



What is spyware?

Over the past few years, a new class of software has emerged that's up to no good. It goes by many names: spyware, adware, foistware, malware, eulaware, or even crapware. For simplicity we'll just call them all **spyware**. Here are some of the "features" you get from spyware. Some spyware may only use one or two of these tactics, while others do quite a bit more:

Deceptive functionality. Spyware often uses a classic "trojan horse" tactic-like a virus. It offers to synchronize your PC's clock or keep track of forms, but it is also doing other hidden things while you browse.

Home page hijacking. Did you ever find that your home page was changed, or discover new sites in Favorites that you didn't add? It might be spyware.

Loss of privacy. Some spyware keeps track of the web sites you visit and sends that information back to the spyware vendor. Do you want to tell everyone?

More advertising. Did you install a popup stopper but you are still getting popups? The ads you are getting may not be from the web site you are on, but from spyware.

Stolen advertising. Instead of showing the ads that should appear on a web site, some spyware substitutes its own ads which can rob a web site of revenue.

Broken web sites. Spyware sometimes changes the actual content on a web page, and in the process it "breaks" the page. The page may not look correct, or you may get Javascript errors.

Reduced performance. Spyware uses up system resources, CPU time, memory, disk space, and Internet bandwidth, making your system slower.

System instability. Most spyware isn't very well tested or debugged, and there is no way to report bugs or obtain tech support. The result can be system crashes, hangs, or other strange behavior.

Security risks. Some spyware has a built-in update feature that lets the spyware maker download and install new code to your system without your knowledge or approval.

Why don't antivirus utilities block spyware?

The short answer is "*spyware is not a virus.*" [Webopedia](#) defines a virus as "A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes." Spyware takes advantage of the fact that people click *I Agree* to most software licenses without actually reading them. So *technically*, spyware is loaded with your knowledge and permission if you read the license, so it's not a virus. Of course, if your teenager uses the computer and installs spyware without *your* permission, that's *your* problem too.

This tricky use of software agreements puts the antivirus companies in a tough situation. It is possible that you really did agree for some of this software to be on your system. If antivirus utilities flag these borderline programs as viruses and remove them, the antivirus companies could find themselves in a legal battle with spyware makers who claim they were given permission to install.

How do I get rid of spyware?

You can either remove each program manually, or use a utility to automatically remove all spyware. For the automatic route we recommend Webroot's Spysweeper, Spybot and LavaSoft's Ad Aware as they the best job of finding and removing all spyware.

To use a manual removal method, you first need to determine what types of spyware have infested your system. Each piece of spyware requires different removal procedures. Sometimes the spyware maker has an uninstaller at their site, but usually there will be some additional steps required before you have completely eliminated it. (This can include editing the Windows registry and/or deleting files, so it is *not* something that we recommend for novice users!) In some cases we provide links to manual removal procedures in your spyware scan results. If not, you can ask in the Spyware section of the [PC Pitstop Forums](#) or use [Google](#) to search for removal instructions using the name of the spyware.

Dirty Spyware Tricks

If you had a complete knowledge of what most spyware was doing to your system, you would never agree to install it. So how does it end up installed on so many PCs? Here are some of the dirty tricks that spyware uses to worm its way onto your system and stay there. (Not all spyware uses every technique.)

1) Hide inside another program's installer.

You will often see this technique in peer-to-peer programs like Kazaa. Hundreds of "freeware" programs install some form of spyware along with the main application. In some cases the spyware is relatively innocuous, but in others it can crash your system or invade your privacy. The only hint you may see is a short sentence or two in the end user license agreement (EULA) to the effect of "third party software may be installed along with the application."

2) Use confusion to get permission.

The license agreements don't just come out and say "we're going to collect information about you and screw up your browsing" since that wouldn't get them a lot of customers. Instead, the licenses are full of vague and confusing prose. For example, the [Gator Terms and Conditions](#) (which you are supposed to read and understand before you click "I Agree") are *14 pages and more than 6,000 words long*, not even including the several additional documents they link to there!

3) Keep asking until you say Yes.

This is particularly common with drive-by downloads such as Comet Cursor. Some spyware is delivered by an ActiveX control that tries to load each time you visit a web page where the spyware is present. As a security measure, the browser will ask if you want to install. If you say *No* it's only good until the next web page you load, where you'll again be asked the question. After a few pages of this, some people will give up and say *Yes*. (A better move would be to give up and leave that site.)

4) Create a false pretense for needing the software.

You get this email message from a friend: "I've just sent you a greeting card, go to this web site to read it!" When you get to the web site it asks you to install a "greeting card viewer" that turns out to be spyware, and it sends a similar card to everyone in your address book. In the license agreement you didn't read but agreed to, you gave it permission to do that!

5) Look essential, or be invisible.

Some spyware will use an official-sounding name like "winstartup" so that you'll be less likely to disable it if you see it running. Others maintain a low profile by using dozens of different file names and locations, or even generating a random file name to escape detection. To further mask its existence and reduce your awareness of it, many spyware packages will even install software updates without your knowledge.

6) Don't uninstall, even when asked.

Whether by design or mistake, a lot of spyware does not remove itself when you uninstall the application that originally installed the spyware. In many cases the only way to completely remove spyware is with a utility like SpyBot S&D. Some, like Gator, have cleaned up their act and have provided uninstallers.