Chapter 1

Windows XP Service Pack 2

Why place this chapter first? Quite simply, if you're running Windows XP, you should also be running Service Pack 2 (SP2). The purpose of SP2 is to render Windows XP more secure, less vulnerable to attacks from the Internet, and more easily integrated with existing third-party security software. SP2 was introduced to the world just after the first edition of this book was completed, and for that reason it represents the single most important change to XP in the intervening months. Even if you never bothered to install Service Pack 1 — for whatever reasons — you owe it to yourself to get SP2 on your system as quickly as possible.

This chapter covers the features of SP2, along with details about downloading (or ordering it on CD) and installing it. Consider this the first step in making your Windows XP machine and the data it stores safer and more stable, a process continued in the chapters that follow.

Getting and Installing Service Pack 2

By far, the easiest way to acquire Service Pack 2 is to through Windows Update. As covered in Chapter 5 (for all Windows Update functions, not just the service packs), you can use Internet Explorer to head for the Windows Update site (www.windowsupdate.com), or you can set Windows to update itself automatically. If you choose the latter method, depending on your settings Windows will do one of the following:

- Inform you that Service Pack 2 is available and let you download and install it
- Inform you that it has downloaded Service Pack 2 and let you install it
- Download and install it without your intervention

In the first two instances, you must use the resulting dialog boxes to tell Windows to put the service pack in place. See the section "The Installation Itself" a little later for details.

There are two other ways to acquire SP2:

- **Order the free CD:** From the Microsoft site, navigate to the Windows XP area, follow the link to Service Pack 2, and look for the link to order it on CD. As of this writing, the URL

is www.microsoft.com/windowsxp/downloads; of course, this URL can change at any time. The CD is free to all (not just those in the United States), so this is worth having whether or not you plan on installing Service Pack 2 that way.

- **Download the SP2 File:** Numerous download sites have SP2 available as a single, large file. One example is www.download.com, where you'll find it as a 266MB download.

Tip

There's a particularly strong reason to install a service pack from CD rather than from Windows Update. If your computer is already compromised — that is, it has already contracted viruses, spyware, and so on — any subsequent download can be affected, including items from Windows Update. For this reason, if you want to use the protection features of SP2, you're much better off ordering the CD and installing from it, simply because the CD won't be compromised. That said, for a completely clean PC, the best idea of all is to reinstall Windows XP from scratch and apply SP2 from the CD after doing so. For instructions on reinstalling Windows XP, see Appendix B. And hey, there is lots in this book to keep you busy while you wait for the CD to arrive.

Before the Installation

Most software you install on your system takes little if any preplanning. Download the file or insert the CD, step through the installation process, and away you go. Usually, you don't even have to shut down any programs before starting, although it's never a bad idea to do so (and a warning box almost always tells you to do so).

Any time you modify your operating system (OS), however, you should always do so with as clean a system running as possible — and with everything you need backed up, just in case disaster strikes. It's not absolutely necessary (many SP2 installations have been done without this planning), but it's recommended anyway.

Following is a list of suggestions for ensuring the greatest possible likelihood that SP2 will install without problems.

1. **Give yourself some time to do the installation properly:** Plan on spending an evening doing the installation, ideally longer. It might take less. While the actual installation is in progress, don't plan to do anything on the PC.
2. **Perform a backup of the files you can't live without:** This includes programs whose installation CDs you no longer possess, and those whose CD or registration keys you couldn't find if your life depended on it. See Chapters 4 and 26 for more on data backup.
3. **Perform a full virus check on your system:** Be sure to set your antivirus software to include all files, including system files and program files. Include all your hard drives. Depending on how much data you have stored on your drives, this process could take several hours. See Chapter 2 for sites to visit to conduct online antivirus checks.

