

Understanding Computer Viruses and Spyware

By BNET Editorial

published on BNET.com 12/12/2007

Computer viruses are a growing threat on the Internet. They cost organizations hundreds of millions of dollars every year. In 2007, there are *thousands* of viruses that can affect— even cripple—your computer. If current security updates are not installed on a computer, it's possible to get a virus just by visiting a Web site or opening an e-mail. To combat viruses, insure that you have the latest antivirus software, that you scan your entire computer regularly, and that you have the latest software security updates (often called "patches") for your computer; immediately delete e-mails that are in any way suspicious; don't download anything from the Internet except from reputable Web sites; and back up your data regularly.

What to Do

Understand What Can Attack a Computer

There are three main threats to your computer:

- In its simplest form, a *virus* attaches itself to a computer's files and then tries to replicate itself. Viruses can affect files ranging from program and system files to Word(r) documents and HTML files. Viruses spread with extraordinary speed via the Internet, usually by sending e-mail to all the contacts in the infected computer's address book.
- A *Trojan horse* seems to serve a useful function, such as a screen saver; however, as soon as it is run, it achieves its true purpose—anything from erasing the hard disk of the computer to using the computer as a host to infect other computers. Never download software from the Internet unless you are sure of its source and authenticity.
- *Spyware* is virus software that takes partial control of a computer to benefit a third party without the computer owner's informed consent. For example, your Internet browsing habits might be relayed to a third party, and this information would be used to target pop-up ads to you. Spyware is often bundled with otherwise useful applications so that the user does not understand the full implications of installing it. Again, never download software from the Internet unless you know it is authentic.

Take Preventative Measures

Viruses can be extremely difficult to remove; they may have inserted hidden code in your operating system that is almost impossible to detect. It is essential to prevent viruses from getting into your computer in the first place. Preventative actions you can take include the following.

- Install the latest antivirus software; popular antivirus software includes McAfee and Norton products.
- Join an e-mail list that will inform you of new virus attacks; as soon as you hear of them, check your vendor for the latest antivirus updates.
- Scan your entire computer for viruses at least once a week.
- Make sure that you have the latest security patches for your computer software; it is vital to implement software patches as soon as they become available, because viruses are most potent in the first hours and days after their release.
- If you use Microsoft Windows(r) software, check www.microsoft.com/security regularly for news and updates.
- Download software only from reputable Web sites.
- Delete e-mails (without opening them) that you are suspicious of in any way.

Know What to Do If a Virus Attacks

Deal with the threat immediately. Never wait; the longer the virus is on your computer the more damage it can do. Some viruses make your computer vulnerable to potential hacking. Even after the virus has been deleted, your system may contain some malicious code that will be used at a future date. To be completely safe after a virus has been identified in your computer system, you should reformat your hard disk and reinstall all your software.

Cope with Hoaxes

The Internet is full of virus hoaxes that waste time. If you get an e-mail about a new virus, check the Web site of your antivirus software provider to find out if the warning is real. Judge a hoax by asking the following questions:

- Does the message come from a reputable source?
- Does it ask you to e-mail it to anyone you know? If it does, it's probably a hoax.
- Does it have a reputable link for more information?

Where to Learn More

Book:

Dwight, Ken. Bug-Free Computing: Stop Viruses, Squash Worms, and Smash Trojan Horses. Teleprocessors. 2006.

Web Sites:

McAfee Antivirus Software: www.mcafee.com

Microsoft anti-Spyware software: www.microsoft.com/athome/security/spyware/software/default.aspx

Symantec/Norton Antivirus Software: <http://shop.symantecstore.com>