Revisiting the Windows Secrets Security Baseline: Part 1

By Susan Bradley

Regular readers know that Windows Secrets discusses the importance of PC and Internet security almost every week.

But it seems many Windows users never get the message. Here are tips for safe computing in the year 2014. Pass them along.

Rebooting the Windows Secrets Security Baseline

In the Feb. 17, 2011, In the Wild column, "Windows Secrets PC Security Baseline," we listed the minimal steps every PC user should take to protect digital information. Back then, it was a bit easier because smartphones were not quite as ubiquitous and the first iPad had been released only the year before.

In that column we listed the four key elements for online security: a hardware firewall, antivirus software, an updated browser, and up-to-date applications. To that list, add password management. All those parts are still important. But with the evolution of online threats, the baseline of PC security has risen a notch or two. In this updated Windows Secrets Security Baseline, I'll review what's important today. And in a follow-up story, I'll discuss some advanced security options.

These days, we have a lot of threats and risks to consider. Now that most of us are connected to the Internet 24/7, we face fewer worms and viruses spreading from system to system, but many more zero-day attacks that come through our connections to the Web. And to make matters more worrisome, cyber attackers are now targeting the sources of our Web experience — banks, online shopping, social networks, and many more back-end services.

Given the many ways our digital world might be compromised, I'm actually going to take a step back from the original WS Security Baseline and start with the most basic protection we have at hand: backing up our systems.

Rolling Windows back to the 'last known good'

Using backups as a security tool isn't new. About 10 years ago, a Microsoft Security program manager (now working at Amazon) wrote an article on the ways to recover from a system breach. He argued that you couldn't recover a hacked system with cleaning tools alone; you needed good recovery media or a trusted backup. A decade later, that advice is still perfectly valid. To be assured you have a clean system, you need to recover or rebuild it.

So again: Item one on any security baseline is to ensure you have a full, working backup — and that you can recover data from that backup.

I'm a fan of Acronis True Image (site) and Runtime's DriveImage XML (site); both are solid backup options, and both provide the ability to back up everything on your computer to an external USB hard drive.

Reviewing the rest of the security basics

As noted, those other basic security requirements are no less important than they were three or more years ago. Here's a summary:

- **Use unique passwords and keep them safe:** Given all the websites and cloud services we now use, keeping passwords is only more difficult — especially because the first rule of password security is to use a unique

password for each site or account. Keeping track of numerous passwords is tough; it would seem the two choices are either to write them down (a dubious solution) or use password-management software.

For sensitive sites such as online banking, try changing passwords at least once every 180 days — or as often as you can without driving yourself crazy. Also, select security-reset questions that can't be guessed from information you post online.

- **Run firewalls:** Ensure that Windows' built-in firewall is up and running. Also check that your router's hardware-based firewall is active. Contrary to what some believe, the two firewalls should not conflict with each other. And what one misses, the other will probably catch.

A properly configured hardware firewall will protect your entire home network — not just PCs, but also other potentially vulnerable devices such as set-top boxes, tablets, and network-attached printers and hard drives.

When Comcast recently updated my home router, I was reminded that most routers use basically the same default sign-in credentials: i.e., "admin" and "password" — or some close approximation. Moreover, the firewall's security was set to "low." Because router settings can be a bit obtuse for the average PC user, I will cover that topic in an upcoming article. For now, just make sure that you have a hardware firewall enabled. Oh — and change your router's default sign-in credentials if you haven't done so already!

- **Run anti-malware software:** For many years I was content with a basic, full-time antivirus application and an on-demand malware scanner. Those two apps were Microsoft security Essentials and the free version of Malwarebytes Anti-Malware. But with the threats from casual websurfing getting only worse, I've switched to the paid, full-time version of Malwarebytes (site) — both on my home system and on others' systems.

There are, obviously, many other excellent anti-malware products. Sites such as AV-Comparatives and AV-TEST publish regular reports of the most popular AV products. You don't need to buy one of the big security suites unless you want defense-in-depth and are technology-challenged.

- **Keep browsers up to date:** Eons ago, our only browser was Netscape Navigator. And the Net was, for the most part, a friendly place. Now it's common to have three or more browsers installed — and you should. Chrome, Internet Explorer, and Firefox are the usual choices, but you might also want Opera (site) as yet another alternative — one that might not be as big a target for cyber attacks.

Along with having several browsers installed, I recommend using more than one search engine. Several, such as the awkwardly named DuckDuckGo (site), promise not to use search-tracking to send you targeted ads.

(For tips on keeping browsers clean, see this week's Best Practices story **[ERROR :: LINK TO COME]**, "Housekeeping tips for your Web browsers.")

- **Keep Windows and apps up to date:** Windows and its associated applications might be getting less buggy, but hackers are also getting more sophisticated. So keeping your machine up to date is still a key element of online security.