4. **Perform a full spyware check on your system:** Delete all spyware files and programs located. If you know you have programs that include spyware, delete them from your system thoroughly. See Chapter 3 for sites to visit that offer free online spyware scans.
5. **Get rid of as many programs you can from the Startup folder, and prevent as many programs as possible from automatically loading when Windows starts:** These programs won't likely do any harm to the installation, but your SP2-enhanced Windows will start more quickly without them; besides, you've been wanting to get rid of those time-wasters for a while anyway, right?
6. **Ensure that you have adequate space:** Check that you have at least 2GB of space available on your primary Windows XP hard drive.
7. **If you are installing to a notebook PC, plug in the power cord:** Do not run it on battery power. If the batteries fail during installation, you can cause significant damage to Windows itself (although SP2 is good at recovery).
8. **Using the disk utility of your choice (Microsoft's CHKDSK is fine), check your hard drives for errors:** Let the utility correct the errors, and proceed from there. See Chapter 22 for more on working with hard drives.
9. **Go to Windows Update, before installing SP2, to get your PC up to date with the latest files:** This is particularly true of noncritical updates. However, if Windows Update lists SP2 as an available download, this means that its scan of your PC has indicated that you may install it without difficulty. Before doing so, however, go to step 10.
10. **Download and install the latest device drivers for as many hardware devices as you need:** You can get these from the support areas of the manufacturers' Web sites. Examples include drivers for hard drives (particularly SATA drives and RAID systems), video cards, sound cards, external drives, printers, and more. Again, these aren't actually necessary, but doing this will ensure that SP2 installs on top of a fully up-to-date system.
11. **If your PC has more than one account, log off all users from your PC, and log in as an administrator:** Better yet, reboot the PC to clear out all users and log in as an Administrator. If you do not have an Administrator account, let someone with such an account perform the SP2 installation. If your PC has one account only, it's almost certainly an Administrator account anyway. However, see Chapter 24 for more on establishing and determining user accounts.

The Installation Itself

Ideally, your SP2 installation will require no thought, no intervention, and no actual work. Start it up and away it goes, with your next act being simply to log in as a user and go back to whatever you were doing before the installation. In fact, in most installations, this is precisely what happens. Here is the process.

1. Start the installation by doing one of these things:

    a. Downloading from Windows Update

b. Inserting your SP2 CD

c. Double-clicking your downloaded SP2 installation file

2. Confirm that you want to update the system. If you're not sure, if there's something you want to update in Windows before you do so, or if you just don't want to take the time right now, this is a good place to cancel the process.

3. If you are installing from Windows Update, Windows XP now downloads the files necessary to perform the installation. You may continue working during this process; Windows lets you know when the download is complete and installation is ready to commence. If you are installing from the CD or the full downloaded file, you don't get this respite — installation begins immediately.

4. Once in progress, the installation of SP2 acts much like installation of any other software — except that it takes longer. In fact, it can take as long as an hour (although it usually takes less).

What SP2 Brings to the Table

When Microsoft says that something is necessary, you're probably tempted to just download it, install it, and be done with it. Usually, it turns out to be a good idea; no matter what the nay-sayers might suggest, Microsoft does actually want its products to run properly and not be the subject of continuing claims about lack of security, stability, or sense. In the case of service packs for Microsoft's operating systems, however, installation is always a good idea. In every case, these service packs offer improvements to the OS itself. These improvements range from bug fixes, to new versions of programs, to fundamental changes in security.

That said, you will also always hear horror stories. No matter how many people successfully install a service pack, you will hear only from the people who, for whatever reason, had a bad time of it. And there's no question that some PCs accept Windows service packs much less readily than others do. The problem is that it's hard to figure out why. Possibly it's an incompatible piece of hardware; possibly it's an old driver or two that simply refuse to get along. Possibly the PC is already loaded with viruses or other malicious software and simply doesn't install anything without incident. And possibly, it's simply a combination of hardware and software elements that just don't work together with the upgrades that the service pack installs.

There is, however, one thing that can safely be said for ***any*** Windows service pack installation: If the version of Windows XP already installed on your system doesn't work well, installing a service pack probably won't help. In fact, it might make it worse. Don't install a service pack expecting it to heal your PC, the way installing an antivirus program or a disk repair utility can help. Those programs are designed to take an ailing system and make it healthier. Windows service packs are designed to make the operating system more effective. But service packs are not healers.

