

# Protecting Computer Software and Data

As society becomes more and more reliant on digital information, copyright and exposure to malicious code have become two important issues among computer users. *Copyright* is protection of digital information. Copyright infringement is the illegal use or reproduction of data (text, pictures, music, video, and so on). Laws, such as the NET Act (No Electronic Theft Act) of 1997, protect against copyright infringement. There have been several well-known cases of high penalties for individuals guilty of copyright infringement.

Copyright infringement includes duplication of computer software when copies are being used by individuals who have not paid for the software. This practice is called *piracy* when illegal copies are distributed. Developing, testing, marketing, and supporting software is an expensive process. If the software developer is then denied rightful compensation, the future development of all software is jeopardized. Therefore, it is important to use only legally acquired copies of software, and to not make illegal copies for others.

Malicious code comes in many forms and is delivered in many ways. A virus, a Trojan horse, and an Internet worm are three forms of malicious code. They can appear on a system through executable programs, scripts, macros, e-mails, and some Internet connections. One devastating effect of malicious code is the destruction of data.

## **Backup Copies**

It is usually legal to make one backup copy of a purchased software program. The permission can be usually be found in the EULA (End-User License Agreement).

A *virus* is a program or series of instructions that can replicate without the user's knowledge. Often a virus is triggered to run when given a certain signal. For example, a virus might check the computer's clock and then destroy data when a certain time is reached. A virus is easily duplicated when the file is copied, which spreads it to other computers.

A *Trojan horse* program appears as something else, usually a program that looks trustworthy. Running the program runs the malicious code and damages files on the computer. A *worm* is a program that is able to reproduce itself over a network. Worms are a threat because of the way they replicate and use system resources, sometimes causing the system to shut down.

Malicious code has become so widespread that software called *antivirus programs* must be installed on computers and networks to detect and remove the code before it can replicate or damage data. Precautions can also be taken to prevent damage from malicious code:

- Update antivirus software. An antivirus program can only detect the viruses, Trojan horses, and worms it is aware of. Antivirus programs have a web link for updating the virus definitions on the computer containing the antivirus program.
- Do not open e-mail attachments without scanning for malicious code. One estimate states that 80% of virus infection is through e-mail.

Newspapers have carried numerous reports of *crackers*, or *hackers*, gaining access to large computer systems to perform acts of vandalism. This malicious act is illegal and can cause expensive damage. The Electronic Communications Privacy Act of 1986 specifically makes it a federal offense to access electronic data without authorization. Networks usually include a firewall, which is a combination of hardware and software, to help prevent unauthorized access.

The willful destruction of computer data is no different than any other vandalizing of property. Since the damage is done electronically the result is often not as obvious as destroying physical property, but the consequences are much the same. It is estimated that computer crimes cost billions of dollars each year.

*Phishing* is the act of sending an e-mail to a user falsely claiming to be a legitimate business in an attempt to trick the user into revealing personal information that could be used for crimes such as identity theft. The Communications Privacy Act of 1986 specifically makes it a federal offense to access electronic data without authorization. Networks usually include a firewall, which is a combination of hardware and software, to help prevent unauthorized access.