

Step-by-Step Guide: How to remove spyware

By Serdar Yegulalp, author "Windows 2000 Power Users Newsletter"

Step 1. Get familiar with spyware now if not already

Spyware is one of the major new scourges of the information age and the Windows platform. "Spyware" is the generic term for software that exploits either user ignorance or system insecurity to install itself, frequently without your knowledge or consent.

Spyware programs are disruptive and often dangerous. They may attempt to hijack your browser to marketing-oriented Web sites, display unwanted advertising, or spy on your browsing or typing habits and report this information back to a third party. This last attribute is where the name spyware comes from, and for many users and system administrators, it puts such programs in the same category as viruses: unwanted hostile intrusions.

You don't want this stuff on your computer. It slows things down, interferes with work and sometimes even prevents your system from being used at all.

What's to be done? The following steps outlined in this guide will help you identify and remove spyware from your own work or home machines.

Step 2. Know where spyware comes from

Spyware most commonly enters a computer one of two ways:

1) It's loaded silently via a Web page, often through a pop-up window or a hidden frame. No warning is given that the page is attempting to install a program, unless the Web browser is specifically designed to warn the user of such things. (The first edition of Internet Explorer 6 and all previous versions of Internet Explorer were vulnerable in this fashion.)

2) It's bundled with another software program, often as a way of generating advertising revenue to support that program's development.

The first of these two vectors has become by far the most broadly used -- especially in organizations where the desktop has not been correctly secured and browser plug-ins can install with impunity. The second isn't as widespread, but still popular, since you may install what you think is a free application and only find out later that it's harboring spyware.

□ **Step 3. Recognize how spyware acts**

Like virus infections, the majority of spyware infestations are silent. The computer rarely gives any indication that a new program has been installed -- certainly not one that is such a nuisance. You only know something is wrong when spyware starts popping up windows or hijacking browsers.

Up until recently, Internet Explorer didn't provide you with an easy way to determine which low-level plug-ins were installed, making it difficult to detect when an unwanted plug-in was wreaking havoc. The latest revisions of IE 6.0 and above allow this; see "Advanced cleanup" for more details.

In some cases, the offending program shows up as a new entry in Add/Remove programs and can be removed this way. Many of the more "above-board" spyware programs that are designed as revenue-generating add-ons for other software work like this (TopMoxie, for instance), but the parent program they're installed with may not work if the spyware is removed. If one breaks, they both break.

□ **Step 4. Understand what damage spyware can cause**

Annoyance is the most common and obvious damage done by spyware. Pop-up advertising windows, unwanted toolbars, Internet Explorer or system tray icons, and unexpected changes in system functionality (such as having your browser's starting home page hijacked and changed to something else) are all common symptoms of spyware infection.

These problems are bad enough in themselves, but many spyware programs are more than just a hassle -- they're invasive and destructive. They may log and track your browsing habits, which is typically an invasion of privacy. They may cause other programs to fail either because they have no friendly interaction (i.e. hijacking certain file extensions) or because spyware programs consume inordinate amounts of system resources.

The worst spyware also interfere with low-level system settings. Some rewrite the HOSTS file to redirect commonly-resolved network address names and hijack network traffic. Others may freely change Registry settings or install programs that masquerade as system-level services, which are nearly impossible to remove easily. Some even install themselves as low-level network components to do even more traffic snooping. Fortunately, because most spyware behave in a fairly obnoxious manner, they tend to at least alert the user to their presence before too long.

Step 5: Choose tools to clean up spyware

The good news: Since spyware has become so prevalent, so have a great many antispyware tools. Even better: The best such tools are free for personal use and they are kept up to date thanks to the tireless work of many contributors.

Spybot - Search & Destroy was one of the first and is still among the best. Aside from scanning for and removing thousands of known spyware applications, it also has a slew of utilities for locking down the system against future attacks. Beginners can clean their system with the push of one button, and expert users can pull detailed information about what may still be hiding and use that to do further surgery.

Lavasoft's Ad-Aware exists in both free and payware versions, but the free personal edition is widely regarded as the "other" best antispyware tool. It doesn't have the breadth of tools that Spybot - Search & Destroy does (at least not in the freeware version), but it generally cleans a broader range of problems and its scanning engine gets updated more frequently.

If you're a novice user and just want to do some cleanup, use Ad-Aware first. If you're more experienced, or have the support of a computer guru, get Spybot. Use that in beginner's mode first to do a basic cleaning, and then switch to advanced mode to see what else you can uncover.

