

ANTI-MALWARE TOOLS & TIPS



Jim McKnight

www.jimopi.net

ANTIMALWARE_Tips.lwp

revised 3-5-2010

CONTENTS:

[ANTI-MALWARE TOOLS,](#)
[AUTOPLAY - DISABLE](#)

[AVG FREE -TIPS,](#)

[COMBOFIX NOTES,](#)

[ONECARE.LIVE Online Scan](#)

[SECUNIA Personal Software Inspector](#)

[SUPERAntispyware Notes](#)

[Removing commercial Anti-Malware Suites](#) [HIJACK THIS OVERVIEW](#)

[MALWARE REMOVAL GUIDE = See page 11](#)

[AVOIDING MALWARE](#)

[AVAST! TIPS](#)

[AVIRA ANTIVIR PERSONAL](#)

[FIREFOX: Enhanced security add-ons](#)

[MSE - Microsoft Security Essentials](#)

[SPYBOT S&D TIPS](#)

[WINDOWS DEFENDER](#)

*** **ALWAYS USE THE LATEST REVISION OF THIS DOCUMENT** ***

ANTI-MALWARE TOOLS *(The **BOLD** Items are my favorites)*

- AVG Free 9 Anti-malware Suite (2000/XP/VISTA/Win7) - Free: http://www.filehippo.com/download_avg_antivirus/
Here is the AVG feature comparison chart (Free vs Paid versions): <http://free.avg.com/download-avg-anti-virus-free-edition>
 - ✓ AVG - Manual Virus Removal Tools: http://www.avg-antivirus.com.au/avg_virus_removal.htm
 - ✓ AVG - LinkScanner (Separate browser add-on from AVG)
http://download.cnet.com/AVG-LinkScanner/3000-2162_4-10610872.html?tag=mncol
- AVIRA AntiVir Personal - (2000/XP/Vista/Win7. Click "Download latest version") Free: http://filehippo.com/download_antivir/
 - ✓ AVIRA RESCUE CD or Anti-Rootkit Tool - Free http://www.avira.com/en/support/support_downloads.html
(This CD does not update the signature files. You have to download it just before running for the latest files)
- Ad-Aware (I no longer recommend Adaware) *(Note: It may have problems with AVG & Spybot S&D)*
- A-Squared Free - 3.5 Scan& removal 98/XP <http://www.emsisoft.com/en/software/download/>
- Aries Rootkit Remover (for Sony Rootkit) http://lavasoft.com/support/securitycenter/aries_rootkit_removal.php
- Avast! (Supports Win98/XP/Vista/Win7) see my notes; http://filehippo.com/download_avast_antivirus/
- CleanUp! (by Steven Gould) - free http://www.stevengould.org/index.php?option=com_content&task=view&id=29&Itemid=72
- ComboFix - Free (Use the Tutorial) www.bleepingcomputer.com/combofix/how-to-use-combofix
- Dial-a-fix (for experts only) - Free <http://wiki.lunarsoft.net/wiki/Dial-a-fix>
- FIX IE (Fixes IE settings after a malware attack - IE7, IE8): <http://www.thewindowsclub.com/downloads/Fix%20IE.zip>
- GMER Rootkit Remover - Free <http://www.gmer.net/files.php>
- HijackThis *(see writeup below)* - Free www.trendsecure.com/portal/en-US/tools/security_tools/hijackthis
- Kaspersky Virus Removal Tool - Free <http://support.kaspersky.com/viruses/avptool2010?level=2>
- Kasperksy Rescue CD (ISO Image) - Free http://devbuilds.kaspersky-labs.com/devbuilds/RescueDisk/kav_rescue_2008.iso
- KillBox - Free <http://killbox.net/>
- Malicious Software Removal Tool (Start, Run, mrt.exe) - Free www.microsoft.com/security/malwareremove/default.aspx
- **Malwarebytes Anti-Malware** - 2000/XP/Vista/Win7 (Free, but no free Resident Shield):
http://www.download.com/Malwarebytes-Anti-Malware/3000-8022_4-10804572.html?tag=mncol
- McAfee Rootkit Detective - Free <http://www.pcworld.com/downloads/file/fid.67387-page.1-c.privacysecurity/description.html>
- **Microsoft Security Essentials** - Free: http://www.microsoft.com/security_essentials/

- Norton Scan & Clean - Free <http://www.softpedia.com/get/Antivirus/Norton-Security-Scan.shtml>
- RKILL (four versions) - Free. Try the first version that works on the infected PC.
 - 1.rkill.exe: <http://download.bleepingcomputer.com/grinler/rkill.exe>
 - 2.rkill.com: <http://download.bleepingcomputer.com/grinler/rkill.com>
 - 3.rkill.scr: <http://download.bleepingcomputer.com/grinler/rkill.scr>
 - 4.rkill.pif: <http://download.bleepingcomputer.com/grinler/rkill.pif>
- RogueFix <http://www.internetinspiration.co.uk/roguefix.htm#uninstall>
- Rootkit Revealer - Free <http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx>
- RUBotted (Trend) - Free www.trendsecure.com/portal/en-US/tools/security_tools/rubotted
- SDFix (for experts only, 2000 & XP) - Free <http://www.bleepingcomputer.com/files/sdfix.php>
SDFix "How to Use" (Note: Safe-mode only) <http://www.bleepingcomputer.com/forums/topic131299.html>
- **Secunia PSI** - Free http://secunia.com/vulnerability_scanning/personal/
- SmitFraudFix - Free <http://siri.geekstogo.com/SmitfraudFix.php>
- SpyBot Search & Destroy - Free: www.safer-networking.org/en/spybotsd/index.html (*Uncheck TeaTimer during install*)
- **SpywareBlaster** - Free <http://www.javacoolsoftware.com/sbdownload.html>
- Spyware Doctor Starter Ed.- Free http://www.download.com/Spyware-Doctor-Starter-Edition/3000-8022_4-10704508.html
(*Caution: May install unwanted Toolbars*)
- **SUPERAntispyware** (98/XP) - Free, but no resident shield: <http://www.superantispyware.com/superantispywarefreevspro.html>
- **SUPERAntispyware** (Portable Scanner for infected PC's): <http://www.superantispyware.com/onlinescan.html>
- Symantec Malware Manual Removal Tools: http://www.symantec.com/business/security_response/removaltools.jsp
- TDSS Killer from Kaspersky - Free: <http://support.kaspersky.com/downloads/utills/tdsskiller.zip>
- TFC Temp File Cleaner (cleans out temp files for all users at once) <http://software.addpccs.com/tfc/index.php>
- ThreatFire Anti-virus - Free: http://www.threatfire.com/?utm_source=download.com&utm_medium=frontdoor
- Trojan Remover (\$34.00, 30 day free trial): http://www.download.com/Trojan-Remover/3000-8022_4-10038982.html?tag=mncol
- Ultimate Boot CD for Windows (UBCD4WIN.COM) See my UTILITY PROGRAMS sheet for details.
- VIPRE PC Rescue Program <http://live.sunbeltsoftware.com/>
- Virus File Analyzer Service - Free <http://www.virustotal.com/>
- VundoFix: Scans & Fixes Trojans. <http://vundofix.tribune.org/>
- Virus Test: Test your A/V Program (RISKY!) - Free: http://www.eicar.org/anti_virus_test_file.htm
- Windows Defender - (XP) Free: www.microsoft.com/athome/security/spyware/software/default.aspx#
Note: Windows Defender is included in the "Microsoft Security Essentials" suite.