Still, there are numerous reasons to install any Windows service pack, but especially Windows XP Service Pack 2. The following sections explain some of the major reasons. The assumption here is that you do not already have Service Pack 1 on your system. For those who do, the text includes notes about what is different in Service Pack 2.

Note

You do not have to install Service Pack 1 before installing Service Pack 2. SP2 contains all the features and fixes of SP1, adding many of its own.

Improved Security

Analysts and critics of Windows XP have continually focused on security issues. As with previous versions of Windows — especially since the popularization of the Internet — XP has been susceptible to hackers, crackers, intruders, and thieves, and this susceptibility has made IT-savvy businesses and users wary of running Windows (including the XP version) on their main production PCs. Service Pack was designed from the outset primarily as an improvement on XP's security, and to that end, it incorporates numerous important security features.

Primary among these security features is the Windows Firewall. To be sure, SP2 doesn't actually represent the first appearance of the Firewall; it appeared, in fact, with the original Windows XP. However, SP2 improves the capabilities of the Firewall along with its default performance. Later in this chapter you look at how to configure the firewall; for now, it's important to note that the firewall is turned on by default in SP2, and that — more important — it has been added to the startup and shutdown processes of Window XP to minimize intrusions from the Internet in the time between the loading of the networking subsystem and the appearance of the desktop. Previously, that time offered a window of opportunity for hackers to break into system and establish control of the network.

The most visible sign of the concern for added security is the Windows Security Center, covered (like the Firewall) in its own section later in this chapter. The purpose of the Security Center is to provide a central interface from which you can see at a glance whether or not Automatic Updates, the Firewall, your browser settings, and your antivirus software are in place, and from which you can configure the features of these security tools. The Security Center loads automatically when you install SP2, encouraging you to take advantage of its controls in order to secure your PC against all possible threats (or at least the ones that it can manage).

Improved Web and Email Functions

For many of us, most of the day is spent on the Web or in email. As a result, email and the Web are the two primary targets for outside intruders. Not all intrusions are malicious, but at the very least, all are inconvenient and are often flat-out annoying. SP2 helps you recover some of the time and energy you've been wasting until now dealing with these annoyances by providing additional features in Windows' two major built-in Internet programs: Internet Explorer (IE) and Outlook Express (OE). Here is a list of the most significant features added to these two programs:

- **Protection from downloads (IE):** One of the classic methods of compromising your PC is for Web pages to initiate procedures to store files on your hard drive. SP2 provides Internet Explorer with an Information Bar, which appears immediately below the Address Bar and informs you each time IE recognizes a potentially harmful download. These downloads typically come from ActiveX controls, but they can include other recognized problem files as well, such as .exe files (program executables). Whenever the Information Bar appears, you can hover the mouse pointer over it to discover what is being called to your attention

and to take action. Two menu items appear: Download File and What's the Risk? Choose the first to override the Information Bar and download the file in question; choose the second to go to the Microsoft site where an explanation page explains what the danger is. In the case of a download, IE causes a Security Warning window to appear, letting you Run or Save the file; in the case of ActiveX controls, it lets you configure IE to accept or reject all such files from specific sources or to ask you every time one appears.

- **Protection from downloads (OE):** Microsoft email products (the full Outlook program in particular) have suffered terribly from their susceptibility to viruses and other malicious code sent as attachments and as images within messages. With SP2, Outlook Express is far more watchful for such code, blocking suspicious attachments and, by default, not displaying graphics in a message opened in a separate window or in the Preview pane. As with IE's Information Bar, you can view the messages by clicking the block notification and instructing OE to download them, but some attachments are simply blocked from download completely. If that happens, and you know the code is valid, you can reply to the sender to have that person reattach and resend them. If you're not certain, be glad that the attachment has been blocked.

- **Control of IE add-ons:** Numerous programs add capabilities to IE to allow you to work with files germane to those programs from within your browser. Typical examples include virus checkers, download utilities, and the unending stream of toolbars available from Google, Yahoo!, MSN, and practically everywhere else. SP2 adds a Manage Add-ons window to IE, accessible via IE's Tools menu. Figure 1-1 shows this utility, in whose viewing pane is displayed all the add-ons currently loaded in IE. Another view, available by clicking the drop-down menu in the Show field, allows you to see what add-ons IE has used, not just those currently loaded. You can click the name of each add-on and choose to Enable or Disable it. If it is an ActiveX object, you can click the Update ActiveX button to have IE go to the manufacturer's site and download the latest version. The most important element here is the capability to disable add-ons because they often result in the worst slowdowns you'll experience when using IE.

