**Malicious Programs**

Hackers and crackers are notorious for creating and distributing malicious programs. These programs are called **malware,** which is short for **mal**icious soft**ware.** They are specifically designed to damage or disrupt a computer system. The three most common types of malware are viruses, worms, and Trojan horses.

• **Viruses** are programs that migrate through networks and operating systems, and most attach themselves to different programs and databases. While some viruses are relatively harmless, many can be quite destructive. Once activated, these destructive viruses can alter and/or delete files. Some delete all files on the hard disk and can damage system components. Creating and knowingly spreading a virus is a very serious crime and a federal offense punishable under the **Computer Fraud and Abuse Act.** Unfortunately, new computer viruses are appearing all the time. The best way to stay current is through services that keep track of viruses on a daily basis. For example, the Virus Radar On-line project tracks the most serious virus threats.

• **Worms** are a special type of virus that does not attach itself to programs and databases. Rather it fills a computer system with self-replicating information, clogging the system so that its operations are slowed or stopped. A recent worm traveled across the world within hours, stopping tens of thousands of computers along its way. Internet worms also can be carriers of more traditional viruses. Once the traditional virus has been deposited by a worm onto an unsuspecting computer system, the virus will either activate immediately or lie dormant until some future time. Viruses and worms typically find their way into microcomputers through e-mail attachments and programs downloaded from the Internet. Because viruses can be so damaging, computer users are advised to never open an e-mail attachment from an unknown source and to exercise great care in accepting new programs and data from any source.

As we discussed in Chapter 5, antivirus programs alert users when certain kinds of viruses and worms enter their system. Some of the most widely used are Dr. Solomon’s Anti-Virus, McAfee VirusScan, eSafe, and Norton AntiVirus. Unfortunately, new viruses are being developed all the time, and not all viruses can be detected. (See Making IT Work for You: Virus Protection and Internet Security on pages 142 and 143 in Chapter 5.)

• **Trojan horses** are programs that come into a computer system disguised as something else. Trojan horses are not viruses. Like worms, however, they can be carriers of viruses. The most common types of Trojan horses appear as free computer games and free screen saver programs that can be downloaded from the Internet. Once the Trojan horse is downloaded onto a computer system, the viruses are deposited and ready to activate. One of the most dangerous types of Trojan horse claims to provide free antivirus programs. They begin by locating and disabling any existing virus protection programs before depositing a virus.

• **Zombies** are computers infected by a virus, worm, or Trojan horse that allows them to be remotely controlled for malicious purposes. A collection of zombie computers is known as a **botnet,** or **robot network.** Botnets harness the combined power of many zombies for malicious activities like password cracking or sending junk e-mail. Because they are formed by many computers distributed across the Internet, botnets are hard to shut down even after they are detected. Unfortunately for individual computer owners, it also can be difficult to detect when a personal computer has been compromised.