

### Ways to remove malware & spyware from your PC (A hopefully helpful document)

Malware & Spyware can infect your computer regardless of your anti-virus software. It is most easily “picked up” by going to unseemly places on the internet, opening strange email attachments and (in general) clicking “OK” to any window that pops up without reading & making sure you want whatever it is getting you to agree to. It can show itself as getting redirected from your intended web-site to another site – mainly ads or sites with delivery instructions for more malware, spyware, viruses, trojans, and worms via your web browser. You may notice your computer being “sluggish” and seemingly doing things on its own. You may notice an increase of Spam e-mail, indicating your entire e-mail address book has been exposed and every one of your contacts might become victims of your infected PC. In short, you should try your best to remove this stuff and cut off the source. Remember that people actually do benefit from this, usually ad revenue but can be on a slippery slope of legal to illegal ploys, otherwise it would not exist. There are no naturally occurring PC infections – they are all man-made ;-}

*Note: you may want to save a copy of this to somewhere you can find it again; we'll be rebooting and it may be tough to get back to it again!*

**The first thing to do is BACK UP anything you absolutely must have** – it may be that you cannot clean it up without a complete re-install of Windows but that is a much more complicated process. If you face this, that is where I can help! I recommend getting a USB thumb drive and copying any files, pictures, emails, etc. to it before attempting anything. Keep in mind that some of these may be the source, so be careful about using this drive after you do get things cleaned up.

The next thing to do is turn off your “System restore”; this may seem counter-intuitive but think about this – if you have had it for a while, it is part of these system “snapshots” and often have mechanisms built in to restore themselves from these if you do manage to clean the running system - One reboot and its back. To turn this off, you want to find your system properties. If you are running Windows XP, right click on “My Computer” and choose “Properties” from the pop up menu. Find the System Restore tab and check the box to turn it off. For Windows Vista or 7, the process is similar, but you may have to find “Computer” from your start menu. A good tip is that Microsoft has put a lot of work into their help systems and using the search tool can be very useful to find out how to do any of the things I mention in this.

Next, I would strongly urge you to begin using a password for your user account. This can be done via the user management tool under the start menu -> control panel. Once you have set up a password for yourself and any other users make sure that your computers “Administrator” account is either disabled or assigned a password as well. I also highly recommend disabling the “Guest” user account. Hint, Windows Vista and 7 disables these two accounts by default – if they are enabled and nobody can recall doing it, chances are that some bad software has begun to make use of them to do their dirty work. A password is the fastest way to stop it.

Once you are ready, I recommend rebooting into Windows “Safe Mode with Networking” to finish cleaning up. To do this, you will have to figure out how to make sure you get a chance to do this. Many PCs use a “Quick Boot” option that may let Windows start up quicker than you can hit the “Hot Key” that gives you boot options. To start, try hitting your “F8” key a few times as soon as you see your computers name brand logo on the screen after rebooting. By this I mean the big blue “Dell” logo if you have a Dell brand PC, I think Toshiba does their logo in Red, HP uses a blue circle with a white “HP”, IBMs and many others use a “Pre-Boot” environment than add to the issues of disabling “Recovery Mode” that may put back any bad software you manage to remove – again, a bigger topic than covering here – just remember that I can help; that’s how I earn a living! Again to stress, hit your “F8” key repeatedly until you get a screen that gives you an option of “Safe Mode with Networking” among others. Choose this option and be ready to enter your password and acknowledge that you are running in safe mode.

Some things to know is that your desktop may have “Big Icons” and your wireless networking probably will not work – you may have to run a network cable into your Home Router. *(Please have a router & not directly connected to your High Speed connection! This leaves you completely exposed to the internet. A Router will provide a “Hardware Firewall” by using a networking method called “Network Address Translation”. This basically allows you to be fairly safe by allowing outbound connections but ignoring most inbound ones – the ones you have not asked for. I hope this helps explain their usefulness & justifies the cost of one!)*

Whew, this seems like a giant chore but it really is not – there are just a lot of different scenarios & I am trying to cover as many as possible so you can be successful! If you manage to get thru all of this and wind up in “Safe Mode with Networking”, below are links to useful software to help you clean your PC. *I want to warn you again though; you may lose data (files, pics, music, email, etc.) & I, nor the makers of these applications, accept any responsibility for this!* I will also caution you to read the instructions for using each piece of software & understand what is going to do. By the way, the reason for booting to “Safe Mode with Networking” is that you only run the bare minimum to allow you to use Windows and connect to the internet; this stops most of this bad software from functioning and allows you to remove it without it “fighting back”. If you cannot download any of the software from the links below from Safe Mode, you may have to download them before booting to safe mode...

#### Malware & Spyware Cleaners:

1. MalwareBytes – <http://www.malwarebytes.org>
2. Spybot - <http://www.safer-networking.org>
3. Hitman Pro - <http://www.surfright.nl/en>

#### Free Antivirus Software

1. Microsoft’s Security Software (Windows Vista/7 & Windows XP) 32-bit & 64-bit versions - [http://www.microsoft.com/Security\\_Essentials/](http://www.microsoft.com/Security_Essentials/)
2. Avast Antivirus (Home Edition) - <http://www.avast.com/index>
3. AVG Antivirus - <http://free.avg.com/us-en/homepage>

\*\*\* This a short list of useful software – there is a lot more & may be worth researching if you still have issues.  
Extra stuff – Free Back up and System “Junk Cleaner” Software

1. Microsoft Synchtoy  
<http://www.microsoft.com/downloads/details.aspx?familyid=c26efa36-98e0-4ee9-a7c5-98d0592d8c52&displaylang=en>
2. GFI’s Free Back-up utility - <http://www.gfi.com/downloads>
3. CCleaner/Defraggler/Recuva Applications (Very useful but be careful!) - <http://www.piriform.com/>
4. Windows Sysinternals Suite-For any brave souls who feel up to using command-line tools as well as very strong GUI tools! – consider yourself warned!)  
<http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>

Thanks & Good Luck!

Vance Hensley - MCP, MCSA, MCSE, MCTS, MCITP, Security +  
PCTECHS4U

2807 Sherwood St.

Greensboro, NC, 27403

336-337-6722 (Call or TXT)

Reach Me @ [vance.hensley@triad.rr.com](mailto:vance.hensley@triad.rr.com), [pctechs4u@triad.rr.com](mailto:pctechs4u@triad.rr.com), [vance008@triad.rr.com](mailto:vance008@triad.rr.com) or

[vancehensley@gmail.com](mailto:vancehensley@gmail.com)

<http://www.pctechs4u.com>