

## **COMPUTER VIRUSES**

Although the term "viruses" is often misapplied to all infections computers may suffer, in reality, it specifically refers to a program that is commonly attached to another program (e.g., Word Document or spreadsheet) and can replicate itself. Every time the program is run, the virus replicates itself, attached to a new document. In time, a virus can completely bog a computer down to a crawl. Viruses may also infect a boot sector or partition sector. In some cases, these latter viruses corrupt the sectors, making it impossible to reboot the computer. Sometimes viruses have built-in timers. They await a specific date and time, then do a predetermined task like completely erasing your hard drive. A common way to pick up these viruses is by loading someone else's infected files into your system or loading an infected file off the Internet. Email viruses are somewhat different. They spread through email. You are typically asked to open an attachment that will contain the virus. Only by having an up-to-date virus scanner and being very careful how you handle unknown files can you be reasonably confident your computer is safe.

## **COMPUTER WORMS**

Worms are unable to replicate within a computer; instead, they replicate by being passed from one computer to another, either via a vulnerabilities in the system or via email. Like the computer virus, they can do a great deal of damage to a computer they infect. Except for being unable to replicate within a computer, they behave much like viruses and can be every bit as damaging. Also like the viruses, you can only feel relatively safe if you use a current update of a good anti-virus software, and if you are very careful about what programs you download and what email attachments you open.

## **TROJAN HORSES**

Trojan horses enter your system by invitation. Typically, they present themselves as something they are NOT– a game perhaps. Once in your system, many Trojan horses send information about your computer to remote locations. Hackers use these "back door" Trojan horses to gain access to your system.

## **HACKERS AND CRACKERS**

Hackers (breaking and entering your system) portray themselves as different from Crackers (also steal or do damage). Most people do not make such a distinction. Most see little distinction between entering your home and handling all of your personal items and entering your home, handling all of your personal items, and stealing some of them. Hackers have a number of methods for finding and accessing your computer. They might mass mail a Trojan horse, but they can also just run programs that ping all of the possible IP addresses. If your computer is exposed and answers, the hacker may take his or her time breaking into your system. Computers have scores of portals exposed to the Ethernet. Many of them can be easily breached. A hacker with your IP address can simply explore all of the ports until he or she finds one that is open. If you do not have good security, breaking into your system can be very easy indeed! Once in your system, hackers may browse your files for private information about you and/or your credit. But they may as easily create hidden directories within your computer that permit them to store (and even deliver) pornography or other information they do not want connected to their systems. Once in your system, hackers frequently use it to attack other systems. A hack attack on a computer will often pass through several "zombies" on its way. Another common use hackers can have for your computer is Denial of Service (DOS)

attacks on other systems. These attacks are designed to interrupt communication in larger systems. For example, when hackers have accumulated enough computers, they might have them all simultaneously ping the server in a corporation as often as they are capable. The computer being pinged, forced to simultaneously answer the pings and becomes useless. Even computers with firewalls that protect them from the pinging are forced to produce a report for each ping – thousands of reports for thousands of pings every few seconds. Since it is your computer and not the hacker's, you are the one the authorities find and question. Computers attached to DSL connections, cable modems, or the Ethernet are particularly vulnerable to hacking and should be protected with up-to-date firewalls.

### **SPYWARE**

Spyware is a program that works much like a Trojan horse. People (often shareware authors) insert spyware into innocent looking programs and people load the files that contain the programs onto their computers. Once on your computer, the spyware will track your movements and purchasing patterns on the Internet. Companies collect the information and sell it as marketing databases.

Spyware that collects only statistical information is not illegal. Nonetheless, when you have spyware loaded, you are serving information from your computer to a remote location. It can be removed by specialized spyware removal programs.

### **CRASHES**

Viruses, worms, Trojan horses, and hackers can destroy your system with no notice. Furthermore, as your operating system becomes older, it tends to become buggy, and it can shut down. Technically speaking, "crashing" a computer refers to the hard drive failing, but it can also mean a board burning up. Over time, it has come to mean any time your computer shuts down without notice.

You should assume that your computer is going to crash. Maybe you get hacked and your computer ruined, or your copy of PhotoShop overloads the system and shuts you down, or maybe you suffer a brownout. It does not matter much why the system shuts down, the question is how do you protect yourself?