- **Protection from the resizing of IE windows:** Few things are more annoying than having your browser window resized simply because you went to a specific Web site and loaded a specific page. Resizing is caused by scripts deliberately encoded to cause the browser window to enlarge (they could shrink it as well, but they never do), a method unscrupulous Web authors use to ensure that you see the pages they want you to see (by hitting you over the eyeballs with them). SP2 gives IE the code needed to stop these scripts from running, thereby eliminating the resizing problem. If you want larger windows, you can resize them yourself.

- **Blocking of popups:** Unwanted resizing of browser windows might be among the most annoying events when Web browsing, but having new windows pop up on their own is infuriating beyond belief. Popups are designed to focus your attention and force you to notice something (usually an ad or a survey) you wouldn't otherwise pay attention to. Popups are intrusive, disruptive, counterproductive, and just plain rude. Numerous toolbars (Google, Yahoo!, MSN) prevent popups from appearing; but with SP2, Internet Explorer can block them as well. And as with all pop-up blockers, you can choose to have the popup appear if you want. After IE has informed you that it has blocked a popup, hold down the Ctrl key while clicking the link, and it will appear as a separate window.

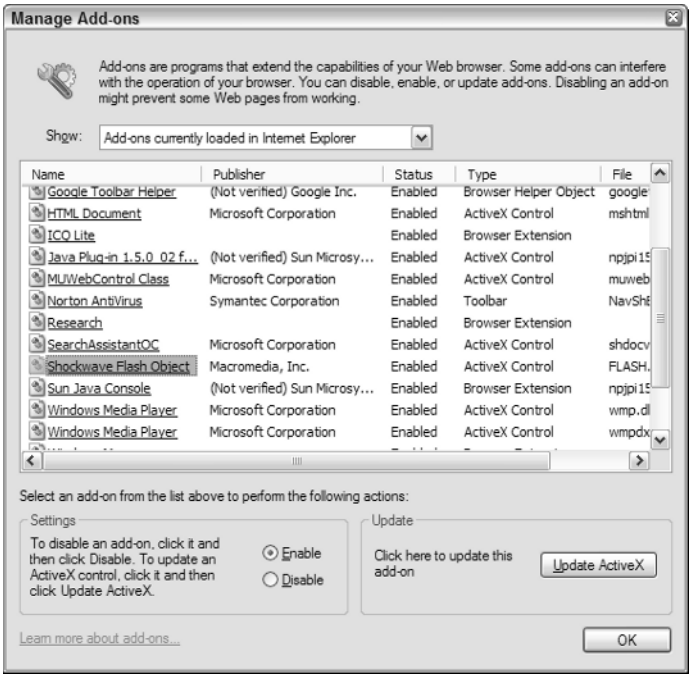

Figure 1-1: Internet Explorer's Manage Add-ons dialog box.

Other Enhancements

The original Windows XP was the first Microsoft OS that offered built-in support for wireless networks, but *Wi-Fi* (Wireless Fidelity, formally known as the IEEE 801.11 networking standard) was relatively new at the time and the support was limited. Service Pack 1 improved the capability of XP machines to connect to wireless LANs, but SP2 makes it easier still. SP2 allows Windows to recognize Wi-Fi broadcasts more reliably, enabling instant connections to public wireless networks in locations such as airports, schools, libraries, coffee shops, and other hotspots. Simply turn on your notebook and wait for XP to offer a choice of connections.

