The Web Page

by Angie Stump Denton, director of Web marketing

Computer viruses

In the past couple months, several new computer viruses have been developed and spread via e-mail. A computer virus is a piece of code that is loaded onto your computer without your knowledge and runs without your authorization. Most viruses can replicate themselves. All computer viruses are man-made.

A simple virus that can make a copy of itself repeatedly is relatively easy to produce. Such a virus is dangerous because it will quickly use all available memory and halt the system. An even more dangerous type of virus is one capable of transmitting itself across networks and of bypassing security systems.

A computer virus spreads itself by infecting executable files on the system areas of hard and floppy disks, then it replicates.

Fortunately, most viruses are easily combated, and effective methods for eliminating them often are developed as soon as they are discovered. If you think your computer may be infected, take any necessary steps to clear your system and avoid infecting other computers.

Since 1987, when a virus infected ARPANET, a large network used by the Defense Department and some universities, many antivirus programs have become available. Some examples are Norton AntiVirus, Virex and McAfee. These programs periodically check your computer system for the most well-known viruses.

There are several computer-virus resources available on the Internet, including *www.faqs.org* and *http://dir.yahoo.com/Computers_and_Internet/Security_and_Encryption/Viruses/*.

What spreads viruses

Viruses have the potential to infect any type of executable code. For example, some viruses infect the boot sector of floppy disks or system areas of hard disks.

A macro virus can infect word-processing and spreadsheet documents that use macros. And it's possible for hypertext markup language (HTML) documents containing JavaScript or other types of executable code to spread viruses or other malicious codes.

Since virus code must be executed to have any effect, files that the computer treats as pure data are safe. This includes graphics and sound files, such as those ending with *.gif*, *.jpg*, *.mp3* or *.wav,* as well as text (*.txt)* files.

In other words, viewing pictures won't infect your computer with a virus. The virus code has to be in a form — such as an *.exe* or a word-processing program capable of macros — that a computer will try to execute.

When you execute infected program code, the virus will activate and try to infect other programs, either on the same computer or on other computers connected to it over a network. The newly infected programs will try to infect yet more programs.

When you share a copy of an infected file with other computer users, running the file may infect their computers also.

If your computer is infected with a boot-sector virus, it tries to write copies of itself to the system areas of floppy and hard disks. The infected floppy disks may infect other computers that boot from them, and the virus on the hard disk will try to infect still more floppies.

Multipartite viruses can spread both by infecting files and by infecting the boot areas of floppy disks.

What viruses do

Viruses are software programs, and they can do the same things as any other programs running on a computer. The actual effect depends on how they were programmed.

Some viruses are deliberately designed to damage files or otherwise interfere with your computer's operation, while others don't do anything but replicate. But even the ones that just spread themselves are harmful, since they damage files and may cause other problems in the process.

Viruses can't do any damage to hardware.

CONTINUED ON PAGE 208

General tips on avoiding viruses

1. Install antivirus software from a well-known, reputable company. Update it regularly, and use it regularly. New viruses come out every day, so an antivirus program that hasn't been updated for several months will not provide much protection against current viruses.
2. In addition to scanning for viruses on a regular basis, configure your antivirus software to start automatically each time you boot your system. This will protect your system by checking for viruses each time your computer accesses an executable file.
3. Scan any new programs or other files that may contain executable code before you run them, no matter from where they come. There have been cases of commercially distributed floppy disks and CD-ROMs spreading viruses.
4. Antivirus programs aren't good at detecting Trojan horses, so be extremely careful about opening binary files and documents from unknown sources. This includes posts in binary newsgroups, downloads and executable files unexpectedly received as attachments to e-mail or during an online chat session.
5. If your e-mail or news software automatically executes JavaScript, macros or other executable code contained in or attached to a message, disable the feature.

Be extremely careful about accepting programs or other files during online chat sessions. This seems to be one of the more common means of spreading viruses or Trojan horses. And if any other family members (especially younger ones) use the computer, make sure they know not to accept any files while chatting.

Do regular backups. Some viruses and Trojan horses will erase or corrupt files on your hard disk, and a recent backup may be the only way to recover your data. Ideally, you should back up your entire system on a regular basis. If this isn't practical, at least back up files that you can't afford to lose or that would be difficult to replace.

CONTINUED FROM PAGE 206

They won't melt your processor, ruin your hard disk drive or cause your monitor to explode. Warnings about viruses that will physically destroy your computer are hoaxes.

Trojan horses

A "Trojan horse" often is confused with a virus. It is simply a program (often harmful) that pretends to be something else, but it doesn't replicate.

For example, you might download what you think is a new game; but when you run it, it deletes files on your hard disk. Or the third time you start the game, the program e-mails your saved passwords to another person.

Simply downloading a file to your computer won't activate a virus or Trojan horse; you have to execute the code in the file to trigger it. This could mean running a program file or opening a document that can execute macros.

Viruses and e-mail

You can't get a virus by reading a plain-text e-mail message or USENET post. But watch for encoded messages containing embedded executable code (for example, JavaScript in an HTML message) or messages that include an executable file attachment (such as an encoded program file or a document containing macros).

In order to activate a virus or a Trojan horse, your computer has to execute some type of code. This could be a program attached to an e-mail message, a Word document you downloaded from the Internet or something received on a floppy disk. There's no special hazard in files attached to USENET posts or e-mail messages: They're no more dangerous than any other file.

Reduce the chance of infection

Treat any file attachments that might contain executable code as carefully as you would any other new files. Save the attachment to disk and check it with an up-to-date virus scanner before opening it.

If your e-mail or news software has the ability to execute JavaScript, Microsoft Word macros or other executable code contained in, or attached to, a message automatically, I strongly recommend you disable the feature.

If an executable file shows up unexpectedly attached to an e-mail message, you should delete it unless you can verify what it is, who sent it and why it was sent to you.

The outbreak of the Melissa virus was a vivid demonstration of the need to be extremely careful when you receive e-mail with attached files or documents. Even though a message appears to come from someone you trust, don't take for granted the file is safe or the supposed sender had anything to do with it.

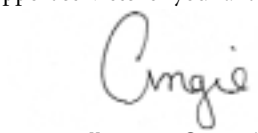
Deal with it

First, keep in mind "Nick's First Law of Computer Virus Complaints"— Just because your computer is acting strangely or one of your programs doesn't work right, this does NOT mean that your computer has a virus.

If you haven't used a good, up-to-date antivirus program on your computer, do that first. Many problems blamed on viruses actually are caused by software-configuration errors or other problems that have nothing to do with a virus.

If your computer does get infected, follow the directions in your antivirus program. If you have backup copies of the infected files, use them to restore the files. Check the files you restore to make sure your backups weren't infected also.

For assistance, check the Web site and support services for your antivirus software.



e-mail: astump@angusjournal.com