Computer Viruses

Understanding Risks and Prevention

5/10/2010

Michelle Hulett

Viruses 101

A computer virus, unlike a human virus, does not occur naturally, but is deliberately created by an individual who is intent on wreaking havoc. It is an actively infectious program that attaches itself to other files and has the ability to alter the way your computer works without your permission. The virus may or may not announce itself. Once a computer is infected, some or all of the application programs may slow significantly or cease working altogether. Unusual error messages may appear on your screen and/or you may run out of memory or disk space. The machine may reboot continually and/or files can become corrupted or can be completely erased.

We often use the term virus to identify any type of malevolent code that adversely affects our computer, when in fact what we are dealing with is not a virus, but a Trojan horse or a worm. A Trojan horse is a file that presents itself as something desirable, but in fact is harmful. For example, it may claim to be a useful utility program or game, but when executed causes data to become corrupted and/or erased. It differs from a virus in that viruses are programmed to replicate themselves, whereas, Trojan horses do not. They typically are spread through email or downloading files from the Internet.

A worm is a program that, like a virus, is written to replicate itself, but unlike a virus, does not have to attach itself to other programs in order to reproduce. Rather, the worm uses holes in the operating system and in network security to replicate itself throughout a network. Because it can travel through a network so quickly, a worm's damage potential is significant and worms have been known to clog Internet bandwidth and bring down hundreds, if not thousands, of computers in very short periods of time.

The best way to protect your system from these threats is through the installation of an antivirus program that can automatically detect a virus, Trojan horse, or worm should it threaten your system. Many such programs are available, but their effectiveness depends on continual updating since new threats appear all the time. The software vendor typically includes a limited subscription to automatic updates to detect new viruses. Once the subscription expires, however, it is incumbent on you to renew it.

Viruses are often spread through ignorance or sheer laziness. Students may say that they do not have the time to update their antivirus program and/or that they cannot afford the cost of the update. If you are prone to think this way, ask yourself how much time will it take to reformat your hard drive if a virus destroys your system. What if the virus permanently destroys an important document such as the term paper you need to graduate? What is the value of your time and/or your documents?

The Essence of Backup

It's not a question of if it will happen, but when — hard disks die, files are lost, or viruses may infect a system. It has happened to us and it will happen to you, but you can prepare for the inevitable by creating adequate backup *before* the problem occurs. The essence of a ***backup strategy*** is to decide which files to backup, how often to do the backup, and where to keep the backup.

Our strategy is very simple — backup what you can't afford to lose every time the data changes. Store the backup away from your computer; e.g., e-mail the file to yourself as an attachment. You need not copy every file, every day. Instead, copy just the files that changed during the current session. Realize, too, that it is much more important to backup your data files than your program files. You can always reinstall the application from the original disks or CD, or if necessary, go the vendor for another copy of an application. You, however, are the only one who has a copy of the term paper that is due tomorrow. Once you decide on a strategy, follow it, and follow it faithfully! Show that you understand the nature of backup by answering the following questions:

- Which files should be backed up?
- How often should the backup be performed?
- Where should the backup files be stored?
- Should you trust anyone else to do the backup for you?