

What is "Spyware"?

There are four general types of software out there:

Freeware - This type of software is available for free, no strings attached, usually online. You can download, install, and use it as often as you want. A good example is the software available from AnalogX at <http://www.analogx.com/contents/download.htm>

Shareware - This type of software is usually distributed free of charge, but you're expected to pay a small fee to the author if you like it and use it on a regular basis.

For-pay Software - This type of software is purchased online or in a retail store. You fork over money to buy a license for the right to use the software.

Ad-ware - This type of software, usually available online, is offered to the user at no charge. However, the author of the software still wants to get paid, so he incorporates advertising technology into the software. As a result, you get the software for free, but you have to view banner ads while using the software. Sometimes ad-ware is offered also in a for-pay version that does not include the ads, giving you a choice from free and ads, or for-pay without ads.

However, there is a major catch with most (not all) ad-ware programs. In order to deliver the advertising to you, the installation program for the software not only installs the program you want, but also installs additional tracking software without your knowledge.

This tracking software monitors your surfing habits and sends this data back "home" any time you're online, again without your knowledge. The advertising company analyzes the data and uses it to deliver targeted ads to you when you use said software. For example, if you have visited several web sites checking out DVDs, this information will be sent back to the marketing company, resulting in them displaying DVD-related advertisements when you use the software.

Therefore, any software that tracks users' surfing habits, abuses a user's Internet connection to secretly send data "home", or employs any other techniques to profile or gather data about a user without express permission is called "Spyware".

Spyware also comes in other forms such as cookies that track your surfing habits.

Some Examples

Here are a few examples of common spyware programs and what they do:

- Gator's webform completion and password saving software includes offercompanion, which is advertising software, tracking your surfing habits, sending info home, and displaying ads. It is also said to

replace website's advertising with its own.

- Download programs like NetZip's Download Demon, Netscape/AOL's SmartDownload, and Real Network's RealDownload keep track of every file you download and assign you a unique ID number, enabling them to keep a detailed record of any files you download off the Internet.

- Aureate/Radiate secretly installs itself, tracks information, has the capability of installing additional software without your knowledge, hides itself, and is responsible for browser crashes.

- Ezula's TOPText/ContextPro/HOTText inserts ads in web pages that you view without your or the web site's webmaster's consent.

- Peer-to-peer file sharing software such as Kazaa, Grokster, Limewire and the likes have been known to secretly install spyware on users' machines that collects and sends personal data to another web address.

Other names you might recognize that also fall into this category are CometCursor, BonziBuddy, Alexa, RealJukebox, and many more.

What's the problem?

Spyware enables advertising and marketing companies to gather data about you without your knowledge, abuse your Internet connection to send the data back to them, analyze and profile the data, then use it for their own profit by selling advertisement.

This is an inexcusable invasion of anybody's privacy. If somebody asked you whether it's ok for somebody to look over your shoulder while you surf, make notes of sites and products you view, put this info into a database, use this info to serve you annoying ads and on top of that make money off of it, would you say "Yes, sure, go ahead" and be comfortable with that? Didn't think so.

Some of the companies defend themselves by pointing out that they clearly disclaim their practices in the fine print. However, any user you ask and inform about this type of software, didn't realize it at the time s/he was installing it.

The majority of companies distributing spyware is very covert about it and takes extra steps to hide the presence and activity of these spyware components, making it even more despicable.

In addition, Spyware only encourages and enhances annoying pop-up ads and flashing banners, wastes your bandwidth, screen real estate, time, and disk space.

Some spyware is also known to cause crashes and stability problems on users' computers.

Other spyware offers a serious security risk by opening a backdoor on your system, offering the capability to secretly install software.

How does that affect me?

Obviously you do not want a computer that

- spies on your surfing habits
- gathers personal data about you and sends it to marketing companies
- takes up your bandwidth
- crashes your browser
- bombards you with more advertising
- secretly installs unknown software
- opens up secret backdoors

Therefore it is important to keep your machine free of such malicious software.

How do I detect and remove Spyware?

Some spyware can be removed via the Add/Remove Programs applet in the Windows Control Panel, provided you know it's there and what its name is. Some of it can be removed manually. Some of it is difficult to remove due to hidden files and registry keys. In order to effectively check and clean up your system you need to be more aggressive.

Right now the most complete and thorough spyware detection and removal tool is a freeware program called Ad-Aware offered by the German company Lavasoft. You can download it at no charge from their web site at <http://www.lavasoft.de/downloads.html>.

Download and install Ad-aware on your machine. Before you use it, you will need to download the latest signature file from the same page and extract it into the Ad-aware program directory, overwriting an earlier version of the signature file.

Once installed, run Ad-ware by clicking the icon in the start menu. The program is pretty self-explanatory and walks you through the process of scanning your hard drives and registry, identifying spyware components, and removing them.

If you have questions about the software or need help, Ad-aware comes with a good manual, which is accessible from the Start menu.