ONLINE SCANNING TOOLS

- Kaspersky On-line scanner: http://download.cnet.com/Kaspersky-Online-Virus-Scanner/3000-8022_4-10723401.html?tag=mncol
- **ESET (NOD32) Online Scanner** (IE7 or IE8 only): <http://www.eset.com/onlinescan/>
(Downloads & installs an ActiveX add-on for Internet Explorer)
- Trend Micro House Call - Free malware scan: <http://housecall.trendmicro.com/>.
- OneCare Live Online Protection Scan (Must use IE6,7,8) - Free: <http://onecare.live.com/site/en-us/center/howsafe.htm>
- Panda Cloud Antivirus - Free http://filehippo.com/download_cloud_antivirus/
- Shields Up! Open Port Scanner: <http://https://www.grc.com/x/ne.dll?bh0bkyd2>

- VirusTotal (upload & scan a suspicious file) <http://www.virustotal.com/>

STANDALONE (PORTABLE) SCANNING TOOLS

- SUPERAntispyware "On-line" scan: (Download & run) - Free: <http://www.superantispyware.com/onlinescan.html>

AVOIDING MALWARE:

- See the "A STRESS FREE PC" article on my website at www.jimopi.net for ideas to help secure your PC.
- MY RECOMMENDED MIX OF ANTI-MALWARE PROGRAMS: Under ordinary operating conditions, my recommended mix of anti-malware programs to give adequate protection:
 - ✓ WINDOWS UPDATES: Set to Automatic (*This is the #1 most important protection*).
 - ✓ MSE - Microsoft Security Essentials: Installed and running, including an automatic weekly "Full scan"
 - ✓ SPYWAREBLASTER for browsing protection. Must be updated manually at least once a month.
 - ✓ LINKEXTEND FOR FIREFOX browsing protection: Firefox Add-on called "LinkExtend". See *Firefox Tips*.
 - ✓ SITE ADVISOR FOR INTERNET EXPLORER browsing protection. Add-on called McAfee "Site Advisor".
 - ✓ SECUNIA PSI: Installed and running. Run a manual scan at least once a month.
- LINK SCANNERS: Malware is getting so insidious that you can get infected by just browsing to the wrong site and viewing an infected image. The best protection against this is the use of browser "Link Scanner" plug-ins that advise you ahead of time that a particular site may be malicious. These scanners are currently included in many anti-malware suites, and are also available separately. See the McAfee Site advisor for IE or a Firefox add-on called "LinkExtend". I also like a free program called SpywareBlaster that sets up all your browsers with protections.
- A common source of malware is by a site popping up a window that tells you that you need to download the latest version of Flash, Java, or some other viewer in order to see the content. By clicking that Window you are actually giving permission that allows the malware to install itself on your PC. Even Pop-up blockers do not deter the bad guys.
- Another common source of malware is a window popping up on a website that says it has detected malware on your PC and to click the box to fix it. Don't believe it. Trust your own anti-virus program. Clicking the box will just download trojans and fake anti-virus programs that take your money and infect you at the same time. Don't even click the box to close it. The safest way to exit if you see a message like this is to immediately close your browser (Big X in the upper RH corner of the browser window), and then run your own Anti-virus program.

AD-AWARE AE 2009 TIPS: (Note: I no longer recommend Ad-Aware. I experienced too many conflicts with other programs, plus other issues.)

AUTOPLAY~AUTORUN DISABLE: Autoplay~Autorun is a big PC vulnerability: Since Autoplay allows code to be immediately executed upon insertion of the media (CD/DVD, FLASH drive, EXT-HDD, FLOPPY, etc), malware can infect your PC before any action can be taken. Autoplay should be disabled for all removable devices:

- Windows 7: Go to (*Control Panel > Hardware and sound > Autoplay*) and un-check the box for: Use Autoplay for all Media and devices". Click "Save".
- XP: The simplest way to do this for XP is to download and install the "Tweak UI" utility (free from Microsoft), then use it to disable Autoplay for all drive types. "Tweak UI" works for all versions of XP.
 - 1) Download and install "Tweak UI"
<http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx>
 - 2) Open "Tweak UI".
 - 3) In the left-hand column, click: (*the + in front of My Computer > the + in front of Autoplay > then Types*).
 - 4) *Uncheck the boxes* for " Enable Autoplay for CD and DVD drives" and " Enable Autoplay for Removable drives".
 - 5) Click OK to exit TweakUI.

