

My Computer is Behaving Strangely

- Extremely slow performance on startup or accessing the Internet
- I get a different web site than I requested
- Pop-up ads are making it a pain to use the Internet
- Pop-up ads appear even when I am not on the Internet
- There new items in my browser toolbar that I did not install
- I am getting much more SPAM email than I used to
- My homepage changed and I can't change it back

What Should I Do?

First: Make sure your anti-virus definition files are current. If not update them before proceeding. (If you don't have an anti-virus software package installed, get one and install it. Be sure to run the pre-installation scan of your computer if it is offered during the install process. Refer to www.exectechcorp.com/av_software_links.htm for links to the most well-known anti-virus software purveyors. On-line virus scans can be obtained at <http://security.symantec.com/sscv6/default.asp?productid=symhome&langid=ie&venid=sym>. An on-line test for Trojans is available at www.pcfllank.com/trojans_test1.htm.)

Opinion: More of my clients who have tried McAfee anti-virus applications have had serious problems than not. It is not suitable for a business in my opinion. For business networks I favor Symantec or Sophos. For home users I prefer Norton Anti-virus or Panda.

Boot/restart your computer in Safe Mode. The easiest way to do this for Win98, WinMe & WinXP is to click on Start > Run > enter "msconfig" without the quotes > click Ok. On the first tab put a check in the Diagnostic Startup option. Click on Apply then Ok. Click Yes to reboot your computer. Select Safe Mode from the menu. For Windows 2000 Professional, touch the F8 key when restarting your PC and select Safe Mode from the menu. Acknowledge the prompt that your computer is running in Safe Mode.

If you are running Windows Me or Windows XP you must turn off System Restore. Click on Start > Help > search for System Restore. Follow the instructions to disable/turn off system restore. This is a must if you are to purge any virus or some spyware programs.

Once your computer is started in safe mode, run a full system scan of your computer with your anti-virus software. Clean infected files if possible otherwise quarantine them – DO NOT DELETE them as they may be system files that have to be restored with guidance from a professional.

If your viruses are detected, make sure that the files have been repaired or quarantined. If your computer is still functioning properly restart it in Normal mode. If you do not get any errors on startup, proceed to the next item, otherwise contact your technical support company for assistance.

Second: Obtain spyware detection and removal software. Two of the leading spyware detection and removal products available are **Ad Aware** and **Spybot Search & Destroy**. Both are free for personal use. They can be found at www.download.com. To protect against installing spyware

Computing & Network Specialists

software, download and install **SpywareBlaster** from www.javacool.com. Save each to your computer where you can find them again. Install each of them. **Be sure to update the reference files in all three of the programs mentioned before running them each time.**

IMPORTANT – READ THIS!!!

Spyware is often linked to free software that has been installed on your computer. You are strongly advised to use the Add/Remove Software function available in Control Panel BEFORE you remove any items found by Ad Aware or Spybot Search & Destroy. Remove any free programs that you installed other than the 3 just installed. Just a few to look for: Precision Time, Date Manager, My Search Bar, My Web Search, HotBar, Internet Optimizer, Ad Delivery System, Interstitial Ad Delivery, Gator, etc. You MUST attempt an uninstall before allowing their removal by one of the spyware removal tool.

TIP: Do NOT immunize your computer with Spybot Search & Destroy. You will regret it.

Ad Aware has some configuration settings (Gear Icon) that need to be set. Click on the gear icon at top of Ad Aware status window. Click on the Scanning button > make the following buttons green and checked:

Scan within archives

Scan my IE favorites for banned URLs

Scan my Hosts file

Click on the Tweak button on the left. Click on the plus (+) sign next to Scanning Engine. Make the following buttons green and checked:

Reanalyze result after scanning, before displaying result

Run scan as background process (low CPU usage)

Next, click on the plus (+) sign next to Cleaning Engine. Make the button for *Automatically try to unregister objects prior to deletion* green and checked.

You have finished configuring Ad Aware. Click on the Proceed button at the bottom of the window. You can now start the scan by clicking the Start button on the status window.

TIP: Ad Aware requires that you check each item you wish to remove. The easy way to do this is to right click when the mouse pointer is on one of the items and clicking on Select All Objects.

A program that will help greatly in identifying and removing changes to the registry, browser settings, and the hosts file is “**hijackthis.exe**”. It could have a better name, but it is a valid and useful tool when you are coached by a professional in what to remove/change. It can be obtained from <http://www.spywareinfo.com/~merijn/downloads.html>. Save the file to your desktop. Run it and save the results to a file on your computer and email it to technical support. If **CoolWebSearch** is identified on your computer then be sure to download the **CWShedder** program at the same location as it will be needed.

Third: You need to determine your vulnerabilities to attack when you are attached to the Internet. If you connect directly to a cable/DSL modem, then you are exposed 24/7. If you use a dial-up, you are still exposed when connected.

To determine just how much you are exposed, navigate to www.pcflank.com. On the left are lists of available tests that can be run safely on your computer. If you are a newbie to testing, I recommend that you visit <http://www.pcflank.com/about.htm>. It explains the tests and which ones you should run.

If you are exposed, then you can install/run a firewall that will close some of these holes in our security. Windows XP users have a built-in firewall that just needs to be turned on. Navigate to your Network Connections window, right click on the connection you use for the Internet, left click on Properties, click on the Properties button, click on the Advanced tab. Put a check in the Internet Connection Firewall checkbox. There is a link there to give you more information.

If you do not trust Microsoft, there are other firewall products available. A “free” firewall named **Outpost** is being promoted on www.pcflank.com. I have not used this software, but it is free. Another firewall software package that may still have a free version is **Zone Alarm**. It has a long history of working well, with a little aggravation to train it.

Tired of Security Weaknesses In Internet Explorer and Outlook Express

If you are like a lot of people, you are tired of patching software only to have another weakness created. Mozilla has just released a new version of **Firefox**, a very effective replacement for Internet Explorer without the vulnerabilities. I use it for 90% of my Internet browsing. The remaining 10% I must use Internet Explorer (IE) because some web sites are designed specifically for viewing in IE. It's free with no strings or spyware attached.

Mozilla's new **Thunderbird** email software is top shelf! It has built in spell checking, SPAM filtering and more. It too is free.

Both can be downloaded from www.mozilla.org.

The registered trademarks referenced within this document are sole property of their respective owners.