

Windows Update

By: Joe Magura, Software Engineer III
Attorneys Title, a division of United General Title Insurance Company

Help Wanted: Protect me from Viruses!

If you were going to hire someone to help you protect your computers, at home or in the office, you might place an ad like this in the classifieds or on Craig's List: *Help Wanted—Need Internet Savvy Geek to Protect Me from Malicious Software.* You'd be looking for someone who could help you make sense of your options to increase the security of your network and computers without spending lots of money and/or making extensive changes to your world. You'd want to avoid viruses, Trojan Horses, worms, browser exploits and all the other risks that stalk your every interaction with the Web.

Odds are your want ad would garner responses from some very high-profile names that you'd recognize. McAfee and Norton would offer to sell you their antivirus software and other Internet security programs and suites. More obscure companies and even local IT consultants would likely offer to physically inspect your network configuration and install hardware like firewalls and other protective devices to guard you. Most of these responses would have at least one item in common - they would all cost money, sometimes a lot.

However, if you sifted through the offers and resumes, you would stumble across one that might surprise you: *College dropout whose products enjoy a less than stellar reputation for reliability and security is interested in keeping you safe from Internet threats. Won't cost you a dime.* Yes, Bill Gates and his brainchild Microsoft are offering to help you for free. But should you jump at the chance or feed the offer into the shredder?

Who Better to Help You?

Most of us use computers that run a Microsoft Windows operating system. Whether it's Windows Vista at home or Windows XP at work, the software that we rely upon was made by every hacker's and every security consultant's favorite target. The fact is that Windows products have, at least until the rather unpopular Vista, been bashed for poor security harder than a hockey puck at a Hurricanes game. The most common argument against Microsoft's operating systems is that they are overly complicated, behind the times and too dependent upon secrecy rather than good design in an age where threats to our productivity and personal information are ever-increasing and increasingly effective.

All that may well be true and the criticism of Microsoft is at least partially deserved, but before you scrap Mr. Gate's offer of help, consider this: who is in a better position to protect you from security problems in Windows than the people who wrote Windows? Presumably these folks have some idea of how all that complicated software code works and what needs improvement. For example, when Chevrolet finds a problem with the brakes on their truck line they announce the recall; they make the repairs via their dealerships; and they foot the bill for making things right. In essence, Microsoft is doing the same thing only it's not a recall; it's called "**Windows Update.**"

Windows Update to the Rescue

Windows Update Defined

Microsoft expends a lot of energy investigating reported and suspected vulnerabilities in their software. Industry security experts who aren't even on Microsoft's payroll notify the company of security flaws they discover before they go public with the information, thereby giving Microsoft a chance to stay ahead of would be hackers. Ideally Microsoft's software engineers figure out what's wrong in their code, come up with fixes (also known as patches) and release an update to Windows to close the security gap. These updates get downloaded and installed to your computer via Windows Update:

- Your computer asks Microsoft's Windows Update servers if there are any updates to install.
- If needed Microsoft will install special update software that enables the servers to see what updates you already have present on your PC, what operating system components are extant on your system and other details of your system.

- Windows Update identifies the updates your system needs and downloads them to your local computer. Some of these updates are quite large and will make your Internet connection seem like overpriced dial-up which is why you should schedule the updates to happen when you are not using your computer.
- Once everything is downloaded each patch's installer runs to update the components that were found to be insecure or defective.
- Finally, Windows Update may reboot your system since some core parts of the operating system can't be updated while they are in use. Trying to do so would be rather like attempting to change a tire in a moving vehicle—only Speed Racer can do that.

Where does Windows Genuine Advantage come In?

They say there is no such thing as a free lunch and Microsoft is in the software business to make money, lots of money. Windows Genuine Advantage is Microsoft's latest attempt to keep people from illegally installing pirated copies of Windows. Since Windows Update is one of the few ways Microsoft can find out who is running Windows on their computer, it is a logical place to check if you actually bought your copy of Windows or if it fell off a truck. Provided you shelled out your hard-earned cash for your software, you have nothing to fear when Microsoft installs the Genuine Advantage checker on your system. Largely a euphemism, this software makes sure that fifty people aren't running the same copy of Windows.

How do I Run Windows Update?

