

# COMPUTER NEWS from the



FEB. 2014

Volume 2 NO. 2

---

As found on the web and other sources

## Free Microsoft Security Tools

FROM: [askbobrankin.com](http://askbobrankin.com)

When it comes to computer and online security, Microsoft Windows is often portrayed as the problem rather than the solution. But don't get the idea that Microsoft doesn't care about security. In fact, Microsoft publishes several free and effective security tools for home and professional users. Try some of these to see if your currently installed security software is doing everything it should to protect you...



### Beyond Anti-Virus:

### Try These Free Microsoft Security Tools

News of security breaches frequently mentions a "vulnerability in Windows." The fact is that any software is vulnerable to hacking; it just so happens that Windows is the most popular target because it's the biggest.

Are you sure your Windows system is correctly configured, has all the latest security patches, and that your anti-virus software is adequately protecting you?

Here are several [free tools](#) from Microsoft that you can use to find out.

Microsoft's [Malicious Software Removal Tool](#) scans for and removes malware after finding it. However, its signature database includes only the most prevalent threats. It would be a good idea to run Microsoft Safety Scanner (see below) after MSRT for greater assurance that you haven't missed anything.



If you use Windows Update (and you should!) there's really no need to [download](#) the MSRT, because Windows Update will do so automatically. But you can download and run it at any time if you suspect a problem.

---

[Microsoft Safety Scanner](#) is a good, quick way to check for known malware on your computer. It includes a malware signature database of known threats and a barebones program that searches your files for matches. Options include a quick scan of disk areas where malware is deposited most often; a full scan of entire drives; or a targeted scan of user-selected folders.

During the download, you have the option to run the tool right away, or save it to a flash drive or CD for use on another computer. To ensure that you use the most recent malware signature database, MSS expires every ten days and must be downloaded again. Because it's a rather large download (over 90MB), I recommend using Microsoft Safety Scanner only if you suspect that your existing anti-[malware program](#) has failed to catch or remove a problem. It can also be run every few months to double-check your antimalware [program's](#) effectiveness.

---

The [Microsoft Malware Prevention Troubleshooter](#) goes by the short name, "FixIt." This utility turns on Windows Firewall; Automatic Update (so you automatically receive and install critical

security updates); Pop-Up Blocker in Internet Explorer; and User Account Control. Note that many users disable some or all of these features deliberately, either relying on third-party firewalls and other protections or simply preferring not to be bothered by UAC.

FixIt also enables features that check for active anti-malware software and nag you if you don't have any installed; stops the Remote Registry service if it is active, preventing hackers from modifying your registry settings; monitors Internet Explorer to make sure it is up to date and privacy/security settings are tight; and resets your proxy settings to ensure a normal browsing experience if [malicious software](#) has hijacked them.

---

The [Enhanced Mitigation Experience Toolkit](#) makes malware's attacks more difficult by protecting certain operating system features that must be circumvented before vulnerabilities in Windows can be exploited. It will also "harden" the defenses of certain programs that are commonly used as attack vectors, such as Internet Explorer, Microsoft Office, Adobe Reader and Java.

In addition, it tightens the rules for verifying the identity of popular online services such as Twitter, Facebook and Yahoo. EMET supports Windows 7 or 8, Windows Vista, Windows Server 2003, and the Home or Premium edition of Windows XP.

---

[Microsoft Baseline Security Analyzer](#) scans local and remote computers to see if they have the latest Microsoft security updates for Windows or MS Office and whether there are any security misconfigurations that leave the door open for malware or hacking. Some things the MBSA looks for are missing security updates, weak [account passwords](#), and misconfigured firewalls.

The Microsoft website says the MBSA is a tool for IT professionals and system administrators, but don't let that scare you away. If you're a typical home computer user, then you ARE the system administrator. You will need to know in advance if you have a [32-bit or 64-bit version of Windows](#), and then select the corresponding download. Note that the program doesn't automatically run after the download. You'll need to find the downloaded program and then launch MBSA. After it runs, MBSA will display a report of any problems found, with links to remedy them.

