

Jan. 7 - 20, 2005

# How to protect your Windows computers from spyware

**E**very few months, it seems, another news story appears about a virus or computer worm that shuts down computers at corporations or government offices. Though most people who go online are unaware, there are many risks to accessing the Internet from a personal or business computer, including risk of identity theft, personal records or financial information and yes, even getting a virus which corrupts files on your computer.

Fortunately, there are ways to keep your information safe and have a good experience on the Internet.

## **Spyware**

Spyware is software that secretly collects information and transmits it over the Internet back to the spyware authors, usually for the purpose of advertising, though sometimes the intent is much more malicious.

Keystroke loggers are a particularly nasty category of spyware. They collect information such as account numbers, passwords and credit card numbers — as they are keyed in — and send it to a remote location. Spyware also can “hijack” your home page, flood your browser with popup ads, spam your e-mail inbox and slow down your high-speed Internet connection. It often consumes many system resources, eventually causing systems to become slow and unstable.

Spyware generally comes “bundled” as concealed components in rogue shareware. Please note, however, that most shareware does not come with bundled spyware.

Automated attacks are also on the rise. By simply connecting your computer to the Internet, your system becomes vulnerable to a barrage of hostile inbound traffic attempting to find weak spots to exploit. A recent example was the Sasser worm that infected over 1 million PCs in May 2004.

So how can you protect your computer? Below are a list of steps to take to keep your computer as safe as possible.

## **Minimum protection**

1. Before making any system updates, be sure to backup your data files.

2. Be careful about shareware programs that you install. File-sharing and music-sharing programs, screensavers, cursors, free games and weather shareware are notorious for including spyware bundles.

3. Surf carefully. Drive-by downloads can happen when a program gets automatically downloaded to your computer — without your consent or knowledge — simply by visiting a malicious Web site.

4. Beware of popups that ask you to download anything. These often look like official security warnings leading you to comply by clicking “yes” or “OK.” Don’t be fooled. Always click the “X” in the upper right corner of the window to close it.



## **GUEST OPINION**

*Neil Simon*

5. Never open unexpected e-mail attachments and never respond to spammers.

The remaining steps require system updates. If you are not comfortable performing these steps, enlist the help of an experienced computer consultant who understands system security.

6. Install a free, safe browser for the majority of your Web browsing. Though some Web sites only will work properly with Internet Explorer, it is safer to use a more secure browser for most of your Web surfing. I recommend Mozilla, Firefox or Opera. They can be downloaded from [www.download.com](http://www.download.com).

7. Install a hardware firewall (if your Internet access is “always on” and you do not use a dial-up connection). I like the Linksys firewalls. They’re inexpensive, easy to set up and provide great defense.

8. Use a software firewall. Windows XP has one built-in; for other Windows versions I recommend ZoneAlarm. Turn on Windows Automatic Updates and use an antivirus program (I like Norton AntiVirus 2005). See [www.microsoft.com/athome/security/protect](http://www.microsoft.com/athome/security/protect) for details.

9. Configure your browser for increased security. For details, see “Browser Security” at [www.mainwaypc.com](http://www.mainwaypc.com).

10. Disable the built-in Windows “guest” account. For details, see “Disabling The Guest Account” at [www.mainwaypc.com](http://www.mainwaypc.com).

## **Spyware removal**

If you suspect spyware is running on your PC, these steps will help remove it. Complete spyware removal, however, can be difficult even for experienced users. In some cases, the help of a spyware removal expert may be necessary.

> CONTINUED FROM PAGE 1

1. Boot the computer into “Safe Mode - With Networking,” by restarting the PC and pressing F8 continuously during startup.

2. Clean out browser temporary files (Control Panel->Internet Options).

3. Download, install update definitions, and run several spyware removal programs. I have found the following combination to be quite effective: AdAware SE, Spybot Search and Destroy and SpySweeper.

It may seem like a lot of work to keep your computer safe. But

the consequences of not protecting your system can, at the least, slow down your system to a crawl. The worst could be corrupted data files or even theft of your personal or financial information. In the long run, it is worth the time and effort to protect your systems.

*Neil Simon has been a computer engineer and consultant for more than 15 years. He is the owner and primary field engineer for Mainway PC Support in Boulder. Simon can be reached at (303) 402-9500 or [neil@mainwaypc.com](mailto:neil@mainwaypc.com).*