

Anti-Spyware Tips for Safe Computing: Spyware Prevention

Just when you thought you were finally comfortable with the computer, along comes another thing to learn...security. With more and more people online, it's no surprise that we have to be increasingly careful about what we do and where we go online. In addition, we need to understand at least a little about safe computing and avoiding things like spyware. Spyware is one of those unfortunate side effects of computer technology and can have cause serious damage, both online and offline. These programs cause anything from annoying advertisements to appear at random to actually monitoring your web surfing and keystrokes so others can steal your personal info. But you don't have to be a computer scientist to combat this growing problem. Some basic safe computing tips will help you avoid spyware and other similar internet nasties.

As scary as the idea of spyware might sound, there is a light at the end of the tunnel. First, there are quite a few things you can do to reduce the risk of a spyware infection or avoid it altogether. And for the most part, all of these things are plain old good computer security practices anyway and apply to issues besides spyware, making this a good list to for all computer users to review. Here are some preventative measures you can take:

- Keep your software up-to-date. This especially includes your operating system (Microsoft Windows for most of us) and your web browser (Internet Explorer, Mozilla Firefox, Netscape, etc). Usually most of these programs can be set to automatically update themselves or prompt you when an update is available. Go ahead and take a few minutes to do that whenever you're prompted. It can save you hours of headaches in the future if it helps protect your system.
- Be cautious about which sites you download programs from. There are tons of free programs, movies, games and other software all over the internet. However some of these programs (like the toolbar example mentioned above) are havens for spyware. All free programs aren't bad, but just like in the real world, be careful about "taking candy from strangers".
- If you don't know what a program is, don't run it or install it. If you're on a Windows machine and see an unknown file ending in .exe, you probably shouldn't run it until you determine what that program is. To find out what a program might be, try going to Google and doing a search for that file name. It will only take a minute and could save you from a huge hassle later on.
- If you're getting bombarded with pop-up ads, don't click on any of them. If you do click on them, you may inadvertently load a spyware program on your computer. This includes links that say something like "Click Here to Close". Use the little orange "X" in the corner of the window instead and that will close the window without you needing to click on anything in the advertisement.
- Don't click on any links that are in email SPAM. It doesn't matter what the offer is, if you're getting emails and you don't know the sender or didn't subscribe to that site's newsletter, etc. then you should avoid the ads and delete the email. Some of those emails will just lead to more SPAM and if they're offering software, the software can actually be riddled with spyware.

If you think your computer might have spyware on it, experts advise that you take three steps:

1. Purchase an anti-spyware program.
2. Set it to scan periodically but at the very least, once a week. It would be even better if it scans every time you start your computer as long as that doesn't slow down your start up too much.
3. Delete any software programs the anti-spyware program detects that you don't want on your computer.

Source: <http://www.articlecircle.com>

About the Author

For a limited time, get exclusive access to our anti spyware mini-course - protect yourself from this growing threat. A \$29.00 value, yours free if you sign up now. Visit: <http://www.fastspywarehelp.com/minicourse>