Also in the networking vein, SP2 improves the interplay between XP's networking and the Bluetooth standard. (Bluetooth is the specification for wireless personal area networks.) Whereas it was often previously necessary to spend considerable amounts of time configuring XP in order to have the connection actually work, with SP2 the connections are more frequently immediate. They're not as reliable as Wi-Fi connections, and in fact are often compared to the Wi-Fi capabilities of XP as of Service Pack 1. But if you own Bluetooth equipment, anything's better than what it was like before, so this will come as a particularly pleasant improvement. Whether or not Bluetooth continues to evolve and capture market share remains to be seen, but Bluetooth devices — ranging from keyboards to network adapters and print servers — are certainly appealing for a wide range of reasons. SP2 makes them that much more appealing.

Only one other major enhancement ships with SP2: a new version of Windows Media Player. WMP 10 is covered in detail in Chapter 14, so here I'll simply say that it works more capably with

DVD movies and that it offers numerous music (and other media) download purchases from directly within the program. In addition, facing obvious competition from the iPod, particularly the iPod's ease of building playlists, WMP 10 gives you better tools for organizing your music files.

Using the Windows Security Center

The Windows XP Security Center, which installs with SP2, is an easily accessible, easily comprehended dialog box designed to help you keep your XP installation more secure. It appears automatically after the SP2 installation, providing you with only a few choices, but these choices are crucial for security enhancement.

Figure 1-2 shows the Security Center in action. You can open the Security Center from the Control Panel (click Start, choose Control Panel, and double-click the Security Center icon), and you'll want to do so to configure it to your needs. Notice that Figure 1-2 shows only one possible view of the Security Center; what it actually looks like depends entirely on how you have your own PC configured. For example, if you have none of the displayed component categories installed, you will see buttons allowing you to configure it to include those components once you do install them.

The Security Center has five separate areas, four of which offer configuration options. The following sections provide a rundown of the four configurable areas, along with what to do with them to make your computer more secure.

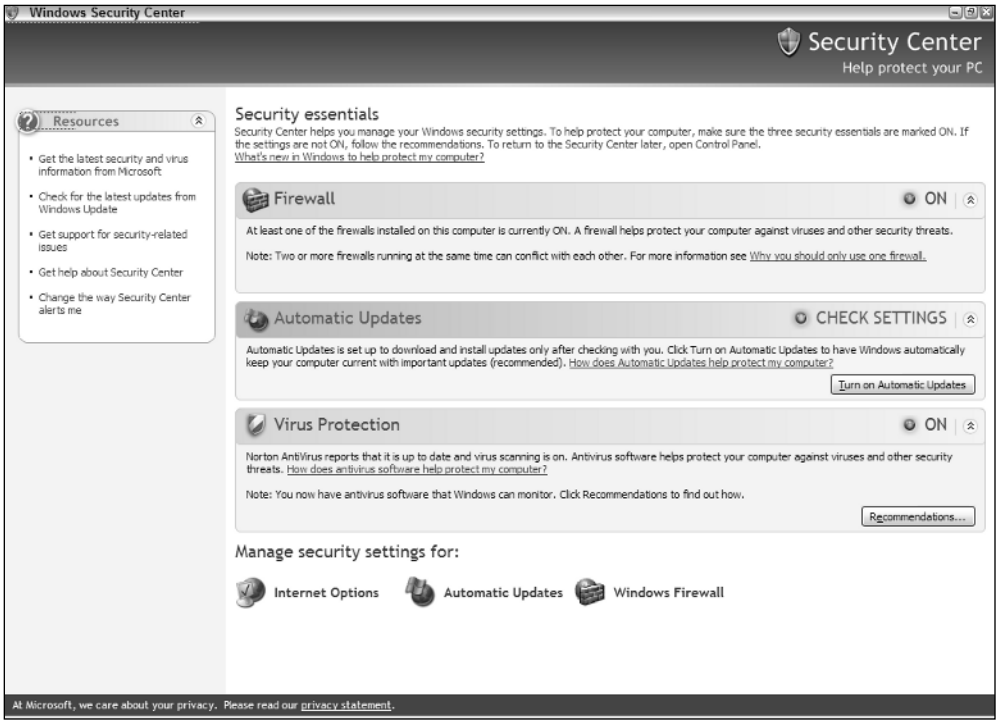

Figure 1-2: Windows XP Security Center installed with SP2.