Along with system updates, take some time to remove applications you no longer need. That's especially true for software that has a history of vulnerabilities. For example, if you don't need Java, uninstall it; if you don't need Silverlight, uninstall it (and ignore Microsoft's seemingly endless offerings of Silverlight).

Also be on the lookout for updates — Java and Adobe Flash Player, for example — that try to install toolbars and other "free offerings." Use Secunia's Personal Software Inspector (PSI; site) to help scan for outdated and/or unpatched software. (Note: Some overzealous security products flag PSI as malware. You can ignore the warnings.)

Set up a limited-rights account: This might be the most overlooked security tool available to Windows users — most of whom are probably running continuously in administrator mode. That's an opportunity for cyber attackers to take complete control of your system. Windows 7, 8, and 8.1 make it relatively easy to work in a "standard user" account and let you provide administrator credentials only when needed.

A blog post (relatively old but still valid) showcases ways to set up both administrator and standard-user accounts. Yes, Windows' User Account Control (UAC) can be annoying, but I don't recommend disabling it. Stick with the default settings in Windows 7, 8, and 8.1.

And though we might not like Win8's Modern interface, keep in mind that Microsoft added SmartScreen technology (more info) to the operating system itself. (It's been in IE since Version 8.) Malware downloads that Win7 might let through stand a better chance of being caught by Win8.

Baseline plus: A second machine for websurfing

You might suspect I'm in league with computer manufacturers, but I have good reasons for stating that the best form of Internet safely these days is to do casual Web browsing on a second machine — one dedicated to just that activity. Alternatively, dedicate a second system just for sensitive activities such as online banking. Some PC users set up dual-boot systems for the same purpose, but I'm not a fan of that technique. I've seen too many patching oddities that seem to be rooted in conflicts between the two installed operating systems.

The ideal system for casual browsing is one of the small, mobile devices such as an Android tablet, iPad, Kindle, or — if you must stick with Windows — a Windows RT device. Any of those platforms is more difficult (or less likely) to be successfully infected.

Super-geek and noted security blogger Brian Krebs recommends using a Linux boot disk when doing online banking. Great idea, but it will defeat communications between bank sites and any accounting software you might be using.

If you want additional security for online banking, I recommend installing two specialized applications on a Windows PC:

Trusteer Rapport (site): This software works with websites to block malicious keylogger programs that steal credentials. I reviewed the software in the March 7, 2013, On Security article, "Using Trusteer to enhance online-banking security." It's running on several of my office machines with no issues. You might check whether your bank supports and recommends Trusteer — or some other keylogger-blocking software.

CryptoPrevent (site): CryptoLocker is still a significant threat, and this software blocks viruses that include the CryptoLocker payload — even protecting the temporary folders that CryptoLocker loves to infect.

Monitoring your system for rogue software

For now, we'll have to stick with the old-fashioned eyeball technique. Once a month, launch Windows' Programs and Features applet and look for software you don't recall installing. Sort the installed software by date. You should be safe uninstalling any applications you don't recognize.

More tools for prevention and cleaning

A tool often overlooked is Microsoft's Baseline Security Analyzer. MBSA 2.3 (site) is geared more toward IT admins than consumers, but it can still be useful on personal machines. I'll cover it in detail in an upcoming article.

A more practical tool for all Windows users is Microsoft's Enhanced Mitigation Experience Toolkit (more info). Microsoft has recommended EMET in particular for preventing Internet Explorer zero-day attacks.

Recently, fellow Security MVP Harry Waldron helped a friend clean up his system. He then posted his recommendations. The tools he mentions are designed to run from a flash drive, ensuring that they get under the installed operating system. The tools are updated regularly, so I suggest downloading them when they're needed (assuming you have access to a second system in order to do so). To prepare for an emergency, I recommend keeping a blank external USB hard drive and empty flash drive of suitable size — so you'll be able to move data quickly from one machine to another.

The Windows Secrets Security Baseline recap

If you want to give those with short attention spans the basics of PC security, send them this list.

- **Step 1.** Have a backup solution.
- **Step 2.** Use unique passwords for each site or account.
- **Step 3.** Have a hardware-based firewall in addition to the Windows firewall.
- **Step 4.** Run — and keep updated — good anti-malware software, both real-time and on-demand scanning.
- **Step 5.** Have alternative browsers and keep them all updated. Consider using alternative search engines.
- **Step 6.** Applications: Either patch 'em or remove 'em.
- **Step 7.** Don't run in administrator mode; set up a standard-user account.
- **Step 8.** Consider using a tablet-style device for recreational web surfing.

If that seems like a lot of work, consider the time and expense of getting hacked. At a minimum, you might end up with an unwanted toolbar. On the other hand, you might have your bank accounts cleaned out and your identity stolen. Keep in mind that cyber thieves are constantly finding new ways to beat the system. Stay tuned for Part II of our series on security.