Technique 1 Making Windows Safe for Office

Save Time By

- Taking control of automatic updating
- Setting up an antivirus program
- Identifying files that can clobber your machine
- Firewalling the living daylights out of your system

Every Office user needs to take security seriously. The cretins who make programs that melt down the Internet, pummel sites with bandwidth-clogging pings, or simply diddle with your data, are constantly trolling for unwitting accomplices. Foil their plans by keeping your wits about you.

Security is more than just an ounce of prevention. On rare occasion, viruses can wipe out all your data, and worms can bring your e-mail connection to its knees. Far more insidious, though, are the time-sucking security problems that aren't quite so obvious: the malware that lurks and infects and destroys invisibly or intermittently.

Office rates as the number-one conduit for infections because it's on virtually every desktop. On most machines, Office amounts to a big, wide-open target. Windows might get infected, but frequently the vector of attack goes through an Office application.

No Office is an island: It's tied into Windows at the shoulders and ankles. To protect Office — and to protect yourself — you must start by protecting Windows, by applying updates, getting Windows to show you hidden information that can clobber you, and installing and using antivirus software and a good firewall.

Updating Windows Manually

Did you hear the story about Microsoft's Security Bulletin MS03-045? Microsoft released the initial bulletin along with a patch for Windows on October 15, 2003. Almost immediately, people started having problems with the patch. A little over a week later, Microsoft issued a patch for the patch. This new patch seemed to take care of most of the problems, but then someone discovered that the program that installed the patch was faulty. A month after the first patch came out, Microsoft issued a patch for the patch to the patch.

Got that?

To protect Office, you need to keep Windows updated. Indeed, some Windows patches — such as the notorious Slammer/SQL patch MS02-020 — are really Office patches disguised as Windows patches. To protect Office, you have to protect Windows. And to protect Windows, you have to protect Office.

Microsoft wants you to tell Windows to heal itself automatically. I think that's a big mistake — and cite Microsoft's track record as Exhibit A. It's a sorry state of affairs, but I believe that every Office user should

- **Set Windows Update to automatically notify you when new updates are available.**
- **Tell Windows Update that you do *not* want to download — much less install — new patches automatically.** If you need a patch, you can take a few extra minutes and give the go-ahead.
- **Follow the major computer publications closely to see whether new patches are stable and effective *before* installing them.**

Some industry observers would have you trust Microsoft and set Windows Update to run automatically. I say hogwash. In theory, a black-hat cretin could unleash an Office-based worm that will destroy your machine while a patch for that very worm was sitting on Microsoft's servers. In practice, Microsoft doesn't work fast enough to release immediate patches. Demonstrably, your risk from a bad patch is far greater than your risk from a ground-zero worm attack. It doesn't make sense to trust your patching to the folks in Redmond.

I follow Microsoft's patching follies extensively in both *Woody's Office Watch* and *Woody's Windows Watch*. They're free electronic newsletters that go out to more than half a million subscribers every week. Sign up at `www.woodyswatch.com`.

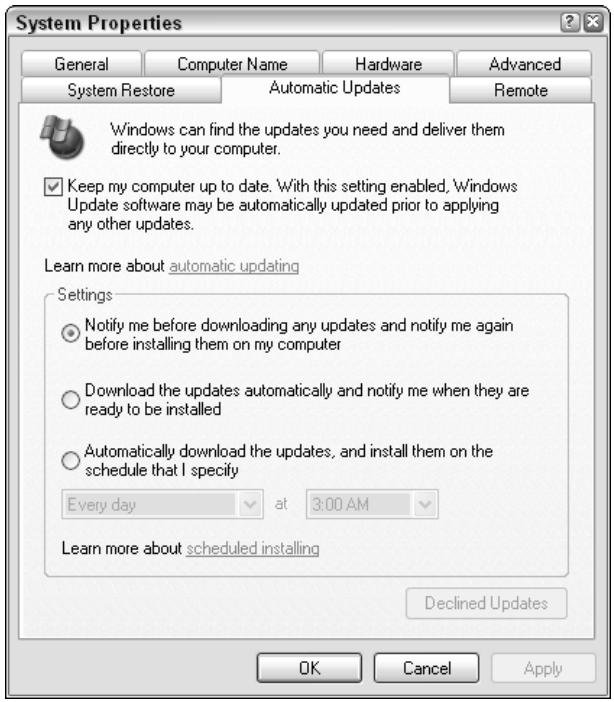
That said, you *do* need to make sure that you install the patches — after they've been tried and tested by a few million guinea pigs.

To tell Windows Update that you want to do it yourself

1. **Choose Start➪Control Panel➪Performance and Maintenance➪System➪Automatic Updates.**

In Windows 2000, choose Start➪Settings➪Control Panel, and go from there.

Windows XP shows you the System Properties dialog box, as shown in Figure 1-1.