---

[Windows Defender Offline](#) is a tool that's fundamentally different from all of the ones I've mentioned here so far. The difference is that it doesn't run while Windows is active. It's a standalone program that runs from a [bootable](#) disk. WDO will boot up a bare-bones environment in which neither the Windows operating system nor viruses can activate. It then scans your hard drive for malware, and will remove any if found.

If your system is so badly fouled up that you can't even download or run a malware scanner, or if you cannot boot Windows because of a malware infection, then WDO is a handy tool to get back to good.

## **What About My AntiVirus Program?**

To be clear, I'm not recommending that you use any of these tools instead of your current anti-virus program. Consider the tools listed here as an extra layer of defense against malware. Use them as a "peace of mind" scan to check for cyber-nasties that can sometimes creep in undetected.

No anti-virus program is going to protect against 100% of all threats 100% of the time. The reason for this is that new viruses are being created all the time, and viruses can morph (change their identifying characteristics) and attack before your antivirus program is updated. It's also possible in some cases for a virus to disable your [antivirus protection](#).

I'm sure many people reading this will be wondering why I didn't mention the obvious -- Microsoft's free Microsoft Security Essentials antivirus program. The short answer is that I don't recommend it. The long answer is in my article [Microsoft Security Essentials: EPIC FAIL](#).

**For a list of free antivirus software that I do recommend, see my article [Free Anti-Virus Programs](#).**

Read more: [http://askbobrankin.com/free\\_microsoft\\_security\\_tools.html#ixzz2rBIeyPw5](http://askbobrankin.com/free_microsoft_security_tools.html#ixzz2rBIeyPw5)

## **In the “IT HAD TO HAPPEN” category.**

Or “dear, did you order two quarts of cat’s milk”?

So-called "smart refrigerators" and other household appliances may not be so smart. According to security research firm Proofpoint, one [WiFi-connected refrigerator was hijacked](#) and used in a network that also included smart TV sets, to send over 750,000 spam [emails](#) in a recent botnet exploit. This brings us one step closer to digital delivery of frozen pizza.



## Full Windows Start Menu Coming Back:

By Brandon Dimmel on 20131218 in "infopackets.com".

Microsoft will revive the complete Start Menu in a future version of its Windows operating system. That's the claim of Windows insider Paul Thurrott, who says he has learned from sources at the Redmond, Washington-based firm that the Start Menu could be back as soon as 2015. Thurrott suggests the new Start Menu could be far closer to the interface seen in Windows 7. Microsoft introduced what Computerworld calls a "pseudo-Start button" with Windows 8.1 (or Windows 'Blue'), which was released this fall.

Thurrott's claim has resulted in an explosion of speculation about how and when the Start Menu will return. (Source: computerworld.com)

### "Threshold": Multiple Platforms, One Interface

Some experts believe it's part of a larger update popularly called Windows 8.2, which is also designed to bring the interfaces of Windows, Windows Phone, and Xbox One closer together. The project, which Microsoft expert Mary Jo Foley calls "Threshold", will apparently make releasing software products on PC, mobile, and gaming platforms far more seamless than is the case right now.

It's worth noting that this is hardly a guarantee that Microsoft plans to revert back to a user interface reminiscent of Windows 7. In fact, Thurrott says things are "still up in the air," and admits that he needs to "verify" what he's learned with others.

## **Microsoft Trying to Win Back Lost Customers**

Nevertheless, it appears Microsoft does have something major in the works. Thurrott suggests that it's part of an attempt by Microsoft to win back consumers alienated by Windows 8. "You can see that Microsoft is, if not moving forward per se, at least continuing to do the right thing and responding to complaints," Thurrott said on his Windows Supersite blog. "It's a good sign." (Source: winsupersite.com)

Of course, the news could spell trouble for companies like Stardock, which is best known for 'Start8', a tool that effectively revives the Start button and Start Menu in Windows 8. Stardock founder Brad Wardell admits the Windows 8.2 (or Threshold) rumors are concerning. "Start8 ... [has] brought us millions of new customers, so we definitely would miss that influx of new users," Wardell said. (Source: computerworld.com)

### **Quote of the month**

“It is only when they go wrong that machines remind you how powerful they are.”

Clive James