Microsoft's Free Anti-Malware Tools ©

Jim McKnight www.jimopi.net MicrosoftSecurityTools.lwp revised 1-16-2014

Microsoft has four relatively unknown, but useful anti-malware tools you may find of interest. These tools all work with Windows XP, Vista, and Windows 7.

MICROSOFT SECURITY ESSENTIALS (MSE) - Overview

Microsoft Security Essentials (MSE) offers real-time protection, automatic updates, and scheduled scans. It is a good overall protection tool.

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. If you decide to keep your old anti-virus along with MSE, remember that if you run multiple programs that each continuously scan in the background it will slow your PC down (a lot), plus they may conflict with each other.

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".

4. EMAIL SCANNING: Although MSE is a complete basic anti-malware solution, it does not include an e-mail scanning feature as do many commerical 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.*

5. BROWSING PROTECTION: MSE does ot provide specific browsing protection. The best browing protection can be had by using SANDBOXIE to open your browser. If you have want more browsing protecton, I suggest you use the free WOT (Web of Trust) browser Add-on. WOT is available for every browser and must be installed separately on each browser. *I use both.*

6. SCAN OPTIONS: Both the "Quick Scan" and the "Full Scan" do run slow, but they are very thorough. Remember, they only run once a week. So far, the scans do not seem to interfere with the operation of other programs as much as other kinds of anti-malware scans do. It the scan does slow you down, you can reduce the maximum percent of CPU that MSE will use in the MSE Settings window. Default is 50%.

7. CONFLICTS 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. Time will tell if any conflicts occur. My advice is that if you want multiple AntiMalware programs on your PC, only allow one of them to run "Real-time" protection.

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 on an XP system. If you leave Defender installed, MSE will disable it. For Windows 7 and Vista, Windows Defender cannot be removed, but will automatically be disabled by the MSE installer.

9. For more details on downloading, installing, and using MSE, see my "ANTI-MALWARE TOOLS & TIPS" sheet at http://www.jimopi.net

WINDOWS DEFENDER (in Windows 7 is obsolete as a separate program. It is included in MSE. *WINDOWS 8 NOTE: MSE has been renamed to WINDOWS DEFENDER in Windows 8. Thanks a lot Microsoft)*

Windows Defender is an anti-spyware tool that has been replaced by MSE (Microsoft Security Essentials), which is a more thorough anti-malware tool. Defender is still available as a download for XP, but MSE is a better choice. Defender is built in to Windows 7 and Vista systems and cannot be removed, but will be automatically disabled when you install MSE.

Just like MSE, Defender is becomes part of the normal Windows Update process and you can basically forget about it. By default. it runs a daily scan and offers full time protection, but you can change the options so it runs a weekly scan or only when you manually start it. You can also turn off the full time protection.

MALICIOUS SOFTWARE REMOVAL TOOL (MSRT)

You probably do not realize that this tool is already installed on every XP, Vista and Windows 7 system and MSRT silently runs each month after you download your regular Windows Updates. The MSRT updates itself (KB890830) each Patch Tuesday, launches once on your system during the Windows Update install process, and runs a Quick-Scan in the background. If it finds malware, it pops up a window suggesting you run a full scan, and removes anything it finds. *(NOTE: There is no quarantine option that I can find, so there is no going back if something important gets removed).*

- You can manually download the latest version of the MSRT at any time from: http://www.microsoft.com/security/malwareremove/default.mspx
- You can manually run a quick or a full scan of the latest installed version of MSRT by typing: Start > Run > mrt > click "OK" *(Yes, "mrt" not "msrt").*
- You can easily create an Icon for your desktop to run the MSRT by: 1) Right-clicking on the Desktop > New > Shortcut. 2) In the "Location of Item" box, type mrt.exe . 3) In the "Name for this shortcut" box, type "Run MSRT" or whatever you want to call it. 4) Click Finish. Now you can start the MSRT at anytime by double-clicking the new Icon.

MICROSOFT SAFETY SCANNER (msert):

1. This new malware scanner from Microsoft is a free downloadable Malware Scanning Tool.
2. If you suspect that your PC is infected, this is a really good tool to try and prove it one way or another.
3. You simply download the file, double-click the downloaded file and let it run a full-scan.
4. When starting the download, you must choose the 32-bit or 64-bit version. *In some cases, like with Windows 7 64-bit and IE8, I know that IE will auto-detect your Windows version.*
5. This scanner is meant to be used in ADDITION to your regular anti-malware tools.
6. The Scanner expires 10 days after you download it, so it is meant to be downloaded and run in an emergency. Do not download it ahead of time.
7. You should always download a fresh copy of the scanner each time you want to run it.
8. *WARNING: This tool has no "Quarantine" capability. If it removes anything, it is gone. There is no going back.*
9. Here is the link to download it: http://www.microsoft.com/security/scanner/en-us/default.aspx

WINDOWS DEFENDER OFFLINE (WDO) (AKA - Microsoft Standalone System Sweeper)

- This is a bootable scanning tool and is used when the malware makes your PC un-bootable or if a rootkit makes the PC hard to clean or reinfects it. You must choose the 32-bit or 64-bit version.
- First, you download a file to a good PC, then run it. The file will download the necessary files to create a bootable flashdrive or CD. Then you boot PC from the flash/CD, and run a scan.
- Windows Defender Offline - Free: http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline
- For more Info, see this link: Http://windowssecrets.com/links/tsmfl3yq3oyld/60278dh/?url=WindowsSecrets.com%2F2012%2F01%2F05%2Fts%2F%3Fn%3Dstory1
- NOTE: WDO requires at least 768 MB of RAM, preferably 1 GB. Otherwise it will fail with a 0x80508007 low memory error.

ALWAYS LOOK FOR THE LATEST VERSION OF THIS DOCUMENT AT www.jimopi.net