- XP: The following manual methods also work, but require you to edit Group Policies or the Registry.
 - ◆ XP Pro: <http://www.howtogeek.com/howto/windows/disable-autoplay-of-audio-cds-and-usb-drives/>
 - ◆ XP Home: <http://antivirus.about.com/od/securitytips/ht/autorun.htm>

AVAST! Home 4.8 Free

- Avast is the only free AV that still supports Windows 98 and has automatic updates and real-time protection.
- You have to request a Registration Key via email once a year to keep it running.
- For a better user interface, download the "Flat'n'Simple " skin from: <http://www.avast.com/eng/flatnsimple.html>
- It offers real time protection and automatic updates, but will not do an automated scheduled scan. You can trick it to do scans by using the XP Task scheduler to run this task:
 "C:\Program Files\Alwil Software\Avast4\ashQuick.exe" C: as a task. For details, see:
<http://forum.avast.com/index.php?board=2%3Baction=display%3Bthreadid=3796>

AVG FREE 9 SET-UP & TIPS

(This setup was tested with AVG Free version 9.0.686)

Version 9 is an Anti-malware suite and not just an Anti-virus. AVG does not play well with Ad-Aware or previous versions of any AVG Products. Before installing AVG, you should remove all other AVG products. Here is a link to the **AVG 8.5/9.0 USER MANUAL** download: http://www.avg.com/filedir/doc/AVG_Anti-Virus/avg_aav_uma_en_85_3.pdf and a link to a quick **AVG 8/9 TUTORIAL**: See <http://www.mesasos.com/avg8.htm>

INSTALL & SETUP:

- Just download the install file and double-click the downloaded file.
- When asked to install the AVG Security Toolbar, I recommend unchecking the box (No). If you say Yes to the Toolbar, then I do not currently know how to remove it. Probably in Add/Remove Programs.
- When asked to Register your AVG, you can do so or just click Next to skip it.
- SETTINGS:** (*Tools > Advanced Settings*) (NOTE: I use all DEFAULT settings, except for the following items.)
 - VIRUS VAULT:** This is where you can alter the default settings for managing the Vault. I leave the defaults: "Max Size = 10%" and "Automatically delete files over 90 days old".
 - LINK SCANNER:** (*Tools > Advanced Settings > LinkScanner*). (Also called "Safe Search"). When browsing with Firefox or IE, this item warns you of potentially malicious websites. It can slow down your browsing experience, but is very beneficial. I recommend checking both " Enable AVG Search-Shield" and " Enable AVG Active Surf-Shield".
 - SCANS:**
 - Scan whole computer: Uncheck " Automatically heal/remove infections", and check the following: " All file types".
 - Shell Extension Scan: Uncheck " Automatically heal/remove infections", and check the following: " All file types".
 - Scan specific files or folders: Check " Automatically heal/remove infections", and check the following: " All file types".
 - Removable Device scan. (Off by default) Check the " Enable Removable Device Scan box and check " Automatically heal/remove infections". This activates a feature that disables autorun/autoplay and scans every device that you plug into the PC (USB Drives, Flash drives, camera cards, etc). This protects you from infections from other people's Infected Flash drives or other USB devices. I recommend activating this feature. It does slow things down though. **WARNING: Do not unplug a USB Drive while this scan is running on it!**
 - SCHEDULES :** (*Tools > Advanced Settings > Schedules*)
 - SCHEDULED SCAN:** (*Tools > Advanced Settings > Schedules > Scheduled scan*).
 - "Schedule settings" Tab:
 - Schedule running: Set up your desired scan schedule. I suggest setting up a weekly scan by choosing "Selected Days" and checking just one day during the week. Also, choose a time.
 - I prefer to un-check the box: " Run on computer startup if task has been missed".
 - Make sure you check the box for " Enable this task".
 - If you do not want an automatic scheduled scan, then uncheck the box: " Enable this task."
 - "How to scan" Tab:
 - Select desired options: I un-check the following box: " Automatically Heal/remove infections". I do check the following: " All file types". I leave all the other boxes checked.
 - Choose a "Scan process priority". Note: "Fast Scan" runs faster and uses more computer resources, while "Slow Scan" runs slower and uses less resources.
 - "What to scan" Tab:
 - Choose to either scan the whole computer or specific Drives and Folders.

ANTI-MALWARE TOOLS & TIPS



- b. VIRUS DATABASE UPDATE SCHEDULE: (*Tools > Advanced Settings > Schedules > Virus database update schedule.*)
 - 1) Schedule running: The Free AVG only allows a daily check, but you can choose the time of day.
 - 2) Advanced schedule options: Check the box " Run on computer startup if task has been missed".
 - 3) Task settings: Make sure the box is checked for " Enable this task".
 - 4) Other update settings: " Run the update again as soon as the Internet connections are available.
 - c. PROGRAM UPDATE SCHEDULE: (*Tools > Advanced Settings > Schedules > Program update schedule.*) I suggest setting this up exactly the same as the above "Virus database update schedule".
 5. E-MAIL SCANNER: (*Tools > Advanced Settings > E-mail Scanner.*)
 - a. Look under "Check incoming e-mail and UN-CHECK the box: " Certify mail"
 - b. Un-check the box: " Check outgoing e-mail". (The status of Certify does not matter here).
 - c. Click APPLY, then OK if you are exiting.
 6. RESIDENT SHIELD: (*Tools > Advanced Settings > Resident Shield.*)
 - a. Make sure the box is checked for " Enable Resident Shield.
 - b. Choose the items you want protected. *Remember that each item selected slows your PC down a little more.* " Scan for Tracking Cookies" should be un-checked: This is good to activate ONLY if you have a really fast PC, otherwise it will slow your browsing down a bunch.
" Auto-heal" should be un-checked: *I NEVER recommend "Auto-heal". I like to know when an anti-virus is going to delete something.*
 - c. In the LH column, click "Exceptions". Here is where you can add Exception paths for drives or folders that you do not want continuously protected by the Resident Shield. I usually create exceptions for all drives (except drive C) and for my Wordprocessing document folder. This helps keep AVG from slowing down my old PC too much. *NOTE: This does not affect the scheduled or manual scans.*
 7. UPDATE: (*Tools > Advanced Settings > Update.*)
 - a. Make sure the following boxes are set as shown:
 - Update immediately
 - If computer restart is required:
 - require confirmation from user.
 - Require confirmation to close running applications.
- E. **DO THE UPDATES:** From the AVG main window, click the "Update now" Button. Keep doing the updates until you see the message: "No new update files are available".
- F. **OVERVIEW WINDOW:** On the AVG Overview window, make sure all the components have green checks.
- G. **RUN A MANUAL SCAN:**
To run a full scan, click the Computer Scanner button and click "Scan whole computer". At the end, you will get a "Scan results" window.
- Warnings: If you get Warnings, go to the "Warnings" Tab after a scan and click "Remove all unhealed infections", the Warnings seem to always go to the Vault. There is a column on the right side of the window that says: "Result" Moved to Virus Vault. (To see it, you may have to make the AVG window full size or use the horizontal scroll bar.)
- Infections: If the scan detects an infection of some kind, you are asked if you want to Delete, Ignore, or Move to Vault. See the "Infections" Tab.