You can manually run Windows Update by going to the Microsoft.com web site and finding the link to Security Updates (mind you, Microsoft changes their web site with some regularity so you may need to poke around a bit or look for the key words "Update" or "Security"). Doing so will provide you with control over what updates you download and install, but you have to remember to visit the site frequently. Fortunately there is a more automatic way.

In all modern Microsoft operating systems (most versions newer than Windows 98) Windows Update is built right into the system and has an automatic download and install capability. For instructions on how to access this feature in Windows Vista [click here](#), for Windows XP [click here](#) (*links may break, search Microsoft.com for "windows update" if the links take you nowhere*).

To make everything totally automatic simply select the recommended *Automatic* option, select a time when your computer will be idle but powered on and connected to the Internet, and press OK. It's that simple—your computer will now stay up to date with the latest security updates that Microsoft publishes.

Are There Any Risks?

It's free; it's automatic; it's Microsoft; what could possibly go wrong, you may ask? Just as scratching a loose flake of paint on a wall in your house can somehow end up in \$4,000 worth of restoration work, even something as seemingly benign as Windows Update can backfire. As those Lotus Notes users who care to relive the painful past can testify, some Windows Updates are more punishment than protection. When Microsoft released Windows NT 4.0 Service Pack 6 every Notes user who installed it suddenly found themselves enjoying an impromptu vacation—no email for you, my friend. Microsoft rushed out a new Service Pack (also known as an "SP"), SP 6a, after much gnashing of teeth and miserable wailing from the afflicted.

The moral of the story is that everyone makes mistakes and sometimes Microsoft acts with the best of intentions but burns a few (or not so few) users in an effort to protect everyone. As nice as it would be to make a blanket statement to the effect that updates are always good, the world of technology is too rife with exceptions to support such a rosy viewpoint.

For users with a corporate IT department, you should certainly confer with your IT staff before doing anything. Many companies test Windows updates before pushing them out to users to ensure that no update breaks critical applications. If you enable Windows Update you could actually be circumventing your own company's policies.

What Else Should I Do?

The topic of what to do to stay secure on the Internet is beyond the scope of this article and has entire books devoted to it. A simple rule of thumb to help you decide how much energy and money to expend in this arena is to answer the question: "How much would it hurt you if someone stole the information you have on your computer and/or if your computer was rendered useless?" If you don't keep your financial records and your Social Security number on your PC and you only use it for playing Mahjong then you can likely relax. Otherwise, you make the call.

Microsoft also provides an Office Update site that will install patches for Office products like Word and Excel. How Microsoft decides what is a Windows patch versus an Office patch is anyone's guess. Visit Microsoft.com to learn more.

Stay on a supported Operating System

Microsoft would like you to buy Windows Vista and all subsequently released versions the second they hit the store shelves, but you don't have to do that to stay reasonably safe. Microsoft makes a commitment to keep "currently supported" versions of Windows secure and up to date. To find out if your Windows operating system is still being supported by Microsoft, visit Microsoft's [Lifecycle Information page](#). You can determine what version you are running by watching your computer boot or usually by pressing the Start button and reading the banner that is displayed along the left side of the Start menu. Microsoft will tell you if you are currently supported and for how much longer you can count on updates to keep flowing for your particular operating system.

Run Antivirus Software

Rather like motorcycle helmets, security software is optional but recommended. Also like headgear, there is some logic to spending as much as the item you are protecting is worth. That said, Open Source software is making inroads into areas that were once reserved for the big players like McAfee. Google is your friend and it can help you find antivirus and antispymware software that ranges from caviar-grade to chopped beef.

Take Advantage of Resources from Your Internet Service Provider (ISP)

Many ISPs provide security features that their subscribers receive by default or at least for free. A call to tech support may require some patience but the technician can likely set you up with lots of protection for the cost of some of your time.

What's a Technical Article without a Checklist?

While it may not be as exciting as filling out your Christmas list, you may thank yourself someday:

- Decide if Windows Update is right for you. Remember, articles abound on the topic and can help answer questions you might have. Ultimately it is up to you to decide how to proceed.
- Assuming you opt to rely upon Windows Update, enable automatic updates on all of the computers you want to protect. If you have multiple PCs on one network you may want to stagger the update times to avoid a spike in network load.
- Let Windows reboot to install updates when it wants to. Some updates don't take effect until after a reboot.
- Consider buying antivirus software or, even better, a comprehensive suite of Internet security software.