How to Remove Spyware and Adware

Last Modified on 06/29/2020 4:08 pm EDT

The installation of "free" software is the #1 source of spyware on computer operating systems. This is a drain on resources and a source of lost productivity. Here's what you need to know, courtesy of Symantec.

Spyware and Adware

Spyware <http://us.norton.com/security_response/spyware.jsp> usually finds its way onto your computer without your knowledge or permission. It runs in the background, collecting information or monitoring your activities. A lot of spyware harvests information related to your computer and how you use it. For example, it may monitor your Web browsing patterns. However, more sophisticated forms of spyware have been known to capture and transmit highly personal information to identity thieves, from your website passwords and usernames to your credit card numbers or copies of your instant messages.

Adware is slightly different than spyware--the intent is primarily to display advertising content on your computer. Often using pop-up windows, adware programs flash advertisements and links to other websites. Many of these ads tout legitimate products. Some adware monitors your browsing activities and then uses that information to deliver more focused advertising content. Some people don't mind, but others consider this practice an invasion of privacy.

The most important question is: Do you want this program on your computer? If it compromises privacy and security as you define it (or at a minimum, becomes a nuisance), then it falls squarely in the category of unwelcome software. And that means you need to learn how to deal with it.

How to Remove Spyware and Adware

Whether they pose security risks or performance headaches, it's clear some types of spyware are more than a nuisance. For example, spyware and adware, working busily in the background, can dominate your computer's resources, sometimes bringing down your entire system. While a slow machine is annoying for anyone, it's especially hard on home office users.

Often these programs get installed along with other programs you've loaded. Of course, there's probably some sort of notification within the software's licensing agreement. However, these agreements tend to be quite long, and most of us don't read them in their entirety. In a typical scenario, spyware or adware gets bundled with freeware you download from the Internet. While some see this as a fair tradeoff-you get free software, the software-maker gets to observe your habits-others find it deceptive and invasive.

Meanwhile, a lot of unwelcome software makes its way onto your machine as you surf the Web. In many cases, they get you to trigger a download by clicking on a pop-up window or fake dialog box. Some pop-ups contain an "urgent" or enticing message. It might offer a free gift or claim that you need to download software to see a Web page. The window often presents what appears to be a "yes" or "no" choice. In reality, if you click the window, it will download spyware or adware to your computer, so be sure to just close the window.

How to Avoid Spyware and Adware

A lot of unwelcome software ends up on your computer in part because of something you did or did not do. Here's how to avoid unwanted spyware or adware:

- Be selective about what you download to your computer. Make sure you really need a program before downloading it. And if you've never heard of the software maker, read its website carefully to learn more about the people behind the technology, as well as the technology itself. Also, watch out for ActiveX, which is a common tool for installing spyware without your knowledge or consent. You can turn off ActiveX via your browser preferences and you can always turn it back on should a trusted site require it.
- Read licensing agreements. It can seem daunting to read these agreements, but to play it safe, don't just scroll to the bottom and click the "I accept" button when installing freeware. Instead, read each agreement carefully and look for language pertaining to any information-gathering activity, which could mean that you'll get spyware or adware along with your freebie.
- Watch out for anti-spyware scams. The Web is rife with "anti-spyware" tools that do little or nothing to prevent spyware. Some even make it worse. Purveyors of these tools often provide free scans, which almost invariably identify hundreds of spyware programs on your computer. They then immediately ask you to buy their bogus product.
- Beware of clickable advertisements. Try to avoid programs-especially freeware-that flash clickable ads. These ads should be a red flag. If you click the ads, it's possible someone is watching how you respond to them.

OP Tech Corner Picks for Best Adware Removal

Our current favorite for adware removal is AdwCleaner. Download the latest versionhere.

For anti-virus software, we recommend the freeMS Security essentials. If you use Norton or McAfee, make sure to keep them update and current. If you let the subscription expire, the production is useless. Windows 8 has Windows Defender (which is the same service as MS Security Essentials).