NOTES ABOUT AVG:

RUNNING "AVG" ALONG SIDE "MSE". If you want run AVG to use features like the Link scanner and email scanner that are not in MSE, you need to disable the real-time protection in AVG so it will not conflict with MSE.

- 1) (*Tools > Advanced Settings > Resident shield.*) Un-check the box to Enable Resident Shield.
- 2) (*Tools > Advanced Settings > Ignore Faulty conditions.*) Check the box for Resident Shield

VIRUS VAULT: (AVG calls Quarantine a "Vault". There are two ways to view the Vault. 1) *Click: History > Virus Vault,* 2) *Click: Computer Scanner > View Virus Vault.* (By default, the Vault deletes its contents after 30 days)

EVENT HISTORY: AVG logs everything that it does. To see the Event Log: *Click: History > Event History Log.*

SCAN RESULTS: The "Results" Window for any past scan can be viewed two ways. First, 1) *Click: History > Scan results* or 2) *Click: Computer Scanner > Scan history,* then double-click the desired Scan entry. (*Note: Automated/scheduled scans do not give a "Results" window at the end of a scan unless something bad is found and "Automatically Heal" is turned off.*)

RESIDENT SHIELD DETECTIONS: To view the problems detected by the Resident Shield: *Click History > Resident Shield detection.*

WARNINGS vs INFECTIONS: This is pretty vague to me. Read the User Manual for some details. User Manual download: http://download.avg.com/filedir/doc/AVG_Free/user_manual/avg_afe_uma_en_80_8.pdf

IF YOUR PC RUNS SLOW: If you have an older PC and you think AVG 8.0 makes it run too slow, try disabling the "Resident Shield" and/or the "Link Scanner" by unchecking the boxes in Item 7 and Item 1 above. To make these changes invisible, go to (*Tools > Advanced Settings > Ignore Faulty Conditions*) and check the boxes for the disabled features. Also make sure the you schedule the weekly scan at a time when you are not using the PC. Especially make sure the Resident Shield is NOT set to "Scan for Tracking cookies".

AVG / SITE ADVISOR WARNING (Firefox and IE): McAfee Site Advisor does not always play well together with the AVG Link Scanner (Safe-Search). For McAfee Site Advisor to co-exist properly with AVG Safe Scan, they need to be installed in the following sequence. 1) Firefox, 2) AVG 8.0, then 3) Site Advisor. If SA or AVG is already installed, they will have to be removed and reinstalled (Add/Remove Programs). If you still have problems with the browser notification icons overlaying each other, I suggest you just remove Site Advisor.

NOTIFICATION WINDOW (RE: AVG PRO & AVG INTERNET SECURITY): When running AVG, you will constantly see a "Notification" at the bottom of the window that tries to scare you into upgrading to the paid "Pro" or "Internet Security" versions. In my opinion, the Free version of AVG gives you adequate protection. I have not found a way to make this window go away permanently.

AVG FREE vs AVG PRO vs AVG INTERNET SECURITY: Here is the feature comparison chart (Free vs Paid versions) to help you decide if Free is good enough: <http://free.avg.com/download-avg-anti-virus-free-edition>

AVIRA ANTIVIR PERSONAL Free - TIPS (ref: version 9)

- **INSTALL:** Note: By default, Avira runs a resident shield and daily auto updates, but is not set up to do a scheduled System Scan. After first installing Avira, go through the following steps to set up a scheduled scan:
 1. Click "Administration" > Scheduler, then verify that daily updates are scheduled.
 2. Right-click "Complete System Scan" > *Edit Job > Next > Next. Verify that it says Local Hard Disks > click Next.* Set up a weekly schedule with a preferred day and time. Check "Repeat job if time has expired" > click Next > Choose a preferred display mode for the auto scan > Click Finish.
 3. Make sure the "Activated" box is checked under Complete System Scan.
 4. Other settings can be default.
 5. Click "Overview". Keep clicking "Start Update" until the message "Your program is up to date" appears.
- I have not found a way to remove the Avira "NAG" Screen on version 9.x. This tip is for version 8.x: http://www.elitekiller.com/files/disable_antivir_nag.htm

COMBOFIX Notes:

Using the Console with Combobox: <http://www.bleepingcomputer.com/combobox/how-to-use-combobox>

Using the Windows Recovery Console: <http://support.microsoft.com/kb/314058/>

Obtaining the XP Recovery Console from Microsoft: <http://support.microsoft.com/kb/310994>

FIREFOX: Enhanced browsing security add-ons

- LinkExtend <http://https://addons.mozilla.org/en-US/firefox/addon/10777>
LinkExtend help <http://www.linkextend.com/help/> See my Firefox Tips for details
- NoScript <http://https://addons.mozilla.org/en-US/firefox/addon/722>

MICROSOFT SECURITY ESSENTIALS (MSE)

Microsoft has finally released their long-awaited free full-function anti-malware program (September 2009). Microsoft Security Essentials (MSE) offers real-time protection, automatic updates, and scheduled scans. MSE works with XP, Vista, and Windows 7.

- **GENERAL INFO:**
 1. **REAL-TIME PROTECTION:** Once MSE is installed you can basically forget about it as long as you keep your Windows Updates current. So far, it appears that the MSE's full-time protection does not significantly slow down your PC like most other anti-malware programs do.
 2. **AUTOMATIC UPDATES:** It seems that no matter how you have your Windows "Automatic Updates" set, MSE has a mind of its own and keeps itself up-to-date as long as you are connected to the internet.
 3. **AUTOMATIC SCANS:** MSE can automatically run a scan either daily or weekly (not Monthly). By default, MSE runs a scan once a week. You can pick the day and time, change it to daily, or turn off the scheduled scan completely. Also, you can pick whether the scheduled scan is a "Full Scan" or a "Quick Scan".

