

# THE WEB

## The Lowdown on Updates

By William Powell

If you've begun to wonder recently whether Microsoft and its related products are under attack, you're not alone. The steady issue of updates for vulnerabilities in Windows and Internet Explorer has chewed up several of my evenings as I waited patiently for my 56K modem to download the proper security patches and fixes.

As I write this, the latest is a critical security update for the Internet Explorer browser, ominously titled "Security

Bulletin MS03-040 (828750)." Apparently IE—versions 5.01 through 6.0—has several vulnerabilities that would allow someone to run programs on your computer while you view a Webpage. It's not dependent on an operating system, as earlier vulnerabilities were. So, if you have IE installed on your computer, you need this fix.

There's just one catch: How would you know about that gaping hole in your computer's security if you're not one to

read the various computer magazines, subscribe to some sort of email update, or receive an alert from your IT department? You wouldn't. And I'd wager that most casual computer users, though aware of viruses and their damaging effects, have no idea that the programs they use on a daily basis could have severe design flaws that would relinquish control of their computer to a hacker.

As more home users take advantage of always-on broadband Internet connections, either cable or DSL, they increase the chance that, if left unprotected, at some point they're going to have their computer exploited through a vulnerability in the operating system or an application. To Microsoft's credit, it has been quick to fix flaws in a product's security once it has been discovered, though some people would object to a product being released with such flaws in the first place. Nevertheless, it's a good time to increase your awareness of such vulnerabilities and start taking advantage of the online updates and security features offered.

**Checking under the hood.** The first thing you should be able to do is determine the exact software that you're running. An update will often depend on a specific operating system, such as Windows 98 or XP, or a specific version of an application—for example, Internet Explorer 5.5.

To find out which version of Windows you have, right-click on the My Computer icon on your desktop and then click on Properties. That will open the System Properties dialog box. Under the General tab, you'll see "System:" followed by the version of the computer's operating system.

For most applications, users can determine the product's version by clicking on Help (on the menu bar) and then on About. A window displaying the product's version will appear.

**Download and update.** Once you've

determined the exact version of the software you're running, you're ready to update your system. Microsoft provides a dedicated site that will scan your computer for all available updates. At the site, just click on Scan for Updates. It will then provide you with a complete list of needed updates, critical and noncritical, as well as the more extensive service packs.

➤ [www.windowsupdate.com](http://www.windowsupdate.com)

Users should take a moment to pick and review the suggested updates. Critical updates and service packs are must-haves, but something like Windows MovieMaker 2 can wait.

Anyone who's using a dial-up connection will want to download only those updates that are necessary. Some service packs can take an hour or two to download. Between updates for Windows, Internet Explorer, and Microsoft Office (Microsoft Office has its own update site), I had to set aside a few late nights to download what I needed. If you're fortunate to have a high-speed connection, you should be able to download and install all needed updates in an evening.

➤ <http://office.microsoft.com/OfficeUpdate>

Getting up to speed by installing the initial batch of updates is just the beginning. You'll want to run the scan once again, because some older updates must be installed first. You can then opt to be notified of future updates (Microsoft flashes a notice on-screen while users are online). Or, you can opt for regular email notification of security updates.

# IM Bad

If you can't IM something nice, don't IM at all—or something to that effect. Perhaps that's why, according to figures from a Blue Coat Systems survey, only 36 percent of U.S. companies currently allow workers to use instant messaging. Aside from security concerns, this modest mode of communication is bringing out some surprisingly bad behavior from employees.

Of the U.S. and British workers polled by Blue Coat Systems, only 27 percent of U.S. workers and 11 percent of U.K. workers actually used instant messaging for business purposes. So, what were the rest of them doing? Here's a list of the top 10 offenses:

- 1 Gossiping about a colleague 77.8%
- 2 Commenting on senior management 63.9%
- 3 Making a negative comment about a customer 51.7%
- 4 Sharing work files 51.7%
- 5 Speaking about wanting to leave their job 48.9%
- 6 Discussing pay 48.3%
- 7 Using abusive language 42.8%
- 8 Using IM to conspire with a colleague while on a conference call 37.8%
- 9 Sharing music or video files 35.6%
- 10 Making sexual advances 29.4%

A word of caution: Hackers have been exploiting email notifications with an email that looks remarkably similar to an official Microsoft email from the email address support@microsoft.com. In fact, it's the vehicle

for spreading the Sobig-B worm. The email contains a program with the .PIF extension. Opening the file automatically infects your computer.

To be safe, if you do receive notification of an update from Microsoft, just go directly to the Windows Update Website rather than follow any links or opening any attachments.

**It's automatic.** In addition to receiving email notifications, Windows XP users have the option of an automatic update feature, which notifies users of available updates and then downloads them automatically, or with the user's approval. This is, by far, the easiest way to keep on top of updates.

Office users will want to double-check with their system administrator before setting up the automatic update feature. For home high-speed users, it's a worry-free configuration.

To set up Automatic Update, right-click on the My Computer icon and click on Properties to access the System Properties dialog box. Next, select the Automatic Updates tab and check the box next to "Keep my computer up to date." Now, depending on the level of control you'd like to have when downloading and installing up-

dates, select one of the three options under Settings. I recommend having Windows notify you before downloading and installing any updates. Home users with an always-on connection might opt for automatically downloading and installing the updates on a regular schedule. At the office, I prefer the ability to get an OK from IT before installing any new software.

When a new update is available, a notification balloon and icon will appear in the Quick Start toolbar. You can click ei-

ther the balloon or the icon to review and then install it.

Keeping your operating system and related Microsoft applications updated is just one way to protect your computer. Home users with a broadband connection should seriously consider having a firewall in place. Windows XP provides a built-in firewall. Though it's easy to start, it can take a while to iron out the wrinkles when used with a home network. If you're not working with a home network, it's easy enough for a beginner to install. Detailed instructions, as well as other security tips, can be found at the Microsoft Security Webpage.

Finally, all users should have up-to-date virus protection. So, while you're waiting for your updates to download, it might be a good time to zip over to your local computer store and purchase virus-protection software, if you haven't already, or tack on an online virus update if you already have the software installed. Any update to your OS is useless if you haven't established your first line of defense.

**William Powell** is learning technologies editor of T+D; [wpowell@astd.org](mailto:wpowell@astd.org).

## Happy Holidays

It's set to be a jolly holiday season online this year. According to Brand Keys, a research consultancy that focuses on brand loyalty and future consumer behavior, 50 percent of U.S. holiday shoppers will

be spending US\$20.4 billion online. That's a 15 percent increase over 2002, and a remarkable increase compared to just three years ago when online holiday spending was a more modest \$8.1 billion.

And as a likely recipient of gifts bought online, you'll be glad to know that online consumers aren't limiting their online purchases to sweaters from Land's End. The average Web shopper will spend US\$710 online, though I guess that could mean matching reindeer sweaters for the whole family. Oh, joy.

