

Computer Viruses and Spyware

Henson Computer Services -- December 21, 2004

The following information is being provided by Henson Computer Services to help you the computer user become more aware of computer viruses and spyware. This information is intended to be a helpful guide and Henson Computer Services shall in no way be held liable for the consequences of this information, either accurate or inaccurate.

Computer Viruses

"Viruses, worms, and Trojan horses are malicious programs that can cause damage to your computer and information on your computer. They can also slow down the Internet, and they might even use your computer to spread themselves to your friends, family, co-workers, and the rest of the Web.

A virus is a piece of computer code that attaches itself to a program or file so it can spread from computer to computer, infecting as it travels. Viruses can damage your software, your hardware, and your files.

Virus (n.) Code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or information. Just as human viruses range in severity from Ebola to the 24-hour flu, computer viruses range from the mildly annoying to the downright destructive. The good news is that a true virus does not spread without human action to move it along, such as sharing a file or sending an e-mail.

A worm, like a virus, is designed to copy itself from one computer to another, but it does so automatically by taking control of features on the computer that can transport files or information. Once you have a worm in your system it can travel alone. A great danger of worms is their ability to replicate in great volume. For example, a worm could send out copies of itself to everyone listed in your e-mail address book, and their computers would then do the same, causing a domino effect of heavy network traffic that would slow down business networks and the Internet as a whole. When new worms are unleashed, they spread very quickly, clogging networks and possibly making you wait twice as long for you (and everyone else) to view Web pages on the Internet.

Worm (n.) A subclass of virus. A worm generally spreads without user action and distributes complete copies (possibly modified) of itself across networks. A worm can consume memory or network bandwidth, thus causing a computer to stop responding. Because worms don't need to travel via a "host" program or file, they can also tunnel into your system and allow somebody else to take control of your computer remotely. Recent examples of worms included the Sasser worm and the Blaster worm.

Just as the mythological Trojan horse appeared to be a gift, but turned out to contain Greek soldiers who overtook the city of Troy, today's Trojan horses are computer programs that appear to be useful software, but instead they compromise your security and cause a lot of damage. A recent Trojan horse came in the form of an e-mail that included attachments claiming to be Microsoft security updates, but turned out to be viruses that attempted to disable antivirus and firewall software.

Trojan horse (n.) A computer program that appears to be useful but that actually does damage. Trojan horses spread when people are lured into opening a program because they think it comes from a legitimate source. To better protect users, Microsoft often sends out security bulletins via e-mail, but they will never contain attachments. Microsoft also publishes all security alerts on its secure web site before we e-mail them to customers. Trojan horses can also be included in software that you download for free. Never download software from a source that you don't trust." ⁽¹⁾

(1) This information provided from the following internet link:

<http://www.microsoft.com/athome/security/viruses/virus101.mspx>

Countermeasures that you should use to improve the resistance of your computer to computer viruses include all of the following:

1. Purchase and install an effective anti-virus software program. Nationally known vendors of quality products include (not an exhaustive list):
 - Norton Anti-virus (Symantec Corporation) <http://www.symantec.com>
 - PC-cillin (Trend Micro Corporation) <http://www.trendmicro.com>
 - McAfee VirusScan (Network Associates Corporation) <http://www.mcafee.com>
2. Anti-virus software protection requires a subscription service (just like buying a magazine). You should keep the list of viruses (the virus definition file and other files) up to date on your computer. New viruses are invented and unleashed on the computing public every day and only by timely updates from the vendor subscription service can you hope to keep your computer virus free. Just purchasing anti-virus software once, or staying only with the initial subscription that you receive with your new computer is not sufficient. This information will become stale over time, becoming less and less useful as new viruses are unleashed.
3. Update your operating system software for all critical (security) updates made available by the manufacturer. Microsoft WindowsTM users are assisted in this task by the Windows Update feature accessed by selecting "Start/All Programs/Windows Update" while you have internet access
4. Practice "safe computing". Here are some helpful Do's and Don't's while using your computer:
 - Don't open email attachments from unknown senders (delete mail without reading)
 - Don't activate the "preview pane" or pre-read window in your email program
 - Don't send email to others while you know you have a computer virus
 - Don't use a floppy disk or CD in your computer that you know has a virus infection
 - Don't visit questionable webpages on the internet
 - Don't click on inviting looking pop-ups that occur on your screen while browsing the internet. Click only on the "X" in the upper right corner to close them out.
 - Do update your anti-virus definition list at least weekly (most vendors update the definitions late on Wednesday)
 - Do inform others when you may have sent them a virus via email or a computer file.

Spyware

"Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent. You might have spyware or other unwanted software on your computer if:

- You see pop-up advertisements even when you're not on the Web.
- The page your Web browser first opens to (your home page) or your browser search settings have changed without your knowledge.
- You notice a new toolbar in your browser that you didn't want, and find it difficult to get rid of.
- Your computer takes longer than usual to complete certain tasks. (slower than usual)
- You experience a sudden rise in computer crashes.

Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information. That does not mean all software which provides ads or tracks your online activities is bad. For example, you might sign up for a free music service, but "pay" for the service by agreeing to receive targeted ads. If you understand the terms and agree to them, you may have decided that it is a fair tradeoff. You might also agree to let the company track your online activities to determine which ads to show you.

Other kinds of unwanted software will make changes to your computer that can be annoying and can cause your computer to slow down or crash. These programs have the ability to change your Web browser's home page or search page, or add additional components to your browser you don't want. These programs also make it very difficult for you to change your settings back to the way you originally had them. These types of unwanted programs are also often called spyware.

The key in all cases is whether or not you (or someone who uses your computer) understand what the software will do and have agreed to install the software on your computer.

There are a number of ways spyware gets on your system. A common trick is to covertly install the software during the installation of other software you want such as a music or video file sharing program. Whenever you are installing something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes the inclusion of unwanted software in a given software installation is documented, but it may appear at the end of a license agreement or privacy statement" ⁽¹⁾

(2)This information has been provided from the following internet link.

<http://www.microsoft.com/athome/security/spyware/spywarewhat.mspx>

There are spyware elimination and inhibit software tools that you can use. Many are available free on the internet. Two free programs that are popular are:

- Spybot Search and Destroy available from <http://www.download.com>
- Ad-Aware Personal Edition available from <http://www.lavasoftusa.com>

As with virus resistance tools, the list of known spyware (a reference or definition file) should be updated to these programs on a regular basis. We suggest a weekly poll of the internet site provided in the update feature of these tools. Finally, weekly scan your computer files using your selected spyware removal tool and tell the program to remove or fix problems identified that you think may be slowing down or inhibiting your computer from functioning properly. The same Do's and Don't's listed previously regarding computer viruses can also apply to spyware. We suggest that you do not click YES on any pop-ups that you do not understand thoroughly while browsing. You should take the time to fully understand the licensing agreement for any software that you purposely install on your computer... you might be allowing the vendor to add spyware type programs to your system.