ANTI-MALWARE TOOLS & TIPS



4. **EMAIL SCANNING:** Although MSE is a complete basic anti-malware solution, it does not include an e-mail scanning feature as do many commercial A/V suites. Be aware of this if you decide to make MSE your only anti-malware solution. This is less important today since most e-mail providers do a good job of scanning e-mails and attachments for malware. *Read my article "A STRESS FREE PC" for ideas on protecting your e-mail.* If you decide to keep your old anti-virus, remember that running multiple programs that continuously scan in the background slows your PC down (a lot).
 5. **BROWSING PROTECTION:** MSE does not have a built in link-scanner (safe-search browsing protection). If you have removed a previous anti-virus suite that did provide a link scanner, I suggest you instead use the free McAfee Site Advisor for IE or one of the free Firefox add-ons (like LinkExtend). Another alternative for browsing protection is a free program called "SpywareBlaster". Also, don't forget that Internet Explorer (IE7 or IE8) now has many built-in protections as does Firefox. .
 6. **MSE SCANS:** Both the "Quick Scan" and the "Full Scan" run slower and longer than most other anti-malware program scans, but MSE is very thorough. So far, the scans do not seem to slow the response of other programs to user input as much as other anti-malware scans do.
 7. **RUNNING MSE ALONG WITH OTHER ANTI-MALWARE PROGRAMS:** Microsoft claims that MSE does not compete with other 3rd party anti-malware programs, but when you go to install MSE, a window tells you to remove all other anti-malware programs before continuing with the install. I can say without a doubt, that multiple programs running real-time protection will slow down your PC as well as cause possible conflicts. If you insist on using another A/V program along with MSE, my suggestion is to disable the Resident (real-time) protection in the other A/V program and leave the MSE real-time protection running.
 8. **MSE & WINDOWS DEFENDER:** MSE includes all the features of Windows Defender, so if you currently have Windows Defender installed, I suggest that you remove it before installing MSE.
 9. Get the free download of MSE and read more about it at: http://www.microsoft.com/security_essentials/
- **DOWNLOAD MSE:**
 1. On the Microsoft Security Essentials Home page, click the <Download Now> button.
 2. Click the <Download> button and save the "mse installer" file.
 3. Close your Browser.
 - **INSTALL MSE:**
 1. Double-click the downloaded "mse installer" .exe file. Click <Next>, Then <Validate>. If you are not a pirate or a criminal, you will be at the License Agreement screen.
 2. Click "**I accept the terms....**", then click <Next>.
 3. Click "**Complete**". Click <Next>, then click <Install>.
 4. You can choose to "Check for definitions and run a quick scan now" or not. Your choice. Click <Finish>.
 - **CONFIGURE MSE:**
 1. The default setup is an Automated Weekly scan. To change this; (*Settings tab > click Scheduled scan*). Then set up your Automatic Scanning as desired.
 2. Unless you are an expert, leave all the other settings at default. Click <Save changes> to exit.

ONECARE LIVE PROTECTION SCAN (On-line Scan)

- This on-line scanner uses an Activex add-on for Internet Explorer. It must be run from IE and not Firefox.
- For details on installing and running this scanner, see my article called: "Free Anti-Malware Tools from Microsoft" at www.jimopi.net.

SECUNIA SOFTWARE INSPECTOR - OVERVIEW

Secunia PSI (Personal Software Inspector)

- **ABOUT PSI:** This free scanner does a very thorough job of assessing many programs on your PC for vulnerabilities. Secunia PSI scans for the latest updates from Microsoft, Adobe, Apple, Skype, and many other companies.

- FIRST-USE SETUP: 1) Click Advanced (upper RH Corner of PSI window), 2) On the "Settings" tab, UN-check the box for " Start the Secunia PSI on boot". Leave it in Advanced Mode.
- CLOSING PSI: You must right-click the Secunia PSI Icon in the taskbar, click exit, then Yes.
- CORRECTING ISSUES:
 1. PROGRAM UPDATES AVAILABLE: When a program is flagged as "Insecure" or at "End-of-life", the error includes a link to the site where the update is located. If the link is blue, you can click the link. If it is black, you must update manually. Some programs can be updated, & others must be removed using Add/Remove Programs and replaced with a newer version. Note: These Blue update link buttons do not always do the job. *Personally, I prefer updating programs from inside the program itself, usually by clicking Help > Check for updates.*
 2. MICROSOFT OFFICE UPDATES: The Blue update link buttons frequently fail to update Microsoft Office products. To update Microsoft Office, see my XP TIPS sheet under: MICROSOFT OFFICE UPDATES.
 3. NO PROGRAM UPDATES AVAILABLE: If a needed program that is shown as "Insecure" or at "End-of-life" has no free updates (IE: Power DVD) and you do not want to pay for a newer version, you can set PSI to just Ignore it. Open the error listing and click the "Ignore Program" Icon. If you don't need the program, I suggest removing it with Add/Remove Programs.
 4. DELETING OLD PROGRAM FILES: Always try to first remove "Insecure" or "End-of-life" Programs using Add/Remove Programs. If PSI shows a program as "Insecure" or "End-of-life", and it is not listed in Add/Remove Programs, then you can safely just delete the offending file. On the right side of the error listing, click the "Folder" Icon and delete the specific file (IE: Flash.ocx)
 5. "FLASH" UPDATES: When you update FLASH to a higher version, residual files are usually left on the machine by the Adobe installer. To the Secunia Inspector, these files look like down-level versions of FLASH that are still actively running on your PC. You must manually find and delete the old files as shown above. Also, be aware that there are two different versions of FLASH on a typical PC. One for IE (ActiveX) and one for FIREFOX (General Plugin). To install the correct version, go to the adobe.com website using the desired browser to download and install the correct FLASH. After that, track down and delete all the old versions using the Secunia error message. You can also use the "Flash Player Uninstall" Tool to remove all old versions of Flash. See: http://kb.adobe.com/selfservice/viewContent.do?externalId=tn_14157
 6. "JAVA" UPDATES:
 - a. First, look in Add/Remove programs for all versions of JAVA and remove all but the latest one. There may be Microsoft JAVA (*Look under "M"*), and SUN JAVA (*Look under "J"*), or it may be listed as JRE (*Java Runtime Environment*).
 - b. In the past, when a new version of JAVA (jre) was installed, residual files and folders from old versions of JAVA were frequently left behind by the SUN installer. Java version 6u11 and newer seems to have fixed this issue.
 - c. After installing the latest JAVA update, if PSI tells you old versions still exist, you must first try to remove them using Add/Remove programs then you can manually delete the folder for each old version as shown above. (*Usually they are in C:\Program Files\Java\jre...*). *Both XP & Windows 7 should be the same.*
- ERROR 1920: If you get error 1920 on startup of Secunia PSI, reset the security settings for Internet Explorer back to "Default" and try again. (*Control Panel > Internet Options > Advanced tab > click the "Reset..." button*).

