My Advice for Avoiding Malware Infections ©

Jim McKnight www.jimopi.net AvoidMalware.lwp revised 4-6-2014

This sheet is for the many people who have asked me what the minimum is they should do to keep their PC from getting infected and feel safe. First of all, realize that NO anti-malware program gives complete protection. This is especially true when users get fooled into clicking a box that gives permission for malware to install itself. Currently, all available paid and free AV Suites only give 80-90% protection. So here are some processes you can put in place to improve your chances of keeping your PC clean:

- First, be sure to read my "A STRESS FREE PC" article for an overview of ideas to help secure your PC and your data. It is on my website at www.jimopi.net**.**
- **WINDOWS UPDATES**: *Keeping Windows and all Microsoft programs up to date is the #1 most important protection from malware vulnerabilities*
  1. AUTOMATIC UPDATES: Be sure Windows Update is set to “Install Updates Automatically”.
  2. MICROSOFT UPDATE: Be sure Windows Update is set up to include the “Microsoft Updates”. This updates all Microsoft programs and utilities *(like Office, .Net, Silverlight).*
  3. MANUAL UPDATES: Manually run Windows Update from time to time to make sure any desired “Optional Updates” are installed.
- **MY RECOMMENDED LIST FOR PROTECTION AGAINST MALWARE**: For ordinary operating & browsing conditions, here is my recommended mix of FREE protection programs to have running:
  1. SANDBOXIE: The best single thing you can do is to install Sandboxie and use it EVERY TIME you browse the internet. If you get tricked into installing malware on your PC, it will go away when you close Sandboxie. Some websites can install malware just by visiting the site. *See my separate writeup on SANDBOXIE at www.jimopi.net under MALWARE TOPICS*
  2. ANTIVIRUS SUITE: I prefer the free Microsoft Security Essentials (MSE) for Windows 7 and AVIRA for XP. Make sure it is installed and running, including an automatic weekly "Full-Scan". *If you feel you need to pay for protection, then I suggest MalwareBytes Anti-Malware Pro or Premium or ESET NOD32 Antivirus.*
  3. WOT (Web Of Trust): This is an add-on for your browsers to help identify untrustworthy websites. WOT must be installed separately on each browser. *See www.mywot.com for details.*
  4. SECUNIA PSI: (Personal Software Inspector) Installed and configured to automatically start on each boot. PSI helps keep your PC secure by scanning your system once a week and automatically updating many utilities and programs like FLASH, JAVA, and Adobe Reader. *(In addition, I run a manual scan of PSI once a month).* Secunia PSI automatically updates most, but not all common programs without manual intervention. Just make sure its Icon in the System Tray stays Green.
  5. SPYBOT SEARCH & DESTROY (IMMUNIZE) (Version 1.6.2 only) for even more browsing protection: This program will help immunize your browser against more known bad (blacklisted) websites. This program must be updated manually. I recommend once a month. *NOTE: I do not use or recommend the new version 2.0 of this program.*
  6. STANDALONE OR ONLINE SCANNERS: I manually run a full-scan with each of these programs every month: SuperAntiSpyware Standalone Scanner, MBAM(MalwareBytes AntiMalware), MBAR(MalwareBytes AntiRootkit), ESET Online scanner, and SpyBot

S&D. If your PC gets infected, the first thing the malware does is disable your regular installed Anti-Malware Suite. This means that your PC can be infected and your Anti-Malware program cannot tell you it has been disabled. *See my "ANTIMALWARE TOOLS & TIPS" for details.*

- **STANDARD USER ACCOUNTS** *(VISTA AND WINDOWS 7)*:
  1. These operating systems allow a user to run in a user authority called "Standard". This limits the PC's ability to secretly install malware.
  2. When you install either of these Operating Systems or buy a new PC, the default authority for the first User is "Administrator". This leaves you vulnerable.
  3. Be sure to create an everyday user account for yourself that is "Standard". This helps keep malware from easily installing itself. *(See my "INSTALL AND CUSTOMIZE WINDOWS 7" sheet for details on creating Standard Users.)*
  4. Be sure to put a password on your "Administrator" user account. Then if you are ever unexpectedly asked for the Admin password, stop and think if it is legitimate.
  5. *(Note: In XP this was called a Limited User account, but it never functioned correctly)*
- **BROWSING TIPS**: *(Please use Sandboxie for all Browsing!)*
  1. BEWARE OF ANY POP-UP WINDOWS THAT LOOK LIKE AUTHENTIC WINDOW "SYSTEM MESSAGES". They are probably fake.
  2. BEWARE OF FAKE "VIDEO VIEWER" PROGRAMS: A common source of malware is from malicious sites 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 their video content. By clicking that Window you are actually giving permission that allows malware to install itself on your PC. Even Pop-up blockers do not deter the bad guys.
  3. BEWARE OF FAKE "ANTI-VIRUS" PROGRAMS: Another common source of malware is a window popping up at a website that says it has detected malware on your PC and to click the box to fix it. Even though it looks authentic, 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 immediatly close your browser (Big X in the upper Right Hand corner of the browser window), and then run your own Anti-virus program.
  4. BEWARE OF FAKE "SYSTEM TOOLS" PROGRAMS: Another common source of malware is a window popping up at a website that says it has detected a failure of your PC's hard-drive or memory. Clicking the box will just download trojans and fake system repair 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 immediatly close your browser (Big X in the upper RH corner of the browser window), and then run your own Anti-virus program.
  5. WHEN IN DOUBT NEVER CLICK A POP-UP BOX. If you are stuck with one of the above Pop-Up windows and are not sure what to do or if the Browser will not close, just click Start, then Shutdown/Turn Off Computer. Then power the PC back up and start your browsing session over.
  6. COUPONS: NEVER download and install any Coupon Printing programs. They can invade your privacy and can also be adware/spyware/malware. Honest coupons are easily printed directly from your web Browser.