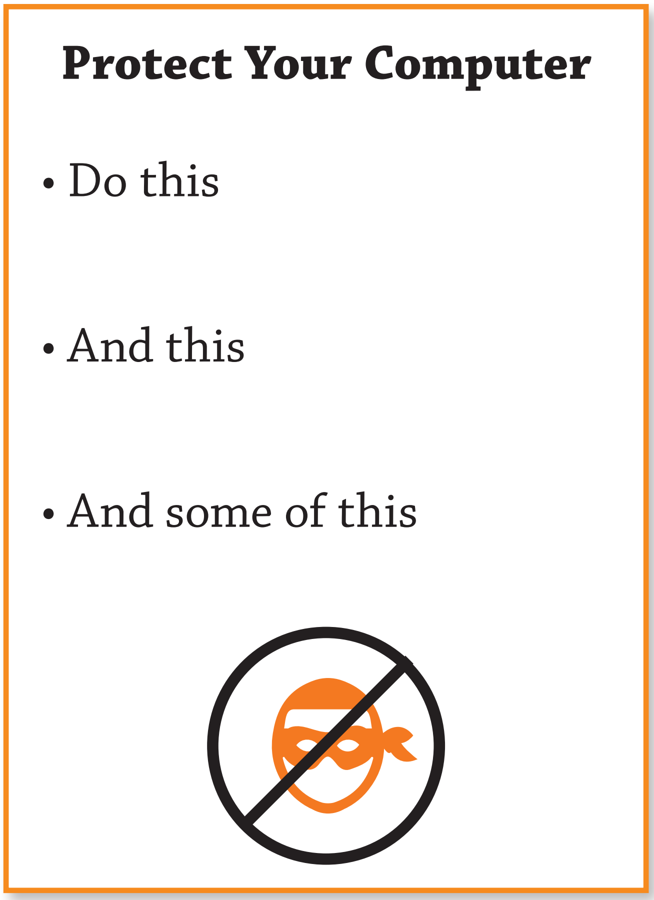
Consumer Computer Protection Tips Poster

Using poster board and colored pencils or a computer design program, create a "Consumer Computer Protection" poster that explains ways consumers can keep their computers safe from malware and other threats. See **Figure 5.2** for a sample "Consumer Computer Protection Tips" poster.

The following topics should be included in your poster:

- Types of malware
- Types of email attacks
- Prevention tips—What can we do to protect ourselves from hackers?

Figure 5.2



Protect Your Computer

- Do this
- And this
- And some of this

continued

Hands-On

Identifying Threats

Read each of the situations below and determine if they are examples of using the Internet safely. Then, participate in a classroom discussion about them. For each situation, answer these questions:

What computer threat(s) exist in this situation? What should be the consequences of these individuals' actions? Who is impacted by their decision to hack? Why?

Situation ①

Three high school juniors steal a master key from a janitor and break into their school after hours. They hack computers with IDs stolen from teachers and alter their records by changing grades and deleting suspensions on their files. After they've hacked the system, they decide to change several of their friends' grades too.

Situation ②

An 18–year–old hacker works part time as an office assistant. He steals computer passwords from a coworker in the human resources department so he can gain access to the company's network. He installs malware that grants him remote access to work computers from home. Over the course of several months, the malware captures bank account information, email correspondence, and credit card numbers from his fellow employees.

Situation ③

A high school senior doesn't completely trust his girlfriend. He is worried that when they go off to separate colleges next year, he won't know what she is doing. He decides to install spyware on her computer so he can see her calendar and emails and can log in to her social networking accounts.

Situation ④

A group of students has been assigned to work on a website project together for school. While setting up an account for a free website creator, the group debates about what username and password to use for the shared account. One student suggests they use his email username and password for the username and password of the shared account. That way, he says, he won't forget them because he uses the same username and password for all of his accounts.

Situation ⑤

Several friends want to make some extra cash, so they pool their computer knowledge and create a spam email that will target everyone on their email contact lists. The email entices readers to provide credit card information, which the friends will then use to make purchases.