Secunia OSI (Online Software Inspector) http://secunia.com/vulnerability_scanning/online/

- Secunia.com offers a free on-line scan of your PC to ensure that many popular User Application Programs are at the latest available levels to minimize your vulnerability to malware. NOTE: There is no software to install on your PC. Secunia runs from your Web Browser.
- From the secunia.com homepage, click "Scan Online" in the LH column.
- The Online Software Inspector requires that you have the latest version of Java (or jre = java runtime environment) or the "Start Now" button will fail or hang up. To fix this, remove Java, then Google GET JAVA to go to the correct site. (<http://www.java.com/en/download/index.jsp>).
- At the end of the scan, Secunia offers to notify you by email if any of the software it scans has new updates. (*I recommend signing up for that*)
- NOTE: Many of the tips for the Secunia PSI (above) also apply to the Secunia OSI. PSI is way better.

SPYBOT SEARCH & DESTROY TIPS

- To stop those nagging messages to "approve or deny Registry changes", turn off "TeaTimer" by doing the following:
 1. First, you should be running Spybot version 1.6.2 or higher. If not, remove Spybot and install the latest version.
 2. Open Spybot, then click: *Mode > Advanced mode > Tools (LH column) > Resident (LH Column)*. In the "Resident" window, UNCHECK both: " Resident SDHelper" and " Resident TeaTimer"
 3. If desired, you can go back to basic mode by clicking (*Mode > Default mode*).
 4. Close SpyBot.
- With both VISTA and WINDOWS 7, Spybot must be run in "Administrator mode".
- IE8: SpyBot is not compatible with Internet Explorer 8 and should be removed if you have installed IE8.

SUPERAntispyware Notes:

- This program is a great scanner, but the free version does not have real time protection.
- SYSTEM & BROWSER REPAIR TOOLS: *Click Preferences > Repairs tab > Select item > click Perform Repair.*
- ON-LINE SCAN: This is actually a downloadable standalone scanner that does not need to be installed on the infected system. If the infected system can go on the internet, download the latest version of the "SAS_nnnnnn.exe" file and run it. If not on the internet, then download it to another PC and burn to a CD or write protectable flashdrive. Run it from that. *Note: Each time you download it, the file name is different. This is to confuse the hackers.* <http://www.superantispyware.com/onlinescan.html>
- UBCD4WIN: SUPERAntispyware is included in the UBCD4WIN CD package and can be updated before scanning if you have Networking enabled.

WINDOWS DEFENDER TIPS:

- **NOTES:**
 - ✓ Defender is built into Vista and Windows 7, but is available as a download for XP.
 - ✓ All of Defender's features are included in the "Microsoft Security Essentials" (MSE) program (release in Sept 2009), so Defender should be removed before installing MSE.
- **DOWNLOAD DEFENDER:**
 1. On the Microsoft Windows Defender Home page, click the <Get it now> button.
 2. Click the "Continue" button (next to "Validation Required")
 3. **FIRST TIME:** If this is the first time you are downloading software from Microsoft, you will be at a WGA Validation screen of some kind.
 - a. **FIREFOX:** "WGA Plug-in installation" page: Click "Download Plug-in" > Click "Save File" > Close Firefox. Double-click the downloaded file: "WGA PluginInstaller.exe". When done, re-open Firefox, then go back to Step "1" and start over.
 - b. **INTERNET EXPLORER:** Genuine Windows Validation Component install page: Click the <Install> button. If you get a pop up stopping the install, click the yellow bar at the top of the web window and click "Allow Install". When done, continue with step 4.
 4. Click the <Download> button and save the "WindowsDefender.msi" file.
 5. Close your Browser.
- **INSTALL DEFENDER:**
 1. Double-click the downloaded "WindowsDefender.msi" file. Click <Next>, Then <Validate>. If you are not a pirate, you will be at the License Agreement screen.
 2. Click "**I accept the terms....**", then click <Next>.
 3. Check "**Install definition updates only**", then click <Next>.
 4. Click "**Complete**". Click <Next>, then click <Install>.
 5. You can choose to "Check for definitions and run a quick scan now" or not. Your choice. Click <Finish>.
- **CONFIGURE DEFENDER:**

1. The first thing I like to do is copy the "Windows Defender" Icon from the Start > "All Programs" menu, then paste onto the Desktop, so I can find it easily.
2. The default setup is an Automated Daily scan. To change this; (*click Tools > Options*). Then set up your Automatic Scanning as desired. Unless you are an expert, leave all the other settings set as default. Click <Save> to exit.
3. Note: A "Full Scan" hangs up on some machines while scanning Archive files. Try a full scan first, but if it hangs, stick with the "Quick Scan" for your system. To select Quick or Full, click the little down arrow to the right of the "Scan" button (on the Defender "Home" screen).

