

A Primer on Fighting Spyware

By WALTER S. MOSSBERG

Free or Inexpensive Software Can Help Combat Programs That Hijack Your PC

[Wall Street Journal](#), December 29, 2004; Page D1

Amid the security crisis afflicting users of Windows computers, the newest, most virulent, and least understood threat comes from a class of malicious software called spyware, or adware. These malevolent programs are different from viruses, spam, or hacker attacks. And the antivirus, antispam and firewall programs you may already use do little or nothing to fight spyware, because these older types of security programs were designed to solve different problems.

During the past year, spyware has topped viruses as the biggest threat to security and privacy on Windows. One leading PC maker tells me it is receiving tens of thousands of phone calls a week from users trying to remove or fend off spyware infections. And Microsoft is so concerned about the problem that, earlier this month, it bought a small maker of antispyware technology and promised to release a preliminary version of its own spyware-fighting software, based on that technology, soon.

So, here's a primer on the spyware problem and what you can do about it.

Unlike viruses and their common variants, spyware programs don't typically seek to corrupt or destroy files, or to turn your PC into a slave for attacking other computers. And they usually don't attempt to replicate themselves, or spread, by commandeering your e-mail program.

Instead, as their names imply, spyware and adware programs try to steal your private information, record your behavior and transmit it to others, and turn your PC into an engine for displaying ads. They can alter your Web browser so it uses a bogus home page or search engine. And, in the worst case, they can steal your identity.

Spyware and adware generally insert themselves on a Windows PC in one of several ways. Sometimes, they are downloaded surreptitiously to your machine when you visit certain Web sites, a process called "drive-by downloading." To my knowledge, there's no comprehensive list of such sites, but they don't have to be obvious candidates, like porn pages.

In other cases, spyware is downloaded and installed on your PC when you visit sites that offer illegal downloads of songs, movies or TV shows. Spyware can also be installed on your PC when you consciously download and install other, legitimate programs. Sometimes, the presence of this malicious companion software is disclosed, but only in the fine print.

Some forms of spyware become obvious quickly, such as those that change your browser's home page. Others are never seen, and are hard to detect. If you have lots of spyware and adware on a PC, it may become quite sluggish, but there are so many other causes of PC sluggishness that slow performance isn't a certain sign you have spyware.

Some spyware can be traced to specific purveyors, but in many cases the programs' origins are murky. Some of it is probably written by the same type of criminals, digital vandals and thrill seekers who churn out viruses and try and break into other people's computers. But much of it comes from sleazy businesses, some of whom have convinced themselves that inserting these programs on your PC, without your permission, is just another legitimate form of marketing, advertising or research.

The most common forms of spyware and adware are:

- Browser Hijackers, which replace your browser's home page with one of their own, filled with links to their own Web pages or those of other slimy companies. You can use your browser options to restore your real home page, but the hijacker's page often replaces it again once you reboot your machine.
- Search Hijackers, which intercept legitimate search requests made to real search engines and return results from phony search services designed to send you to sites they run, or which are run by slimy partners.

- Pop-up Generators, which litter your desktop with ads, even when you're not using your Web browser, or have a pop-up blocker installed.
- Key Loggers, which record every keystroke typed on your computer, then send this information back to companies which use or sell this private information, either to blast you with ads or spam, or even to conduct identity theft.

The absolute best way to avoid spyware is to stop using Windows, and switch to an Apple Macintosh, which gets little or no spyware and adware. Almost all spyware is written to run on Windows, and it won't work on a Mac.

It's possible to write spyware for a Mac, but it's much harder, because any time a program that might affect system files tries to install itself on a Mac, the operating system requires you to enter a user ID and password. That means it's very hard to install anything surreptitiously or deceptively. Also, spyware authors gain little from invading Macs, because of Apple's tiny market share. (These are also the reasons there haven't been any recorded successful viruses on the current Mac operating system.)

But, if you're not prepared to switch platforms, there are still some ways to protect yourself from spyware and adware. The most important is to obtain and use a good antispymware program, one that is specifically and entirely focused on defeating spyware and adware. You can't rely on your existing antivirus, antispam or firewall programs, because they are primarily aimed at other threats, not at spyware and adware. Even the antivirus programs that claim to foil spyware do a poor job of it, because fighting spyware is an afterthought in their design, not their principal purpose.

I recommend three programs that can clean out most spyware and adware from your PC. Two are free: Ad-Aware SE Personal, available at www.lavasoftusa.com; and Spybot Search & Destroy, which you can get at www.download.com, and typing "spybot" into the search box.

But I prefer the third program, even though it costs a little money. It's called Spy Sweeper and is from a company called Webroot, at www.webroot.com. Like the others, Spy Sweeper can find and expunge spyware, but it also blocks new infestations. Spy Sweeper costs \$29.95, including a year of automatic updates.

Whichever program you choose, make sure and run regular scans of your system, either manually or on an automatic schedule. If you have a particularly stubborn spyware problem, you may need to run all three programs, since one may catch something another overlooks.

There are other legitimate antispymware programs, but I haven't tested them and can't recommend them. Beware of antispymware programs offered via pop-up ads or e-mail spam. Some of these actually are malicious, and will install spyware and adware, rather than expunging it.

In addition to obtaining antispymware software, I suggest adopting a few simple policies that can reduce the risk of getting spyware or adware.

First, never download files from the Internet unless you are absolutely certain what they are, and that you really need them. If a file you don't recognize tries to download, click "no" on the Windows security dialog.

Second, never download any viewer or "helper" program you don't recognize, even if a Web site says it is required to use the site.

Third, if you are tempted to download an Internet utility, like a program that automatically fills out forms, pore over all the fine print. Make sure that the program isn't collecting information, or isn't accompanied by any other software that looks like spyware or adware.

Someday, Microsoft and the makers of Windows computers may offer effective, integrated protection against spyware and adware. Someday, governments may explicitly make spyware a crime, and punish its purveyors accordingly. Until then, unfortunately, you will have to get protection and be on guard.