

Online Computer Security: Malware Prevention and Removal

By David Stansbury, January 6, 2006

The term “malware” describes many forms of malicious software that may infest a computer. These include *viruses, spyware, adware and other unwanted programs*. Malware can slow your computer, cause advertisements to pop up on your screen, log and report what you do and where you browse on the internet, infiltrate your emails and even damage the operating system of your computer! Malware can disrupt your work, cause programs to slow or stop working, hijack your web browser and create many other undesirable and damaging effects. Chances are, at some time most of us will be affected by some form of malware.

While this may sound scary (or familiar) to you, there is hope! With a little education and by taking some preventive measures, you can enjoy a safe and productive online computing experience.

Your first line of defense should be a comprehensive internet security software suite. For as aggressive and damaging malware is, there are very good applications available, many at no cost, that can help fight against the bad stuff. You need both anti-virus and anti-spyware software, since anti-virus software many not solve a spyware problem, and vice versa. Secondly, a good internet gateway firewall is highly recommended, discussed later. Third, you need to keep your computer updated with the latest security patches. Then finally, learn safe internet surfing habits and avoid bad websites!

Anti-Virus

My last count found over 40 anti-virus vendors on the market and I have tried most of them. Each is effective, the greatest differences being in the user interface and price. Anti-virus programs from the big-name vendors like Symantec and McAfee are very good. Grisoft AVG anti-virus offers a fully-functional free (for personal use) version that works great on all versions of Windows, even on older computers.

You need to keep your anti-virus software updated with the latest virus definitions at least weekly. Anti-virus software that is not active and updated is practically useless. Most good programs can be scheduled to update and scan your computer regularly. Hundreds of new viruses appear each month; an anti-virus program with last month’s virus definitions may not be effective against that new email virus you could receive tomorrow.

Anti-Spyware

Anti-spyware software is a little more complicated since there are many variants out there. From my extensive research and experience I can recommend a few that are particularly effective and easy to use. In fact I would download and use each of the applications listed below. Several programs working together tend to compliment each other's effectiveness to give you more complete protection.

- Javacool Software makes "SpywareBlaster", a freeware program that can prevent the downloading or installation of over 5200 bad programs. It does not remove spyware, but prevents it from ever installing!
- Another highly recommended program is "SpyBot S&D". It can prevent the installation of over 8400 malware applications, and can remove many existing infestations.
- Lavasoft makes a program called "Ad Aware" (free personal version available) that is very effective at removing stubborn spyware programs. It compliments the system cleaning abilities of SpyBot S&D very well.
- Microsoft offers a free "Malicious Software Removal Tool" that can scan your computer and remove some particularly nasty malware. It is routinely included with the regular Windows Update for Windows 2000/XP/2003.
- Microsoft also offers a highly effective "Windows Antispyware" program. It is free and available to all users of Windows 2000, XP and Server 2003. Supported by a world-wide "SpyNet" community, this software is at the battlefield against the latest and most aggressive malware on the internet. Windows Antispyware can run real-time in the background, monitoring your computer against unwanted changes and applications which may try to gain entry into your computer.

Windows Updates

Microsoft strongly recommends all Windows users to keep their computer updated with the latest security patches. Keeping your computer updated can help prevent attacks against your computer from malware or hackers who may try to take advantage of a security hole or vulnerability. The service is free and available for Windows 98, NT, 2000, XP, 2003 and all future releases. It is also available for Microsoft Office 2000 and up. If you're not keeping your computer updated, do it today!

Internet Firewall

An internet firewall is a software application or hardware device placed between your computer and the internet. Think of it as your internet gatekeeper, only allowing certain authorized traffic to pass to and from the web. It helps protect you from many computer viruses that may be “probing” for a new home. Having a firewall is a very good idea for any computer connected to the internet. The two basic types are hardware and software firewalls.

- A hardware firewall is a device, typically a router or dedicated appliance that acts as an internet gateway. Internet traffic is filtered to allow normal access while blocking unwanted activity. Many devices can be customized by the user or system administrator to restrict usage, especially useful in a corporate environment.
- Software firewalls are much more economical and easier to use for the normal personal computer owner. Modern Windows operating systems with the latest Service Packs (Windows XP Service Pack 2, etc.) include a basic software firewall. More comprehensive protection is available from third party vendors. One very popular and recommended software firewall is called Zone Alarm. Both subscription and free products are available.

Safe Web Browsing

Even if you implement all of the preceding recommendations, it is still possible to infect your computer. Malware is often bundled with “free” screen savers, computer games, desktop backgrounds, fancy mouse cursors, password managers and other software downloads. Once you install the software, malware can take root in your computer – and it can be very difficult to remove.

Use common sense! Avoid unknown websites offering free downloads or offers that seem too good to be true. Stay clear of “warez” sites, “free” adult websites or other related content. If your computer is for business, do not allow the kids to use it to play games or download software.

You should also consider using a more secure web browser for online activities such as Firefox or Opera. Both are free, fully functional browsers and are not subject to the same security vulnerabilities as the ubiquitous Internet Explorer.

Reference URLs

Anti-Virus

Symantec <http://www.symantec.com>

McAfee <http://www.mcafee.com>

Grisoft <http://www.grisoft.com> *free version* <http://free.grisoft.com>

Anti-Spyware

Javacool Software <http://www.javacoolsoftware.com>

Spybot S&D <http://www.safer-networking.org/en/index.html>

Lavasoft Ad-Aware <http://www.lavasoftusa.com>

Microsoft Windows Malicious Software Removal Tool

<http://www.microsoft.com/security/malwareremove/default.aspx>

Microsoft Windows AntiSpyware Software

<http://www.microsoft.com/athome/security/spyware/software/default.aspx>

Windows Updates

Microsoft Windows Update <http://windowsupdate.microsoft.com>

Firewall

Zone Labs <http://www.zonelabs.com> *free version* <http://tinyurl.com/7cn6a>