REMOVING COMMERCIAL ANTI-MALWARE SUITES

- APPREMOVER (from OPSWAT.COM) <http://www.opswat.com/appremover/AppRemover.exe>
- AVG REMOVER: <http://www.avg.com/download-tools>
- AVIRA ANTIVIR REMOVAL TOOL http://www.avira.com/en/support/support_downloads.html
- CA (Computer Assoc's): Go to <http://support.ca.com/irj/portal/anonymous> and search for TEC481327
- CA: eTrust Antivirus 7.x <http://supportconnect.ca.com/sc/kb/techdetail.jsp?searchID=TEC436187&docid=436187&bypass=yes&fromscreen=kbresults>
- Kaspersky Products Removal: <http://support.kaspersky.com/faq/?qid=208279463>
- McAfee Consumer Removal Tool = MCRT: <http://service.mcafee.com/FAQDocument.aspx?id=TS100507> or http://download.mcafee.com/products/licensed/cust_support_patches/MCPR.exe
- Microsoft MSI cleanup utility: <http://support.microsoft.com/kb/290301>.
- Norton Removal Tool = NRT: After removing all Norton Products from Add/Remove Programs, download and run the NRT. <http://service1.symantec.com/Support/tsgeninfo.nsf/docid/2005033108162039>
Note: If you are unable to remove Norton because you need a password, download the "Cleanwipe" Utility. Use caution.
- SUPERAntispyware: <http://www.superantispyware.com/downloads/SASUNINST.EXE>
- Threatfire Removal tool: [http://www.threatfire.com/files/RemoveThreatFire\(3.0\).zip](http://www.threatfire.com/files/RemoveThreatFire(3.0).zip)
- Trend Micro or PC-cillin: <http://esupport.trendmicro.com/Pages/How-do-I-remove-old-or-new-versions-of-Trend-Micro-products-in-my-comp.aspx>

HIJACKTHIS (overview)

- HijackThis is a Utility that scans your PC and creates a report listing important information about settings and processes running in your computer.
- Experts are available in online Forums to help you interpret & analyze the report. Hopefully they can help you find & remove the malware in your computer.
- This is the last resort before formatting your hard-drive and re-installing Windows from scratch. It is assumed that all you have tried all other Utilities to remove the malware.
- Removing malware this way is very complex and should only be done on advice from knowledgeable people.
- If you Google "HijackThis", you will find many, many resources to help you.
- Trend Micro bought this Utility in 2007 and continues to make it available for free, but they do not help you analyze the results of a scan or guide you on what action to take.
- The Trend site does give instructions on downloading and using HijackThis. *See the section above on "Virus, Spyware & Rootkit Tools" for the link to trendsecure.*
- After creating your Report, Google: "hijackthis forum" (no quotes) to find people to help you. Log into some of the forums that turn up and ask for help. Here are a few example Forum sites: <http://www.hijackthis.de/> or <http://www.bleepingcomputer.com/> or <http://www.castlecops.com/> or <http://help.lockergnome.com/general/HijackThis-Logs-forum-48.html> or <http://hjt.networktechs.com/>

VIRUS ~ SPYWARE ~ MALWARE REMOVAL GUIDE FOR XP

These Step-by-Step ideas & advice are for use on a system that is infected with malware. If the system does not allow you to complete a step, continue on with the next step. Be sure to do all the tasks that are **BOLD**.

See the video podcast at: <http://www.technibble.com/categories/video-podcasts/> for a virus removal tutorial, and this video from Microsoft: <http://www.microsoft.com/emea/spotlight/sessionh.aspx?videoid=359>.

For ideas, go to this site: <http://www.bleepingcomputer.com/>. Go to the site search box, select "Search BC" and then enter the name of the malware you are trying to remove in the search box.

NOTE: Be sure to run all BOLD steps to make sure the malware is really gone.

- a. **IF PC WILL NOT BOOT, OR THE PC DOES BOOT, BUT DOES NOT RESPOND:**
 - 1) Go to the safe-mode boot screen (F8, F8, F8), and select boot to "Last Known Good Configuration".
 - 2) If you still cannot boot the system, boot a UBCD4WIN CD and try Restoring the System to an earlier time with the EZPCFIX Utility. If you do not have this CD, continue on.
 - 3) If you still cannot boot the system or the system does boot, but is non-responsive, then download & burn a KASPERSKY RESCUE CD or AVIRA RESCUE CD on another PC. Boot the CD and run scans against the system's hard-drive. (Personally, at this point I use the UBCD4WIN CD and then run SUPERAntispyware and the other anti-malware programs available on it.)
 - 4) If you are short on Support Tools, you can install the hard-drive as a slave drive in a good PC and run anti-malware scans on it from there. (WARNING: This is very risky and can spread the infection!)
- b. **IF PC SHUTS DOWN AND/OR REBOOTS ON ITS OWN**, before you can troubleshoot: This can be the result of a rootkit. If you get a shutdown warning, quickly do a (Start > Run > shutdown -a > "OK"). This will abort the shutdown and give you time to run "combofix", then continue with this list.
- c. **SYSTEM RESTORE:** If the system will boot and respond either in Normal or Safe-Mode, try doing a System Restore to get the system back to where the malware is not active. **Whether or not this helps, now is the time to TURN OFF SYSTEM RESTORE and continue with the next steps.**
- d. **REMOVE SCHEDULED TASKS:** Remove any tasks that you do not understand. (Control Panel > Scheduled Tasks)
- e. **MALWARE REMOVAL PROGRAMS:** (If possible, do these steps, then continue). If the malware prevents the installation or running of these programs, re-boot the machine, then rename the ".exe" of the desired program and try running it again. (NOTE: You may have to download these programs on another PC).
 - 1) If not already done: Download, install, update, and run the Microsoft Security Essentials.
 - 2) Download the latest version of the standalone SuperAntispyware program and run it. (Note: It does not need to be installed). If the system will not let you do this, download it on another PC and put it on a CD or write-protected flashdrive, then run it.
 - 3) Install & run MalwareBytes Anti-Malware (MBAM). If you cannot do this, try killing processes with "RKILL" and trying again. If SUPERAntispyware or MBAM still will not run, continue with the next step.
 - 4) Download and run the latest version of the Kaspersky Virus Removal Tool. (See my link above).
- f. **SMITFRAUDFIX & COMBOFIX:** FIRST record the name of the Desktop background image file and the IE Homepage URL/s so they can be restored after running these programs. Also, first disable any real time anti-malware program processes. For details, see: <http://www.bleepingcomputer.com/forums/topic114351.html>
 - 1) **SMITFRAUDFIX:** Be sure to download the latest version. Run SmitFraudFix and do the following steps in Safe-Mode (Safe-mode = press F8, F8, F8..... when first turning on the PC):
 - a) First run option 2 = Clean files & registry, Y; then option 3 "delete trusted zone", Y; then Q for quit).
 - b) Now do a restart and let the system boot back into regular mode.
 - 2) **COMBOFIX:** Be sure to download the latest version. See my notes above for help with COMBOFIX. (Note: COMBOFIX auto-reboots at the end of the run).
- g. **CLEAN "TEMP" FILES:** Complete these tasks for EACH user on the PC. (Optionally, the "TFC" Temp File Cleaner Utility cleans the temp files for all users at once and saves doing steps 1 & 2 below).
 - 1) Make a list of all User Accounts on the PC. From any "Computer Administrator" level Account: (Right-click My Computer > Properties > Advanced tab > User Profiles "Settings" button).
 - 2) **CLEAN EACH USER ACCOUNT:** Log on to each User Account (including the "administrator" account) and run the following items:
 - a) **TEMP FILES:** Click Start, run: %temp% and delete all the files listed.
 - b) **CCLEANER:** Run the CCleaner Utility (with all boxes checked) to clean out more temporary files, then run the Registry cleaner portion of CCleaner. (Glary Utilities is also a good program for this).
- h. **INTERNET OPTIONS** Clear and Reset (Do this for each user):
 - 1) (Control Panel > Internet Options > Security tab > Trusted Sites > Sites). Delete all Trusted Sites
 - 2) (Control Panel > Internet Options > Advanced tab). Click "Reset.." (Note: The Home page/s may be lost)

