

Spyware or Adware

Has this ever happened to you? One day you're browsing the Internet as normal. The next day your browser's homepage has been changed to some off-color site and your desktop is serving up some program you don't recall installing. Termed Adware, the Internet is filled with programs that hijack your PC for profit, most hidden inside so-called "free" downloads and pop-up ads that forcibly install software on systems with improper security configurations. This doesn't mean that all free downloads are bad or that all pop-ups try to surreptitiously install software. It does mean, however, that you'll want to play close attention to both the licensing agreement of free downloads and the security settings in your browser.

What exactly is Adware? Generally speaking, it's a program that installs an additional component that feeds advertising to you or points your browser homepage to sites feeding advertising. Unless you're a fan of guerilla marketing, such tactics can be annoying. Worse, the mechanism that feeds the advertising can introduce system anomalies or incompatibilities that cause problems with other programs and can even disrupt the functioning of the operating system. Finally, a hijacked start page or toolbar can be difficult to reconfigure to its original settings because adware typically integrates itself in a manner that exceeds the average user's technical capabilities. Even more frustrating, the now present system anomalies can prevent even seasoned users from accessing the system areas they need to delete the offending program. When it is successfully removed, the original free program you did want may not work without the accompanying Adware component, forcing users to either abandon a program they do like or subject themselves to a constant onslaught of advertising.

Some Adware is a bit more insidious than others. In order to provide targeted ad banners, Adware often contains another hidden component that tracks web usage. When this occurs, the program is no longer considered Adware but instead is termed Spyware. Information gathered, often referred to as "traffic data", can consist of rather benign cookies and time spent on certain sites. However, more often it also obtains your system's unique numerical hardware ID (MAC address) and IP address, combines it with your surfing habits and correlates it with any personal information you provided when the "free" program was downloaded. Worse, it trades this information with affiliate advertising, building an increasingly complex dossier on who you are and what you like to do on the Internet. Is having your local temperature displayed on your desktop a fair trade for your privacy? If not, dump the freeware and buy a thermometer, because the odds are that's the trade you are making.

Of course, there are shining examples of free software that really are free with no strings attached. Admittedly tedious, the best way to sort good from bad is to simply read the end-user licensing agreement or privacy statement that accompanies the intended product or site.

Considering the lengths some companies will go to in order to ensure their adware/spyware cannot be easily removed, the best protection is prevention.

Fortunately, preventing adware and spyware is simple enough and won't cost you a dime.

Your first step should be to ensure your system cannot and will not install programs automatically over the Internet or launch them automatically from email.

Ensure your operating system is fully patched against any known security vulnerabilities. Visit Microsoft's [Windows Update](#) site and install any patches marked "Critical". This step should be repeated periodically, at least monthly, to ensure your operating system is fully protected against known exploits. For example, a common tactic of malicious marketers is to forcibly change your Internet Explorer startup page to their own site. They do this by exploiting a vulnerability that was first patched by Microsoft in January 2001. Despite the availability of the patch, many users have not updated and continue to be taken by this simple ruse. This is just one of literally hundreds of vulnerabilities in the Windows operating systems that leave your system open to malicious marketers and virus writers. Keeping your Windows operating system fully patched is the single most important thing you can do to ensure security.

Configure your browser to use a higher security setting. In Internet Explorer, choose Tools | Internet Options and select the Security tab. Make sure that the Internet Zone is configured to Medium Security or above.

Once you've taken steps to ensure your system cannot automatically download and run malicious code either via the Internet or email, you should see a prompt anytime an application attempts to install itself. Do not click "OK", "Yes", or "Run This Program" to anything unless you fully understand the implications of what it is trying to do. If you've deliberately downloaded an application, make sure you read and understand the End-User Licensing Agreement *before* you install it. More often than not, victims of adware and spyware click "yes" or accept the action without reading about its intentions. The following articles discuss some of the tactics employed by two purveyors of adware and spyware. Familiarize yourself with these tactics and apply that knowledge to ferret out other potentially unscrupulous vendors before letting them attach themselves to your system.

The Three Big Questions aka "The Summary"

What is adware and spyware? Adware is any program that is installed on your computer and displays ads, usually based on where you go in the Internet. Spyware is similar but its main purpose is to gather information about you and your surfing habits and "phone home" to help companies target advertising based on your interests.

Why are you so sure that I have it on my computer? Because of a tight advertising market, marketers have become very aggressive and devious in order to secure income. They have found that it is very easy to slip these programs onto users computers. They either do it with no warning or they trick you by masking the true purpose of what you are downloading and installing.

Why is it something I should be concerned about? There are numerous reasons to be concerned. Spyware and adware programs tend to be poorly written and cause drastic performance and stability problems with your computer. There is no way to know how the information gathered from your computer is going to be used and who will get it. There is a chance that very sensitive information such as social security numbers, bank account numbers, credit card numbers, and passwords could be collected.

Useful Resources

Information and reviews on Spyware/Adware software

CNET Central www.cnet.com
PC World www.pcworld.com
About.com <http://antivirus.about.com>

Spyware/Adware Software Companies

Ad-Aware <http://www.lavasoftusa.com/>
Lavasoft is the industry leader and most respected provider of anti Trackware solutions

Spybot Download from www.pcworld.com

Pop-Up Stopper Download from www.pcworld.com