Resources

The bar on the far left of the Security Center houses the Resources area. At first glance, this area seems nothing more than a set of links to information screens, but in fact, it's more valuable than that. Each of the five links offers its own useful security details:

- **Get the latest security and virus information from Microsoft:** This link leads to the Security home page on the Microsoft site (www.microsoft.com/security/default.mspx). That page, shown in Figure 1-3, provides a wealth of detail surrounding security updates, viruses and other malicious software, and how to configure your PC for the highest possible security. Clicking the link More Security Updates on this page, for example, leads to a list of security bulletins and downloads. Farther down the page (not shown in the figure), the Trustworthy Computing section provides a list of best practices and technology information.
- **Check for the latest updates from Windows Updates:** Clicking this link leads to the Windows Update site (covered in detail in Chapter 5). It's useful to have the link on the Security Center, especially as you get more and more used to checking the Security Center for possible issues surrounding your PC.

Figure 1-3: Microsoft's Security site.

- **Get support for security-related issues:** This link leads directly to the Microsoft Support home page for security issues, a compendium of information about intrusions, viruses, and protection mechanisms. Included here are recent announcements about dealing with security problems, including information about such matters as how to determine if a security warning, received via email or the Web, is genuine.

Caution

When you receive an email message about security or about the need to log in to an account in order to confirm anything at all, **DO NOT COMPLY** unless you are *absolutely* certain the message is legitimate. To determine legitimacy, visit the Web site of the organization or company that apparently sent the information to you, and browse their site for information surrounding fraudulent messages. The general rule of thumb is that sites such as banks, eBay, and any other site that can get their hands on your money will *never* issue such messages. Sending fraudulent messages in order to gain access to your accounts is known as *phishing* and is one of the most dangerous security problems facing computer users today.

- **Get help about Security Center:** Clicking here loads the Windows Help system for the Security Center applet. It's a pretty useless Help page.
- **Change the way Security Center alerts me:** This link opens the dialog box shown in Figure 1-4. Checking each of the options (Firewall, Automatic Updates, and Virus Protection) tells Windows to inform you when your computer might be at risk because of the way you have Security Center configured. Although less useful than the warnings provided by some third-person security utilities, this is certainly a step in the right direction for Windows itself. Notice that the pictured dialog box has the Virus Protection button unchecked; you might choose to do this if your antivirus software already has its own alert system.

Figure 1-4: The dialog box for configuring Security Center alerts.

Firewall

The Firewall area of the Security Center gives you a button for turning Firewall monitoring on or off, as well as a link to a Help screen explaining why you should use only one firewall on your system. The answer to the second point is that different firewalls work differently, to the degree that they might very well prove incompatible with one another. That said, many users have two or even three firewall packages running on their PCs: the Windows Firewall, a third-party firewall (such as ZoneAlarm), and the firewall built into their network routers.

However, if you install a product such as Norton Firewall, the installation strongly recommends that you let the product disable the Windows Firewall automatically. Users attempting to work with both firewalls simultaneously have reported slowdowns and lockups.

The most important Security Center link to the Firewall is in the Manage Security Settings area at the bottom of the screen. Clicking this link yields the Windows Firewall configuration dialog box with its three tabs: General, Exceptions, and Advanced. From here, you control the workings of the Windows Firewall; even if you change nothing, exploring its various screens lets you see what firewalls actually do.

The General tab offers only three choices: On (recommended), Off (not recommended), and Don't allow exceptions. By default, except on Domain installations of SP2, only the first choice is selected. If you install a third-party firewall product that does not automatically disable the Windows Firewall, check the Off radio button and click OK to disable it manually in favor of the newly installed product.

The check box labeled Don't Allow Exceptions tells Windows to ignore any settings under the Exceptions tab, which you come to next. Essentially, checking this box tells Windows to inform you of any and all incoming data from the Internet, no matter what. This setting means that you will have to override every single program with a connection from the Internet, even those such as email and Web browsing that you do all the time. Check it only if you have the time to do such extensive monitoring.