- i. **SCANS & TASKS:** Install and run the following free programs in Regular Mode. If Regular mode is inaccessible, try Safe-Mode (press F8,F8,F8..... when first turning on the PC):
- 1) **DIAL-A-FIX:** If available, run DIAL-A-FIX to fix any damaged system files. especially if Windows Update will not work. Run it with all boxes checked. Then scan for restrictive Policies with the "Hide disabled policies" un-checked. (*Dial-a-Fix is only for experienced technicians*).
 - 2) **STARTER:** Run Codestuff Starter and stop any "unusual" programs, processes, or services from automatically starting during Boot. (*Do not stop any "Microsoft Services"*.)
 - 3) **RE-SCAN:** Again, run full-scans of your preferred (and updated) Anti-virus, and Microsoft Security Essentials and any other desired Programs (even if you have already run them) (*see above in the Malware Tools section*).
 - 4) **SCHEDULED TASKS:** Check again for any that do not belong: (*Control Panel > Scheduled Tasks*).
 - 5) **TEST IE.** If it does not work correctly, again reset it to factory defaults: (*Control Panel > Internet Options > Advanced tab > click "Reset..."*). If IE still does not work, run the "Fix IE" Utility program.
 - 6) **ONECARE SCAN:** Do a free on-line scan from Microsoft called Windows OneCare Live Protection Scan (*You must use Internet Explorer, no other browser will work*). **NOTE:** This scan runs a long, long time.
 - 7) **MSRT:** Run the Microsoft MSRT (Malicious Software Removal Tool) FULL SCAN, after downloading the latest version from Microsoft. (*Start > Run > MRT*) Note: Verify the Tool's version date on the title bar.
- j. **SAFE-MODE:** If you are stuck, some technicians recommend trying all the above steps in Safe-Mode. (*You can get to Safe Mode by pressing F8 (many times) when you first turn on the PC*).
- k. If malware is detected, but cannot be removed, write down the exact name (and syntax) of the malware detected. Then Google search using the keyword "removal" plus the specific name of the malware for ideas on how to remove it. The most well known commercial anti-malware sites all have individual removal tools available. (Usually for free). You should use these sites to get a removal tool or you may download a new infection. Also, check out www.download.com to see the ratings of various removal programs. Warning: Some programs come with a free trial & will detect for free, but you have to buy it to remove the malware. Read carefully before spending any money as most good removal tools are free.
- l. **NOTE:** If you are unable to install or run your tools, try the TDSS Killer Program or check out this process from Malwarebytes.com (Re: The "Antivirus 2009/2010" virus). 1) Boot to Safe Mode. 2) Open Device Manager & click View > Show Hidden Devices. 3) Under Non-Plug and Play Drives, disable (not remove) "TDServ.sys" and anything else beginning with "TDSS". 4) Reboot in Safe Mode and you should be able to install your favorite tools. If not, rename your desired Tool's install exe file & try again.
- m. If there is still suspect malware on the PC or if none of the removal tools will run, try Trojan Remover, RogueFix, Rootkit Revealer, and the other tools listed in the ANTI-MALWARE TOOLS section. *Again, you may have to rename the ".exe" program files to get them to run.*
- n. Try the "HijackThis" Utility from Trend Micro. The Trendmicro site tells you how to download and use the program. Also, see the "HijackThis Overview" in this document.
- o. If none of the above tools can remove the malware, you will have two choices: 1) Restore your system from a full image backup taken prior to the malware, or 2) Do a "Nuke & Pave" (*This involves saving all your personal data and e-mails to a CD/DVD or Flashdrive, re-formatting your Hard-drive, and reinstalling Windows from scratch. This includes re-installing all of your application programs*). Before you shutdown the system, see my Tips sheet on "Backing Up Your Personal Data". **WARNING:** Malware can follow your personal data files.
- p. For more ideas, see the Malware Removal Guides from majorgeeks.com and gemstatecomputers.com:
<http://forums.majorgeeks.com/showthread.php?t=35407> and from
<http://docs.google.com/Doc?docid=0AaqZNZywWLNIZGc1cHZjZ2NfMGc0N2ZucWNw&hl=en>
- q. **SECUNIA PSI:** Once all is back to normal, make sure all the Windows Updates are installed, then test your system for vulnerabilities by downloading, installing, and running the "Secunia PSI" program.
- r. **CLEAR SYSTEM RESTORE HISTORY.** At this point, be sure to turn off Windows "System Restore" and then turn it back on. *This will remove old Restore Points that may still contain some malware.*
- s. **Add the WOT** (Web Of Trust) add-on to all browsers to help the user browse more safely.

Special thanks to Stephen Cherubino (www.podnutz.com), Mike Smith (www.miketechshow.com), and Bryce Whitty (www.technibble.com) for many ideas that helped me complete this guide.