• **Figure 1-1: Windows Automatic Updates settings.**

2. **Mark the Keep My Computer Up to Date check box.**

This allows Microsoft's sniffer program to come in and look at your copy of Windows. The *sniffer program* sends an inventory of Windows pieces and patches back to the Microsoft Mother Ship, but as far as I (and several independent researchers) can tell, it doesn't appear as if Microsoft receives any information that can identify you individually.

3. **Select the first radio button under Settings (Notify Me Before Downloading Any Updates and Notify Me Again Before Installing Them on My Computer).**

   That's exactly what you want to do. Microsoft might change the wording of this dialog box slightly. (As this book went to press, there were rumors that the next version of Windows Update would encompass both Windows and Office.) The intent, however, stays the same: You want to be in control of what Microsoft puts on your machine — and when.

4. **Click OK.**

I talk about Windows Update, its implications, and vulnerabilities in *Windows XP Timesaving Techniques For Dummies*. Well worth reading to get the entire Windows perspective.

Windows and Office are so inextricably interwoven that a security hole in one frequently shows up as a security hole in the other. It's important to keep both Windows and Office up to date, because Microsoft may have a vital patch for an Office component, and not even realize it, much less warn you about it!

Showing Filename Extensions

This is the most important Technique in the entire book.

If you're an old DOS fan (or even a young one), you've been working with filename extensions since the dawn of time. Microsoft shows them in all its documentation — Help files, Knowledge Base articles, and white papers. If you're not familiar with extensions (see the sidebar "Since When Did Filenames Have Extensions?" for a definition), it's probably because Windows hides filename extensions from you unless you specifically tell Windows otherwise. These hidden extensions are supposed to make Windows more user-friendly. Yeah. Right.

You probably know about EXE (executable) and BAT (batch) files. Windows simply runs them when they're opened. You might not know about VBS (VBScript) or COM files (command files; good old-fashioned PC programs), which run automatically, too. And I bet you didn't have any idea that SCR (screen saver) and CPL (Control Panel add-in) files get run automatically, too.

The bad guys know. Trust me.

The creators of Windows decided long ago that filename extensions should be hidden from mortals like you and me. I think that's hooey. *Every* Office user should be able to see her filename extensions. If you can't see the filename extensions either in Windows or in Office, you stand a chance of getting zinged — and spending lots of time fixing the damage.

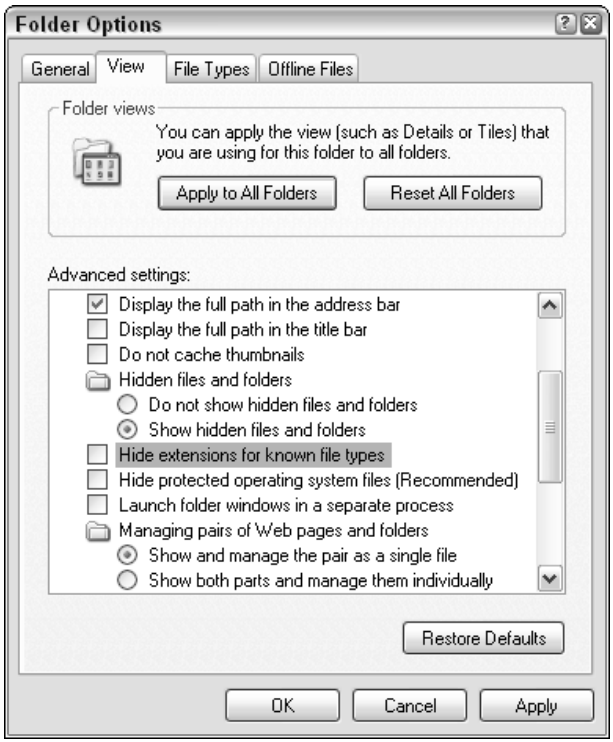
Files attached to e-mail messages rate as the number-one Trojan infection vector, and being able to see filename extensions can make all the difference. For example, that innocent file called `ILOVEYOU` doesn't look so innocent when it appears as `ILOVEYOU.VBS`. You might be tricked into double-clicking a file that's called `Funny Story.txt`, but you'd almost certainly hesitate before double-clicking `Funny Story.txt.exe`.

If you've been looking around Office trying to figure out how to force Office to show you filename extensions in dialog boxes, you've been looking in the wrong place! Windows itself controls whether Office shows filename extensions.

To make Windows show you the entire filename

1. **Choose Start➪My Computer.**
2. **Choose Tools➪Folder Options➪View.**

   Windows shows you the Folder Options dialog box, as shown in Figure 1-2.



• Figure 1-2: Windows hides its view options here.

3. Clear the Hide Extensions for Known File Types check box.

While you're here, seriously consider selecting the Show Hidden Files and Folders radio button and also clearing the Hide Protected Operating System Files (Recommended) check box. You can find a detailed discussion of the implications of both in *Windows XP Timesaving Techniques For Dummies.*

4. Click OK.

All the directions and screenshots in this book (indeed, nearly all of Microsoft's Help files, Knowledge Base articles, and more) assume that you've instructed Windows to show filename extensions.

