

The Difference Between Adware & Spyware

As technology advances and more people come to rely on the [Internet](#) for information, leisure, and business it seems as if keeping your [computer](#) free of advertising is a daunting task. Not technically fitting into either the [virus](#) or [spam](#) category we have spyware and adware, which are growing concerns for Internet users. At times these [programs](#) may invade your privacy, contain malicious code, and at the very least they can be a nuisance when using a computer connected to the Internet.

Adware

[Adware](#) is considered a legitimate alternative offered to consumers who do not wish to pay for software. Programs, games or utilities can be designed and distributed as [freeware](#). Sometimes freeware blocks features and functions of the software until you pay to register it. Today we have a growing number of software developers who offer their goods as "sponsored" freeware until you pay to register. Generally most or all features of the freeware are enabled but you will be viewing sponsored advertisements while the software is being used. The advertisements usually run in a small section of the software interface or as a [pop-up ad](#) box on your [desktop](#). When you stop running the software, the ads should disappear. This allows consumers to try the software before they buy and you always have the option of disabling the ads by purchasing a registration key.

In many cases, adware is a legitimate revenue source for companies who offer their software free to users. A perfect example of this would be the popular e-mail program, Eudora. You can choose to purchase Eudora or run the software in sponsored mode. In sponsored mode Eudora will display an ad window in the program and up to three sponsored toolbar links. Eudora adware is not malicious; it reportedly doesn't track your habits or provide information about you to a third party. This type of adware is simply serving up random paid ads within the program. When you quit the program the ads will stop running on your system.

Spyware

Unfortunately, some freeware applications which contain adware do track your surfing habits in order to serve ads related to you. When the adware becomes intrusive like this, then we move it in the spyware category and it then becomes something you should avoid for privacy and security reasons. Due to its invasive nature, spyware has really given adware a bad name as many people do not know the differences between the two, or use the the terms interchangeably.

Spyware is considered a malicious program and is similar to a [Trojan Horse](#) in that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain [peer-to-peer](#) file swapping products that are available today.

Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware type program or application. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about [e-mail](#) addresses and even passwords and credit card numbers.

Because spyware exists as independent [executable](#) programs, they have the capability to monitor your [keystrokes](#), scan files on the [hard drive](#), snoop other applications, such as [chat](#) programs or word processors, install other spyware programs, read [cookies](#), change the [default home page](#) on the [Web browser](#), while consistently relaying this information back to the spyware author who will either use it for advertising and marketing purposes or sell the information to another party.

Licensing agreements that accompany software [downloads](#) sometimes warn the user that a spyware program will be installed along with the requested software, but the licensing agreements are not always be read completely by users because the notice of a spyware installation is often couched in obtuse, hard-to-read legal disclaimers.

Combating Spyware

While one may not realize they have installed spyware, there are some signs that it exists on your computer. If you notice any changes to your [Web browser](#) that you did not make such as extra [toolbars](#) or different [homepage](#) settings, as well as changes to your security settings and favorites list, you could have spyware running on your system. Other signs of a spyware infection include pop-up ads which aren't related to a [Web site](#) you're viewing; usually spyware advertisements are adult content in nature and are not displayed in the same fashion as legitimate ads you would normally see on your favorite Web sites. You may also see advertisements when you're not browsing the Web. Clicking [hyperlinks](#) which do not work (or take you somewhere you didn't expect), a sluggish system, or your system taking longer to load the [Windows](#) desktop are all signs that your computer may be infected with spyware.

With the onset of spyware comes a plethora of anti-spyware software packages to rid your system of these unwanted and malicious programs. Anti-spyware software works by identifying any spyware installed on your [system](#) and removing it. Since spyware is installed like any other application on your system it will leave traces of itself in the system [registry](#) and in other places on your computer. Anti-spyware software will look for evidence of these files and delete them if found.

It is important to remember that not all companies who claim their software contains adware are really offering adware. There is always a chance that adware is spyware in disguise so to speak, and that programs with embedded spyware may not state its existence at all. Always stay on the side of caution and be sure to research privacy policies and licensing agreements that come with freeware. You should also become familiar with Internet lists of companies reported to be using spyware. Much like a [firewall](#) or [anti-virus program](#), anti-spyware software is crucial to maintain optimal protection and security on your computer and network.