Microsoft has also released a beta-test version of its **AntiSpyware**, which has a number of systems analysis and cleaning tools, and allows the user to submit suspected spyware to Microsoft for analysis. Finally, a number of antivirus packages now recognize and deal with spyware as a subclass of virus -- a movement which has frankly been long overdue. (**Symantec's Norton AntiVirus** is one such program, along with **Trend Micro Inc.'s PC-cillin.**)

Step 6: Use these advanced techniques to clean up spyware

If you have a greater familiarity with the inner workings of your Windows system, you can take the next step and do a more meticulous cleanup. Here are some of the best things to look for. (Note that Spybot - Search & Destroy has built-in tools for managing many of these problems.)

BHOs: Browser Helper Objects are IE plug-ins that can be installed through a Web page. Some are benign and even useful (i.e., Microsoft's own Research BHO), but any unknown BHOs should be disabled. In IE, select Tools | Internet Options | Programs | Manage Add-Ons to see the list of browser plug-ins or BHOs present in IE.

Startup: Unwanted programs often load themselves at startup. Spybot - Search & Destroy lets you browse the startup list and prune out anything that looks like it doesn't belong there. However, be careful what you turn off: Some of those programs may be legitimate.

Changes to the HOSTS file: The HOSTS file, a plaintext file with no extension found in `\windows\system32\drivers\etc.`, contains a list of pre-resolved network addresses. Usually this only contains an entry for localhost, and, unless it's been set as read only, many spyware programs love to load it up with misleading entries. For instance, a spyware program may redirect Microsoft.com to its own servers. Set HOSTS to read-only whenever possible (this is something Spybot - Search & Destroy allows).

Step 7: Install service packs to prevent spyware infections

Microsoft realized it left the doors -- or rather, the windows -- in Internet Explorer wide open to spyware, and made a number of important changes to Internet Explorer 6 in Windows XP Service Pack 2. IE now no longer allows BHOs to install themselves without your explicit permission, thus preventing the vast majority of browser-based spyware from getting a toehold in your computer.

Installing Service Pack 2 on any new Windows computer should be more or less mandatory at this point. All factory-built systems come slipstreamed with it, and any existing systems that aren't already patched ought to be. Normally, you can install SP2 through Windows Update, but if you'd rather do it by hand, or burn it to CD for the sake of updating multiple computers easily, Microsoft makes it available as a single download.

SP2, however, doesn't block the installation of spyware that comes bundled with other applications. To do so would be prohibitively difficult and might also break many legitimate programs as well.

Step 8: Take additional initiatives to prevent spyware infections

Rather than remain at the mercy of Microsoft and IE's insecurities, past or current, many people have elected to switch to a different browser entirely -- one that doesn't provide third parties as direct a path to install unwanted software on a computer. Mozilla's Firefox browser has gained explosively in popularity not only with individuals but on desktops in corporations. What it lacks (so far) in integration with Windows's domain management functions, it makes up for in new features and a better basic level of security -- especially since it doesn't run ActiveX controls (i.e., BHOs) by default.

As for spyware that comes with other applications, the only thing that makes sense is self-policing. If a program is billed as "freeware", read the installation manifest completely and pay attention to all stages of the installation process. If you see the installer attempting to install another program you know nothing about, stop the installation process and do some homework, or at least run a spyware scanning application after the fact. The odds are that any free application that needs spyware to run isn't worth the price in pain.

□ **Step 9: Plan ahead for new spyware tactics**

What of future spyware infestations? Even though it's much harder to infect a machine now than it was in the past, spyware authors are unfortunately becoming clever. The rise in the popularity of Firefox, for instance, has people worried that Firefox-specific exploits will be written to inject spyware into a computer, too. Many of the most sophisticated new breeds of spyware register themselves as operating system components, and can only be teased out by a very experienced user.

The good news is that the defensive line against spyware is also rising just as rapidly. Most out-of-the-box Windows machines as of this writing are nowhere nearly as vulnerable to spyware as they were even six months ago. Better yet, most antivirus and defensive-software makers are taking spyware more seriously as a threat, and finding ever-better ways to counter it that don't require dedicated programs or low-level system hacking.

About the Author

Serdar Yegulalp is the editor of the *Windows 2000 Power Users Newsletter*. Check it out for the latest advice and musings on the world of Windows network administrators -- and please share your thoughts as well!

©2005 TechTarget. All rights reserved. The TechTarget logo is a registered trademark of TechTarget.