Since When Did Filenames Have Extensions?

For those of you who haven't been around since pterodactyls provided CPU cooling, a *filename extension* is just the last bit of a filename — the part that follows the final *dot-whatever* (like `.doc`) period in the name. So the file called `ILOVEYOU.VBS` has a filename extension of `VBS`; `MELISSA.DOC` has the extension `.doc`, and so on.

Office programs are all hooked up to their allotted filename extensions. For example, files that end with `.xls` are assumed to be Excel spreadsheets; double-click an XLS file (or try to open one that's attached to a message), and Windows knows that it should run Excel, feeding Excel the file. Same with DOC and Word, PPT and PowerPoint, MDB and Access, and even the little-known PST and Outlook.

Using an Antivirus Product

These days, an antivirus package is an absolute necessity — not only to protect your Office files and programs but to protect Windows itself. Antivirus software is cheap, reliable, easy to buy (you can get it online), frequently updated (sometimes with e-mailed notifications), and the Web sites that the major manufacturers support are stocked with worthwhile information. I know people who swear by — and swear at — all the major packages (see Table 1-1).

Every Office user must

- **Buy, install, update, and religiously use one of the major antivirus products.** Doesn't matter which one.
- **Force Windows to show filename extensions.**
- **Be extremely leery of any files with the filename extensions listed in Table 1-2.** If you download or receive a file with one of those extensions (perhaps contained in a Zip file), save it, update your antivirus package, and run a full scan on the file — *before* you open it

TABLE 1-1: THE MAJOR ANTIVIRUS SOFTWARE COMPANIES

Product	Company	Web Site
F-Secure Anti-Virus	F-Secure	www.f-secure.com
Kaspersky Anti-Virus	Kaspersky Labs	www.kaspersky.com
McAfee VirusScan	Network Associates	www.mcafee.com
Norton AntiVirus	Symantec	www.symantec.com
Panda Antivirus	Panda Software	www.pandasecurity.com
Sophos Anti-Virus	Sophos	www.sophos.com
Trend Micro PC-cillin	Trend Micro	www.antivirus.com

The final filename extension is the one that counts. If you double-click a file named `Funny Story.txt.exe`, Windows treats it as an `.exe` file and not a `.txt` file.

I cover many important details about antivirus software, its care, and feeding in *Windows XP Timesaving Techniques For Dummies*.

TABLE 1-2: POTENTIALLY DANGEROUS FILENAME EXTENSIONS

.ade	.adp	.asx	.bas	.bat
.chm	.cmd	.com	.cpl	.crt
.exe	.hlp	.hta	.inf	.ins
.isp	.js	.jse	.lnk	.mda
.mdb	.mde	.mdt	.mdw	.mdz
.msc	.msi	.msp	.mst	.ops
.pcd	.pif	.prf	.reg	.scf
.scr	.sct	.shb	.shs	.url
.vb	.vbe/.vbs	.wsc	.wsf	.wsh

Firewalling

The Slammer worm demonstrated, loud and clear, that Office users need to protect any PC that's connected directly to the Internet. Slammer slipped in through a little-used *port* (Internet connection slot), infected a particular type of Access database, and then shot copies of itself out that same unprotected port.

A *firewall* blocks your ports. It ensures that the traffic coming into your PC from the Internet consists entirely of data that you requested. A good firewall will also monitor outbound traffic in order to catch any bad programs that have installed themselves on your machine and are trying to connect to other PCs on the Internet.

Windows XP's Internet Connection Firewall works — and it's a whole lot better than nothing. But it's a big target: If you were writing Internet-killing worms, where would you direct your efforts? The upshot: Enable Internet Connection Firewall (which is in the process of being renamed *Windows Firewall*) by all means, but to guard against all intrusions, you want a third-party firewall as well.

Every Office user needs to ensure that a firewall — some firewall, any firewall — sits between his Office machine and the Internet.

If you have a PC that's connected directly to the Internet, you can enable Windows XP's Internet Connection Firewall by following these steps:

1. **Choose Start➪Control Panel➪Network and Internet Connections➪Network Connections.**

   Windows presents you with the Network Connections dialog box.

   If you're using Windows 2000, you need to choose Start➪Settings to get into the Control Panel.

2. **Right-click the connection to the Internet and then choose Properties➪Advanced.**

   You see the Properties dialog box.

3. **Enable the Protect My Computer or Network by Limiting or Preventing Access to This Computer from the Internet check box.**

4. **Click OK.**

I have detailed instructions for setting up a firewall — including, notably, the free version of ZoneAlarm — in *Windows XP Timesaving Techniques For Dummies*.

Version notes: Internet Connection Firewall is only available in Windows XP (unless you're running Windows 2003 Server — and if that's the case, you need all the help you can get).