Woody Underwood
Computer Repair
Website Development
Multimedia Services
Photography/Videography

Phone: 860.747.9829
E-mail: woody@woodyunderwood.biz
Web: http://www.woodyunderwood.biz
Mail: 22 Canterbury Lane, Plainville, CT 06062

Computer, Internet, and multimedia services at a price you can afford!

About Viruses and Malware

Your Guide to Malicious Computer Programs

Though there is a lot to read in this guide, you should read it thoroughly and understand it before continuing to use your computer to ensure that you will not end up with more malicious programs on your computer.

If you remember nothing else from this guide, remember this: the number one thing to remember when using the Internet on your computer is to always read messages thoroughly, and click "Ok", or "Run" only if you are sure that it is safe. Otherwise, click the "X" in the top right of the window to close it.

Computer viruses have long been the bane of system administrators. With the coming of high speed "always on" Internet connections into people's homes, viruses have become a problem not only for administrators, but also home computer users.

Malware is a more recent phenomenon that is related to, but not a synonym for viruses. Malware, like viruses, usually gets onto a computer through the Internet, and can make a computer run slowly, and cause annoying popups and ads while surfing the net.

This guide describes the difference between malware and viruses and explains how you can avoid getting these annoyances on your home computer.

Definition of a virus: Any application or computer code that deliberately attacks a PC by destroying or stealing data, corrupting applications, hijacking e-mail, irreversibly damaging computer hardware, or otherwise deliberately damaging computer hardware or software.

Definition of malware (a.k.a. adware/spyware): Any application that causes unwanted advertisements (like pop-ups) to be displayed while browsing the Internet, or that steals generally non-sensitive information about computer use. Malware will often take up system resources and cause the computer to behave more slowly, but is not meant to deliberately degrade computer performance.

Where malware and viruses come from: Most malware and viruses come from programs you download over the Internet. Malware and viruses can also come through peer-to-peer programs like KaZaA and WinMX. Rarely, malware is installed by a commercial application purchased in a store, generally to track demographics information.

How to steer free of malware: The key thing to remember when trying to avoid malware while downloading things on the internet is: **Can you trust the website you are visiting?** A large company like MSN or Yahoo can be trusted. If you are not sure whether to trust the site you are visiting, do a Google.com search to find out if the product you are going to download has malware. For example, to find out if a product called Rabbit by company Animalsoft has malware, search for something like "Does Rabbit by Animalsoft have malware?". Some of the search results that come up should describe if the product comes packaged with any malware.

A few other good practices to avoid malware:

- Never listen to prompts saying "You must install ____ to continue." These are common on song lyrics sites and other similar sites on the Internet.
- If you ever are asked a question that you are not sure how to answer, rather than clicking OK, click the red X in the top right corner of the window. This will ensure you don't install anything you didn't mean to.
- Never download anything other than MP3s from peer-to-peer filesharing programs, and avoid their use altogether if possible. Some filesharing programs are not only capable of downloading malware, but come bundled with malware themselves.
- Remember that nothing is really free. If you are downloading a free program, do a search first to see if it might contain malware.

How to steer free of viruses: Generally you can steer free of viruses in the same way you stay away from malware. It is also essential however, to **always install virus updates within 24 hours of when you are prompted to install them.** Virus updates are generally released around one week before new viruses have time to spread to a large number of computers, so keeping up-to-date can save you a lot of hassle. **It is also essential to install Microsoft Windows updates within several days of when they are released.** They are generally released two weeks or more before a hacker finds the security flaws that they correct.

Good practices to avoid viruses:

- Keep your virus definitions and Windows updates up-to-date.
- Never open e-mails, especially those with attachments, unless you recognize and trust the person who sent them to you.
- Run a full-system virus scan at least once a week.
- Follow all good practices for avoiding malware (listed above).

What to do if you get a virus: If you've kept your virus definitions up-to-date, your chances of getting a virus are slim, as your anti-virus software should automatically delete any viruses as you work before they can harm your system. If you are prompted by your anti-virus software that a virus was detected, simply follow the on screen prompts to fix, quarantine, or delete the virus. If the anti-virus utility fails to remove the virus, generally there is no need to worry. Some viruses are stored in compressed files downloaded in the background from the Internet from e-mails. Your anti-virus utility may not be able to delete these, but it should be able to stop them from damaging your computer.

If your computer exhibits virus-like behavior, update your virus definitions and run a full system virus scan right away. If no viruses are detected, your computer may have malware. If viruses are detected and are not able to be removed, you should contact a computer repair technician right away. Some technicians may be able to diagnose the severity of the virus problem over the phone if you read the information provided by your anti-virus utility.

If you think your computer has malware: **At the first sign of malware (suddenly slowed performance, excessive popups, etc.), you should run the Windows System Restore utility.** Click Start→Programs→Accessories→ System Tools→System Restore. Follow the on screen prompts to restore your computer to a time before the problem began. After the restoration is complete, you can ensure that you are malware free by running Microsoft's Windows Defender or a similar program.

If you still experience problems on your computer, contact a computer repair technician right away. He/she will have the best chance of correcting the problem without erasing everything on your computer if he/she receives the computer as soon as possible after the problem started.