The heart of the Firewall lies in the Exceptions tab. As Figure 1-5 shows, this tab displays a list of some of the programs and services currently installed on your PC (see the following bulleted list for adding others), along with a check mark denoting which ones you are allowing to bypass your firewall. To force Windows to block a program from bypassing the firewall, uncheck its box and click OK. To prevent Windows from even notifying you of such occurrences, uncheck the box at the bottom of the dialog labeled Display a Notification When Windows Firewall Blocks a Program. With this box checked, you have the option of overriding the Firewall each time a block occurs; with this box unchecked, Windows Firewall blocks programs without your intervention (which essentially means that you won't be able to use those programs if their design is to download data).

At the bottom of the dialog box are these four buttons:

- **Add Program:** This button opens the Add Program dialog box, which consists of a list of everything installed on your PC, letting you manually select (or browse for) the programs you want to control via the Firewall. This option is important for adding programs that Windows has not initially determined to perform data downloads but that you know do engage in such activity.
- **Add Port:** This button allows you to declare that data using a specific port, which uses either the TCP or the UDP protocol, will bypass the firewall automatically. The primary use for this option lies with online games that require specific ports to work properly. When you open a port for any purpose, however, you should always return to the Windows Firewall dialog box after using it in order to close it again. Intruders are always looking for open ports — to leave them open invites disaster.

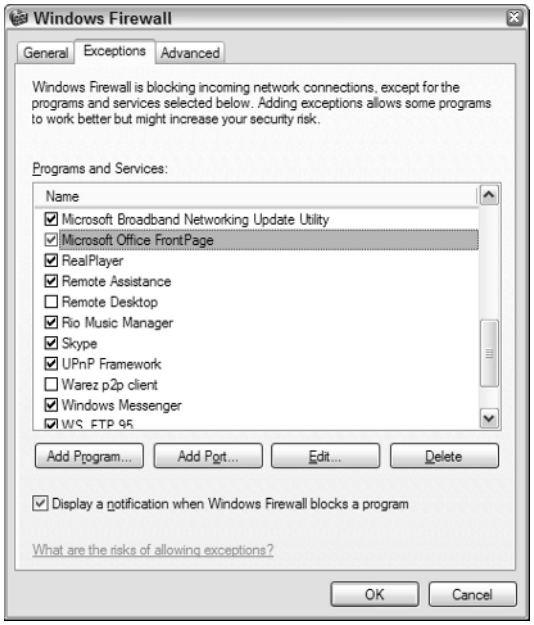

Figure 1-5: Allowing exceptions to Windows Firewall blocking.

- **Edit:** This button shows you the folder path for the program you've selected in the list and lets you change the scope of the exclusion. Figure 1-6 shows the dialog box that appears when you click the Change Scope button (this button is also available when you click the Add Port button). The options are for any computer on the network to allow this program through the firewall, for only those in this computer's subnet (with all PCs outside that subnet blocking the program), or for a customized list of PCs (listed by IP address) that will allow that program to bypass the firewall. If you have only one member of your family or your office who needs to unblock data from a specific program, use this feature to unblock that person's PC address.

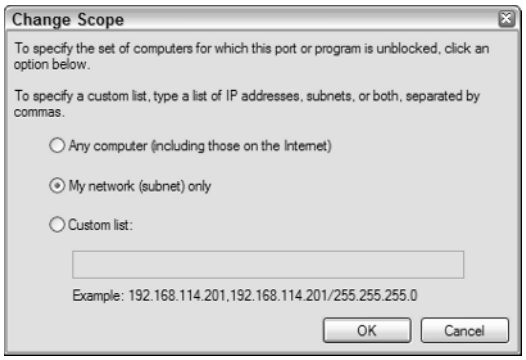

Figure 1-6: The Change Scope dialog box.

- **Delete:** This button gives you the option of deleting a program from the Programs and Services list. Doing so prevents it from being monitored entirely, so before deleting it, consider simply checking it and, therefore, allowing it access as an exception.

The Advanced tab of the Windows Firewall dialog box (see Figure 1-7) offers still more options. In the Network Connection Settings area, you can specify which of the connections shown in your Network Connections folder will use the Windows Firewall. Be aware, however, that unchecking an option renders that connection open to unprotected intrusion. It is possible to allow one or more connections to use the Windows Firewall while other connections use a third-party firewall. There's little (if any) reason to ever do that, though.

