

Using Windows Update for Windows XP

Introduction

This document provides instructions on updating Windows XP with the necessary patches. It is very important to update your operating system software in order to plug up any existing vulnerabilities and help protect your system from computer virus attacks. This is especially the case if you just bought a new computer or recently reinstalled your operating system.

You need to perform this procedure regardless of whether or not you have been infected with a virus or worm.

How the Procedure Works

- You will be installing components from Windows Update in a specified order. The reason for this is that some components will overwrite the other components if they are installed in the incorrect order.
- If “Already Installed” appears to the right of any of these components, then that component is already installed on your computer and you will not need to install it again. (You can display the installed updates by clicking **Show Installed Updates** from Microsoft’s **Windows Update** Web page.)
- After you perform each install, you will need to reboot your computer.
- Toward the end of this procedure, you will be given the opportunity to install optional components. If you decide not to install these components, you will not affect the vulnerability of your computer.

Before You Begin

The following are required before you can perform this procedure:

- High-speed Internet connection (e.g., Ethernet connection)
- 150 MB of free disk space (to install Windows XP SP1)
- 350 MB of free disk space (to back up your data files)
- Windows XP CD
- Microsoft Office CD (If you are updating Microsoft Office, versions XP and 2000 require the CD)

Downloading and Installing the Windows Update Components

Step 1: Install the Service Pack

A service pack is a downloadable update to your software (e.g., Windows XP) that fixes existing problems (e.g., vulnerability to computer viruses) or provides product enhancements.

Microsoft's **Windows Update** Web page explains the product updates that are available as well as how to download and install the updates.

Open Internet Explorer. Go to the **Windows Update** Web page at <http://windowsupdate.microsoft.com> or select **Windows Update** from the **Tools** menu within Internet Explorer.



You will see a **Security Warning** window appear asking you to whether to accept content from Microsoft Corporation. Click on **Yes** to continue.



Click the link **Scan for updates** so that Windows Update can scan your computer to determine what packages are required for your system.

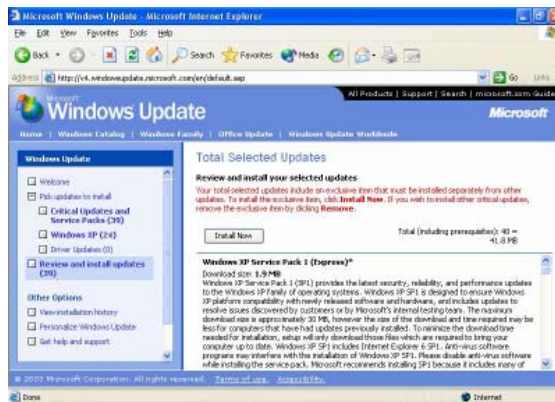


Click **Review and install updates** to begin the download and install process.



NOTE: Owners of new computers may find that Service Pack 1 has already been installed by the manufacturer, and will not need to install it themselves. If you do not see anything about a service pack when the Selected Updates are displayed, you can assume that it has already been installed, and you may continue with **Step 2** below, installing the Critical Updates.

A list of updates that may have been found will be displayed on the screen. If this is the first time you have run **Windows Update**, you will probably see a message like the one at right, in red, which reads: "Your total selected updates include an exclusive item that must be installed separately from other updates. To install the exclusive item, click **Install Now**."



Click **Install Now** and **OK** to confirm that you wish to install Service Pack 1 and accept the license agreement.

You will now be walked through the Setup Wizard for the Service Pack. Click **Next** to continue and agree to the license agreement, clicking **Next** again to continue.

Once the process has completed, click **Finish** to complete the installation process and **OK** to reboot the computer.



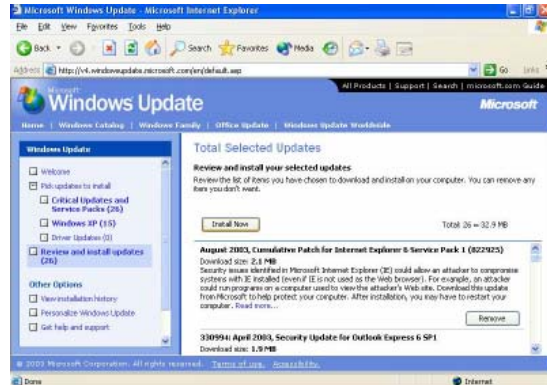
Step 2: Install the Critical Updates

The critical updates are essential patches which have been introduced since the release of Service Pack 1. Failure to install all of the critical updates will leave a machine vulnerable to dozens of methods of attacks.

Once your machine has rebooted, open Internet Explorer and go into **Windows Update**.

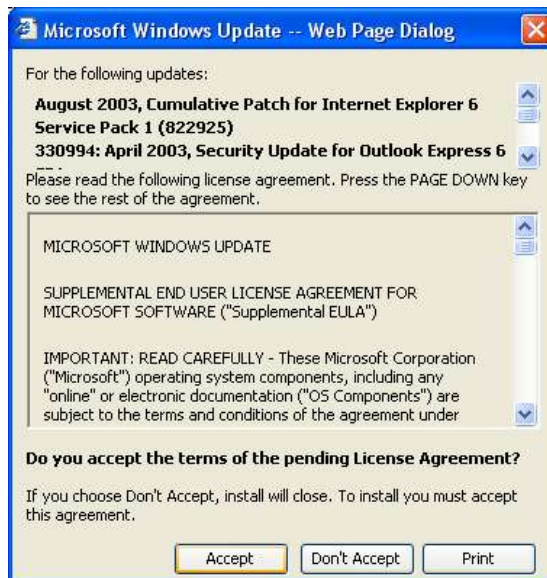
Once the service pack is installed, it should default to the remaining critical updates you need to install.

