

Spyware/Adware Removal and protection

What is spyware/adware?

Spyware is software that is installed with or without the user's consent and monitors or "spies" on your PC, transmitting its findings to someone else over the internet. Very similar is adware, which uses similar methods of installation, but instead of transmitting data, mainly attempts to bring pop-ups and other forms of advertisement to your desktop. Some software is a combination of the two. These programs often use subtlety and deception to get installed on your PC. They are usually installed as a part of another program labeled as "free", but can also be installed via some websites which prompt the user with a security warning requesting that they install the software; most users do this without even reading it. Examples of spyware/adware and programs that come with it are:

- The free version of Kazaa Media Desktop
- Gator and Gator Wallet applications
- Comet Cursor Software
- Most toolbars and other customizations for Internet Explorer (Hotbar, MySearchBar etc.)

Apart from the privacy concerns, this software that runs in the background uses up computer resources, and can slow down a PC considerably. In addition, the amount of annoying pop-ups while surfing the internet increases dramatically. Lastly, some programs can even take control of the user's PC and use that PC as a broadcast station to send adware to more users. Some of those programs do not have a proper uninstall feature or do NOT allow the user to uninstall them. In some cases, when some of them are removed, they may cause the Internet connection to stop functioning normally since they were routing the Internet traffic through themselves and not through the normal Windows channels.

It is estimated that about 50% of all the e-mail messages transmitted in the U.S. at any given time is SPAM (i.e. Junk e-mail.) About 20-30% of that 50%, are messages generated by those PCs that are taken over by some of those ad-ware programs and are being used to relay more ads to other PCs.

What can be done?

There is software available that can remove most adware and spyware. After much experience and field testing, we recommend these three products to be used together:

Spybot-Search & Destroy (<http://www.safer-networking.org/>) is a spyware removal tool. It is free.

AD-Aware SE Personal Edition (<http://www.javasoftusa.com/support/download/>) is an adware removal tool. The Personal Edition is free.

SpywareBlaster (<http://www.javacoolsoftware.com/spywareblaster.html>) is a spyware prevention software. It is free for personal use.

How to use the Software

Spybot

- 1.) Open the software. Click the **Update** button on the left side. Click the **Search for Updates** button at the top of the right side. If there are any updates they will appear in the white window at the bottom. Select every update and click the **Download Updates** button at the top.
- 2.) Select the **Immunize** button on the left side. Then click on the **Immunize** button on the right side at the top to block all known bad products. This helps to prevent you from getting spyware installed in the first place.
- 3.) Click on the **Search & Destroy** button on the left side. Click the **Check for Problems** button at the top. When the results come up, click on **Fix Selected Problems**. If you receive a message stating that Spybot could not clean some selections because they were in use and asks you whether you want to allow Spybot to run automatically the next time you restart your PC, say yes and restart your computer. When it restarts, Spybot will start before everything else and automatically scan your system again. When it is done, click on the **Search and Destroy** button and select **Fix Selected Problems** again. This should remove most of the spyware from the system.

Ad-aware SE

- 1.) Open Ad-aware. Click the link in the lower-right corner of the window that says **Check for Updates Now**. Click the **Connect** button on the following window (make sure you are connected to the internet first). Click **OK** on the pop-up window and click **Finish** when the reference file has finished downloading.
- 2.) Click the **Start** button in the lower right corner and then click the **Next** button directly after. The software will scan your system for adware. When it is finished, You can either click the **Finish** button (if nothing was found), or click the **Next** button. Make sure everything in the window is checked, then click **Next** again. Select **Ok** on the pop-up confirmation window. After removing the adware, the program should return to the original screen.

Spywareblaster

- 1.) Open Spywareblaster. Click the **Download Latest Protection Updates** link at the bottom of the screen. Then click the **Check for Updates** button. When it finishes, Click the word **Protection** in the upper left corner of the window.
- 2.) Click the **Enable All Protection** link at the bottom. This helps to prevent you from getting spyware in the future.

It is recommended that you check for updates and update the protection for spywareblaster once a week. You only need to run Spybot and AD-Aware approximately once a month, or more often if you suspect you may have spyware/adware on your

system, (i.e. you start seeing more pop-ups or programs in your system tray [next to the time on the bottom right corner], or the PC seems to be running slower).

Recommendations & Summary

Even with the SpywareBlaster and Spybot blocking tools, it is still possible for spyware to be installed on your PC. Sometimes when you visit a website, you will see a pop-up such as: “Congratulations, you are the 1,000,000 visitor, click here to ...”, or “Your PC is infected with Spyware, please click here to...”, or “Your PC is slow! Please click here to...”, or “Would you like to download and install this free software...”. These pop-ups should be ignored, and the above programs run to remove any potentially unwanted software. At other times, you will see an official-looking grey box come up before a webpage and request to install software from a certain company. This software is usually NOT necessary to view the website, and the user should promptly click cancel, unless they are sure that it is something safe (i.e. this window comes up the first time you run Microsoft Windows Update and asks you to install a component from Microsoft is completely benign). The reason that that software is allowed to do this, is that some legitimate web sites require that you install a small program for them to work and if that was automatically blocked, the website would not function normally (like Windows Update for instance). However many companies are using this to spread their own advertising software instead.

Secondly, be careful what software you download and install on your PC. Be wary about “Free” software as it usually is “Ad-supported”. This is a fancy term for software that comes with adware/spyware and installs it to pay for their product. However some software is genuinely free with no strings attached (like the above removal software). Generally if you read the documentation on the website or on the license agreement, they will say they are also installing “Other Software” or “Third-Party Software”. Some downloads today are even encoded with a dependency on the adware/spyware with it, and will cease to function if it’s removed. These programs are not recommended in their “free” versions.

It is strongly recommended that you choose reputable on-line vendors for shopping and other general on-line transactions. It also recommended that you avoid any sites posting illegal or adult content, as these sites are well known for spreading these kind of programs, as well as viruses. In addition, if you want to sign-up for special offers, newsletters, or web accounts, it is recommended that you create a free hotmail or yahoo webmail account and use that address instead of your main e-mail address so that you can reduce the amount of junk messages you receive in your “good” inbox.

Furthermore, making sure that you have kept your operating system up to date by downloading all of the Critical updates from Microsoft Windows Update website, and having a regularly updated Antivirus solution, is a necessity to help with this growing problem.

There is a constant war between spyware program writers and spyware removal software. The most insidious spyware programs thus far are variants of the **Cool Web Search** spyware program. Those require very specialized tools and heavy manual intervention that is beyond the scope of this article. Suffice it to say, if you follow the above steps and you are still getting an increased amount of pop-ups, or your internet browser start page has changed from what it was set to and keeps changing even if you manually set it back, chances are that you have been infected with one of the more exotic spyware variants. In that case you would need to give us a call.

Spyware, adware, and spam can never be fully eliminated, but by taking the steps above you can help keep your PC as clean from this malicious software as possible and reduce the chance of being infected with the more exotic and harder to remove variants.

