

Microsoft's Free Security Tools

Jim McKnight www.jimopi.net MicrosoftSecurityTools.lwp revised 12-15-2009

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)

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.

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".
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" 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.
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. I can say without a doubt, that multiple programs running real-time protection will slow down your PC. If your PC is fairly new, you may not notice the difference.
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. If you leave Defender installed, MSE will disable it.
9. For more details on downloading, installing, and using MSE, see the "ANTI-MALWARE TOOLS & TIPS" at <http://www.jimopi.net>
10. Get the free download of MSE or read more about it at: http://www.microsoft.com/security_essentials/

Windows Defender

Windows Defender is an anti-spyware tool that is fully integrated into Windows 7 and Vista. This tool is also available for Windows XP and you can easily download it from the Microsoft Website:

(<http://www.microsoft.com/windows/products/winfamily/defender/default.aspx>).

Once Defender is installed on XP, it 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. For details on Windows Defender, see the ANTI-MALWARE TOOLS & TIPS sheet at www.jimopi.net

The Malicious Software Removal Tool (MSRT)

You probably do not realize that this tool is already installed on your system and Microsoft silently runs it each month after you download your regular Windows Updates. The MSRT updates itself (KB890830) each Patch Tuesday, launches once on your system, and silently 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. (No quarantine option that I can find).

- At any time, you can manually download the latest version of the MSRT from:
<http://www.microsoft.com/security/malwareremove/default.mspx>
- You can manually run a quick or a full scan of the MSRT at any time by typing:
Start > run > mrt > 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.

The Windows OneCare Live Protection Scan (On-line Scanner):

(<http://onecare.live.com/site/en-us/center/howSAFE.htm>)

The Protection Scan is part of the Windows OneCare "Full Service" Online Scan and is free to all users. In addition to the Protection Scan, you can also choose to run a Tune-up Scan (Defrag Scan) or a Cleanup Scan (Registry Scan) or the "Full Service Scan".

My only hesitation in recommending the OneCare Protection scan is that I have not yet found if and where they quarantine the suspected bad stuff. For this reason, I always run MSE and other programs first. Most Anti-virus programs offer a recovery path by allowing you to quarantine any suspected malware that it is about to remove. Cleanup programs like CCleaner also offer a recovery path by allowing you to backup any registry entries that are about to be removed. The only recovery option I have found for the online scans is via Windows "System Restore" (and pray that it works).

(You are supposed to only use Internet Explorer to run the Live Scans, but you can use Firefox if you first install the Firefox addon called IE Tab. I do not recommend this).

Installing the Live scanner in IE has a few glitches, so follow this sequence.

1. First set up IE security to allow the onecare.live.com site to function:
 - a. TRUSTED SITES: Open IE and add the site "onecare.live.com" as a trusted site. (*Tools > Internet Options > Security Tab > Trusted Sites Icon > Sites*). Add <http://onecare.live.com> to the trusted sites.
 - b. POPUP BLOCKER: Set the IE Popup blocker to allow "onecare.live.com". (*Tools > Popup Blocker > Popup blocker settings*). Add onecare.live.com to the allowed sites.
 - c. Close IE, and open it again to activate these settings.
2. Go to the <http://onecare.live.com/site/en-us/center/howSAFE.htm> & click the "Protection Scan" button.
3. As IE attempts to install the scanner, it will usually fail on the first try. Try it again, and it should then install OK. Now run the scan.
4. Note: If you have not run a scan for a few weeks, IE makes you install the scanner again.
5. If desired, you can create a handy Start Icon for the "OneCare Live Protection Scan" that opens Internet Explorer and goes directly to the Protection Scan website:
 - a. Right-click on the Desktop, and click New > Shortcut.
 - b. In the box called "Type the location of the item", enter the following text exactly:
"C:\Program Files\Internet Explorer\iexplore.exe" <http://onecare.live.com/site/en-us/center/howSAFE.htm>
Note: There is only space in the text and it is after ...iexplore.exe"
 - c. Click <Next>, name the shortcut "Windows Live Protection Scan", and click finish.

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