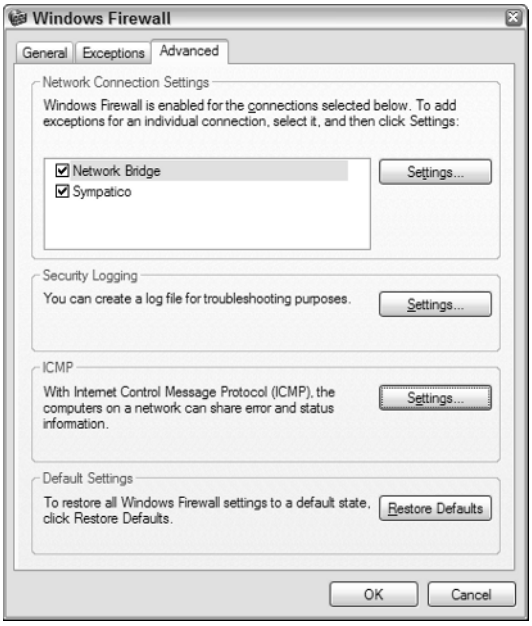

Figure 1-7: The Windows Firewall Advanced tab options.

You can specify the firewalled components of each connection by clicking the Settings button. This opens the Advanced Settings dialog box, with one list of selectable items under the Services tab and another under the ICMP (Internet Control Message Protocol) tab. Each item you choose for inclusion will be available through that specific network connection to anyone who uses that connection. For example, you can specify whether users on that network connection are able to access FTP or Web servers or Windows features such as Remote Desktop.

If you want to study the workings of the Windows Firewall, click the Settings button in the Security Logging area. The resulting Log Settings dialog box lets you specify if you want to log successful connections or dropped data packets, along with where on your system to store the log file created by this option. You can also specify the maximum size of the file, 4MB by default, but as small or as large as you want. With the logging feature turned on, you can open the file at any time

(using any text editor, such as Notepad) to see what the firewall has been doing. The information is highly technical and is primarily useful for troubleshooting purposes. But if you're determined to understand firewalls (and especially the differences among firewalls), the details can be fascinating.

Automatic Updates, Virus Protection, and Manage Security Settings

The Automatic Updates and Virus Protection Settings areas work similarly. Both provide information about what the specific feature does, and both offer a button that lets you turn the feature on. Automatic updates are covered in detail in Chapter 5, and antivirus protection is covered in Chapter 2.

Windows XP does not have any built-in antivirus protection (although rumors persist that it will be added before too long). What the Security Center does, however, is work in conjunction with third-party antivirus packages (from McAfee, Symantec, and so on) to monitor your system continually for attempted viral intrusion. Clicking the Recommendations button (refer back to Figure 1-2) yields a dialog box with only one choice: whether to monitor your antivirus software yourself (the default) or allow Windows XP to do so for you. Check the box if you regularly check your antivirus settings. If you see no Recommendations button, it means that Security Center already knows that the antivirus software is installed and that you want Windows to monitor it.

At the bottom of the Security Center are three links under the heading Manage Security Settings for: Internet Options, Automatic Updates, and Windows Firewall. All three simply open the dialog boxes necessary for configuring these options. Internet Options are discussed in Chapter 9, and Automatic Updates are covered in Chapter 5. The Firewall settings are detailed in the section immediately following this one.

All three dialog boxes are available from the Control Panel; having them in the Security Center is merely a matter of convenience.

Summary

Windows XP Service Pack 2 provides a level of security that no desktop version of Windows has managed to achieve in the past. The Windows Firewall alone is worth the price of admission; however, the Security Center points to a solid future of drawing together the myriad threads of security options that have been available to Windows users for a long time but that have always worked disparately and often at odds with one another. Third-party security solutions remain not only valid but also frequently preferred. But even out of the box — except for the crucial omission of antivirus software — SP2 can render any PC much less vulnerable than before. Simply put, do not let anyone in your office or your household run Windows XP without it.