



Getting rid of Adware

Even if you consider yourself the most casual Web surfer and downloader, you are still not immune to nefarious forms of spyware, also known as malware and trackware that quietly and secretly monitor everything you do online, and can communicate your activities to a third party such as an online advertiser.

- It is commonly installed on your PC as a hidden addition to a legitimate program, by visiting websites, or through spam e-mail.
- Unlike the instant impact of a virus, well-written spyware and adware programs never reveal their presence on your PC.
- Pop-up ad problems, a different homepage that you can't change, and a slower PC or online experience are indications of a spyware problem.
- No one is immune from spyware infection. A recent study by Earthlink and Webroot found an average of 26.5 spyware and adware traces per SpyAudit scan.

Why do you need protection from spyware?

- Spyware is everywhere: It infects 9 out of 10 Internet-connected computers.
- ***It can seriously disrupt your computer operations and compromise your privacy:*** Spyware can make your computer's performance and Internet access slow to a crawl. Serious infections can lead to a corrupt hard drive, and exposure of private information, usernames and passwords, or, at its worst, identity theft.
- ***Anti-virus and firewall fail to protect:*** Anti-virus software and firewalls are not capable of stopping spyware. Firewalls can't detect spyware that is embedded in legitimate programs, or protect a user from already existing internal threats. Anti-virus software is not programmed to recognize or remove spyware programs, which possess different signature files and behaviors.

Spyware and adware is often bundled with software such as Kazaa, Morpheus, Grokster, Imesh, Xolox.

When you consider the amount of valuable personal information stored on your PC, including credit card and banking details, personal e-mails and documents, shopping and browsing habits, the risks of having software intruders become obvious. Known consequences of spyware and adware include identity theft, computer problems, slow Internet access, changed homepage and favorites, and excessive numbers of adware generated adverts.

Anti-virus software and firewalls do not fully protect your system against the majority of spyware and privacy threats. Spyware is commonly bundled with software downloads, attached to e-mails, or transmitted through networks so it can appear to be legitimate software, but once installed it can be nearly impossible to detect and remove without the help of a dedicated spyware removal tool.

Spyware protection should be an essential part of your protection to defend your privacy and computing habits from prying eyes and virtual trespassers.

It is important to obtain effective protection and adhere to a strict system-cleaning regimen. Though some might suggest staying offline completely is the only foolproof privacy solution, allowing harmless cookies to remember your settings at particular sites is not that big of a deal. With the right software, you can keep malicious intruders at bay, without watering down your Web-surfing experience.

What is spyware?

Spyware programs make money for their publishers by reporting your Internet travels and sending you advertisements. Some also report your name, e-mail address, and other personal information.

Are adware and spyware different?

Different people have different definitions for each. CNET calls any program designed to deliver ads or to get marketing information *adware*. *Spyware* is a subset of adware, focused on reporting personal information.

How do adware-removal tools work?

Most adware-removal tools act like antivirus tools. They maintain a library of spyware filenames and registry keys, searching for and removing them from your computer.

Safe behind the firewall

The first thing you need to do is choose a personal firewall to make sure would-be criminals can't gain access to your computer. If your PC is already infected, a firewall will stop offending applications from reporting back to the mother ship. A number of commercial options are available, but to safeguard your system immediately, you're going to want a trustworthy free program until you decide which firewall to buy. In fact, some free firewalls provide sufficient protection against attacks, but the paid versions offer more features that might be worth your money. **If you have Windows XP, this comes with its own firewall.**

Some examples of good firewall programs are:

ZoneAlarm <http://www.zonelabs.com/store/content/home.jsp>

Kerio Personal Firewall <http://www.kerio.com/kerio.html>

Sygate Personal Pro <http://smb.sygate.com>

These programs let you use a wizard to immediately get started and defend against almost all types of attacks. Both also offer free versions that provide basic protection until you decide whether you want to buy the whole suite of security software.

Do you have adware on your PC? Do you know what adware is? Is the adware benign, or are you hosting a notorious rogue program?

Adware

Typically, adware components install alongside a shareware or freeware application. These advertisements create revenue for the software developer and are provided with initial consent from the user. Adware displays Web-based advertisements through pop-up windows or through an advertising banner that appears within a program's interface. Getting pop-up advertisements when you're working on your computer is very annoying.

Spyware

Spyware often installs as a third-party component bundled with a freeware or shareware application, just like adware, making the distinction between the two somewhat vague. Spyware includes code used to gather and transmit information about the user or his or her behavior to a third party. This statistical data often is collected without the knowledge or consent of the user.