Click on **Install Now** in order to install the remaining critical updates.



Click on **Accept** in order to agree to the terms of the license agreement.

Once it has finished the installation, you may or may not be prompted to reboot your machine. If you are prompted, you should reboot immediately in order for the changes to take effect on your machine.



Step 3: Install the Microsoft Office Updates

Microsoft Office, especially Outlook, also has many security vulnerabilities.

1. When your computer has rebooted, open an IE browser window and return to the **Windows Update** Web site.

Warning: Before you install any updates, you must disable your anti-virus software.

If you have Symantec AntiVirus, for example, you can disable the File System Realtime Protection feature by performing the following:

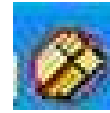
- a. Right click on the icon shown here, located on the far right side of the taskbar.



- b. Select **Enable File System Realtime Protection**.



A red circle and slash appear over the icon.



2. If not already installed, install the following (located under **Recommended Updates**), just as you did for the Critical Updates:
 - a. *Non-Gregorian Calendar Update for Office 2000 SR-1*
3. Click **Product Updates** from <http://office.microsoft.com>. From the **Product Updates** Web page, install the service pack and all security updates. (You can click **Show Installed Updates** to display all the updates that are already installed on your computer.)

Note: You may be asked to insert your Microsoft Office CD to install the updates depending on your version of Office (Office XP and 2000 require it).
4. Download and install the update.
5. Shut down and then restart your computer.
6. If it is still disabled, re-enable Symantec's File System Realtime Protection by following the same procedure listed for disabling it. Once enabled, the red circle and slash will disappear.

Step 4: Check to Make Sure There Are No More Critical Updates

After updating all of your Microsoft software, there may be more Critical Updates that only apply to systems that have installed those updates. Therefore, follow the instructions in Step 2, one more time.

Maintaining a Secure Computing Environment

The most important thing we can do to protect our computers after closing known vulnerabilities is to alter our online behaviors. When there are no vulnerabilities available to exploit via active attacks across the networks, the virus writers must wait for users to provide them an opportunity.

Behaviors You Should Adopt

It is vitally important that you adopt behaviors that will your computer if you have not been attacked by a virus, as well as be able to disinfect your computer if you have been attacked. Safe computing practices include:

- Check for software updates often and check news reports regularly for computer security issues. (See alerts links below in the Resources for Secure Computing section)

- Use virus protection software. (See <http://www.columbia.edu/acis/software/nav>)
- Make regular backups of critical data.
- Change your default settings in your network applications to disable scripting and other insecure “features” (Refer to the resources below for more information).
- Exercise extreme caution whenever receiving data from the Internet, no matter how trusted the source is. (Refer to the resources below for more information)
- Never open an attachment in email without first confirming with the sender that it was intended for you. (Many worms spread via email attachments with forged “from:” addresses.
- Never click on a link sent to you in an email message unless you absolutely trust the source. When in doubt, confirm with the sender that the link is legitimate before you open it, or retype the address into your web browser manually.

Resources for Secure Computing

The following list contains links to sites that help you protect your computer and keep you informed of the latest security-related news and tools.

- http://www.cert.org/tech_tips/home_networks.html
CERT’s guide to Home Network Security.
CERT is part of the Software Engineering Institute (SEI), a federally-funded research and development center operated by Carnegie Mellon University. CERT researches the causes and prevention of system security vulnerabilities and the improvement of system security, publishes information about security issues on its Web site, and develops information and training to incident response professionals and system administrators.
- <http://www.microsoft.com/technet/security/bulletin/notify.asp>
Free e-mail notification service that Microsoft uses to send information to subscribers about the security of Microsoft products. AcIS strongly recommends that you subscribe to this list.
- <http://www.microsoft.com/security>
Microsoft’s “Get Secure and Stay Secure” campaign . This site contains general information about Microsoft’s support of security issues.
- <http://www.microsoft.com/technet/security>
Microsofts’ TechNet Web site. Contains links to security bulletins, the latest security news and technical information, discussion and chat groups, and troubleshooting tips and advice.
- <http://www.securityfocus.com/microsoft>
Contains security-related news, existing vulnerabilities, tools, and mailing lists.
- <http://www.microsoft.com/technet/security/current.asp>
The complete list of vulnerabilities for all Microsoft products.
- 1-866-PC SAFETY

Microsoft's toll-free security support line.

- <http://www.microsoft.com/technet/security/tools/w2kprocl.asp>
Windows 2000 Professional baseline security checklist.
- <http://www.microsoft.com/technet/security/tools/w2ksvrcl.asp>
Windows 2000 Server baseline security checklist.

For information on current threats and alerts:

- AcIS Alerts:
<http://www.columbia.edu/acis/>
- CERT's Advisories:
<http://www.cert.org/advisories/>
- Microsoft Security Bulletins for Microsoft Products:
<http://www.microsoft.com/security/bulletins>