Hijackers

Often installing as a helpful browser toolbar, hijackers may alter browser settings or change the default home page to point to some other site.

Trojan horses

Trojan horses slip into an individual's system and run without the user's knowledge. They can have many functions. For example, some use a computer's modem to dial long-distance, generating huge phone bills for the computer owner. Unlike viruses and worms, Trojan horses do not make copies of themselves.

Tracking cookies

Internet browsers write and read cookies, files with small amounts of data (such as site passwords and settings) based on instructions from Web sites. In many cases, cookies provide a benefit to users. However, in some instances cookies are used to consolidate and track user behavior across different sites, which provides marketers with private information about an individual.

Software that smacks down spies

Getting a good firewall program is only part of the solution. Next, you will need to download one or more anti-spyware applications to check your system for current culprits. You should also start a regimen of checking your computer on a weekly (or daily) basis for new or repeat offenders.

The best anti-spyware software scans your hard drive for offenders and lets you obliterate them with the click of a button. These applications offer easy-to-use update features, so you can catch the latest forms of adware and spyware as soon as they hit the Internet. Some of these programs also can be used to clear traces of PC activities and Web-surfing history, quite useful if you share your computer. As a bit of added insurance, we recommend using several spyware-removal programs to make sure your system is spic-and-span. These four reliable antispyware tools, have proven to be highly effective.

- **Spybot - Search & Destroy** spybot-virus-scan.com
- **Ad-aware SE Personal Edition** lavasoftusa.com
- **Webroot Spy Sweeper** webroot.com/wb/products/spysweeper
- **Spyware Doctor** pctools.com/spyware-doctor
- **Bazooka** <http://www.kephyr.com/spywarescanner/>
<http://www.kephyr.com/spywarescanner/library/index.phtml?source=bassindex>

Bazooka Adware and Spyware Scanner detects a multitude of spyware, adware, trojan, keylogger, foistware

and trackware components; sources of irritation that antivirus software does not deal with. The scanning process will only take about two seconds and tell you how to uninstall the potentially unwanted applications using simple step-by-step instructions or put you in contact with the vendor for the most up-to-date and safe uninstall instructions.

- **HijackThis** <http://www.spychecker.com/program/hijackthis.html>

HijackThis is a tool, that lists all installed browser add-on, buttons, startup items and allows you to inspect, and optionally remove selected items. The program can create a backup of your original settings and also ignore selected items. Additional features include a simple list of all startup items, default start page, online updates and more. **Intended for advanced users.**

With a good firewall program and one or more spyware-removal tools installed, your home computer should be safe from almost all forms of adware and spyware. Just remember to stay in the habit of regularly scanning your PC, and you will be rewarded with a system that is nearly bulletproof.

Before you scan

Any quality spyware-removal tool lets you configure it to decide which system areas to scan and what types of files to check for. To make these adjustments, look for a button marked Options, Preferences, Configuration, or Settings. For example, **Ad-aware SE** has a link labeled Customize on its Scan Now screen, whereas **Webroot Spy Sweeper** has an Options button on its main interface.

On the configuration screen, you should be able to choose which drives to scan, particularly helpful if you have multiple hard drives installed on your system. You also may choose not to scan specific folders. For instance, if you have folders containing thousands of MP3s or digital photos, you can cut down your scan times by excluding them, since it's not very likely spyware components would have invaded those folders.

In many anti-spyware applications, you also can choose to ignore specific files. You could, for example, not scan for cookies, saving some time if you don't think cookies are worth sweating. You may also be able to turn off drive scanning and just scan your machine's registry and memory. This option is fairly safe if you've previously removed all spyware from your hard drive and your removal application has a monitoring feature that scans all new software introduced to the system.

Beware of floating ads that appear to be legitimate but are in fact not. E.g. Gator or GAIN application that users unwittingly instal on their computers. <http://www.pcpitstop.com/gator/Confused.asp>

After the scan

After you have finished a scan, take a look at what your spyware remover has found. Most applications should show you the system or registry path where the unwanted components were located. You can confirm the existence of spyware by using Windows Explorer or the **regedit** command to manually follow the path noted by the spyware remover. As always, **do not** delete any registry keys unless you know what you are doing, since you could completely disable your system. Also, be wary of removing any files in folders of known, useful programs. Your anti-spyware application might have misidentified a file, or a component of a good program might use the same filename as a spyware component.