

Three Security Essentials for Your Home PC(s)

While there are many things that can be done to improve the security of home computers and networks, most security experts agree that regardless of the operating system you use (Macintosh, Windows or Linux), the following three techniques are fundamental:

- Keep software up-to-date
- Use a host-based firewall
- Install anti-virus software

Just as you would secure a house by locking the front door *and* all of your windows *and* installing a security system, it is critical to take a multi-layered approach to computer security. Threats seek entry through many access points, especially if you connect to the Internet, which is like a big unsafe neighborhood. The following steps detail how to put security measures in place for a Windows-based PC with connectivity to the Internet.

BEFORE YOU PROCEED:

Make sure you have Microsoft Windows XP Service Pack 2 (SP2) installed. Running SP2 is one of the most important security measures you can take. Furthermore, these instructions may not work unless you are running SP2. Also, please note that these instructions are aimed specifically at students, faculty and staff members at the University of Michigan, who are all covered by the University's anti-virus software license.

WHAT'S IN THIS DOCUMENT

Three Security Essentials for Your Home PC(s)...1

Requirement 1: Keep Software Up-To-Date...2

Requirement 2: Use a Host-Based Firewall...4

Requirement 3: Install Anti-Virus Software...6

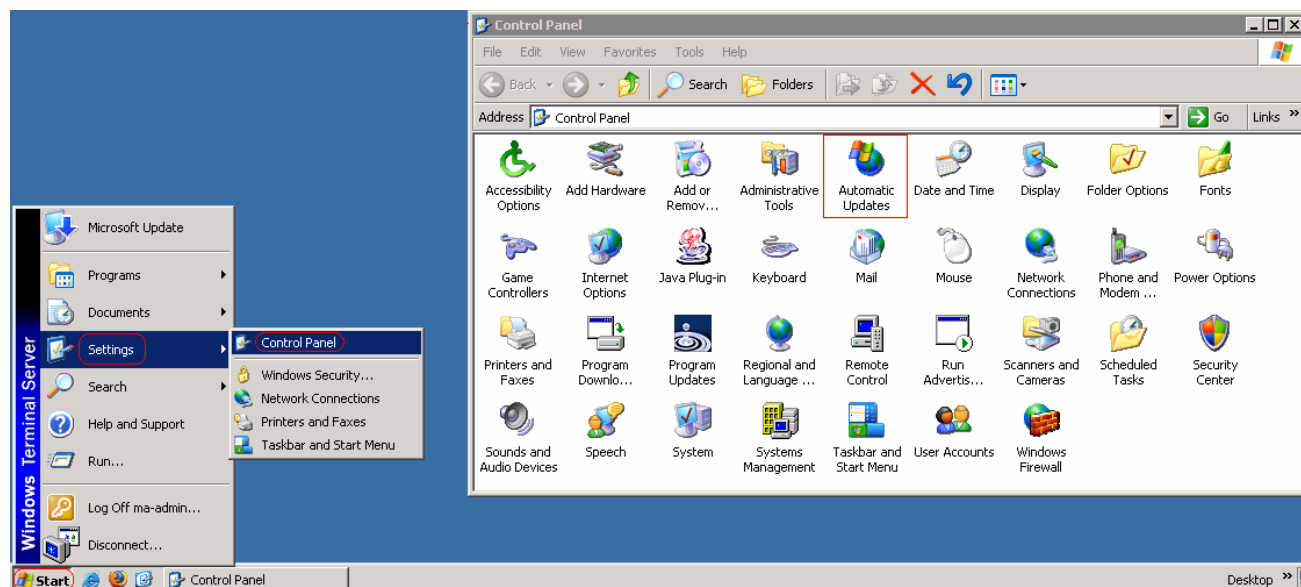
Remember to Monitor...7

Requirement 1: Keep Software Up-To-Date

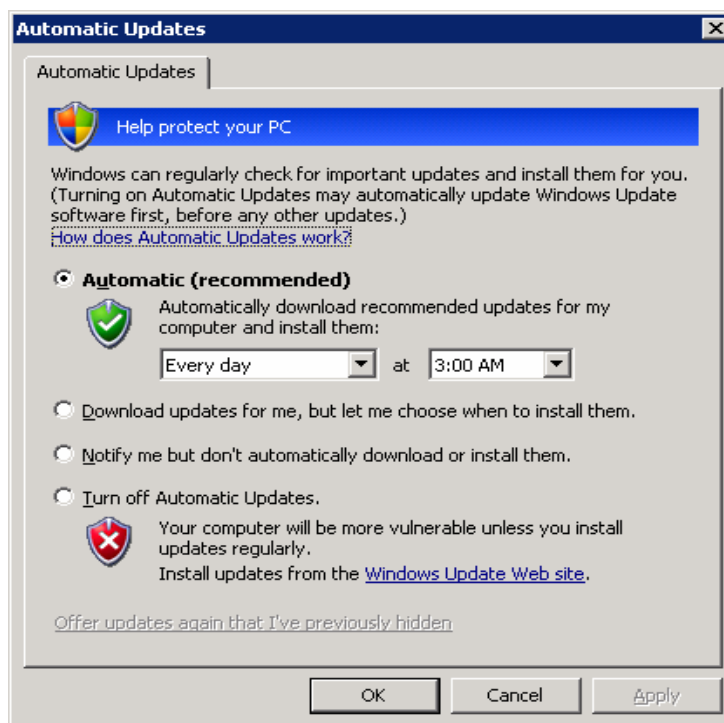
ENABLE AUTOMATIC UPDATES

The best way to keep your system up-to-date is to let Windows do it automatically through Automatic Updates. To enable this:

1. Click **Start** and select **Settings > Control Panel**.
2. In the **Control Panel** window, double-click **Automatic Updates**. The Automatic Updates window displays.



3. Turn on the **Automatic (recommended)** button.



4. Select **Every Day** from the drop-down menu to automatically download and install recommended updates. Click **OK**.

USE MICROSOFT UPDATE INSTEAD OF WINDOWS UPDATE

An important complementary aspect of enabling automatic updates is to configure it to use *Microsoft Update* instead of *Windows Update*. This allows automatic updates to download critical updates for applications that run on Windows, such as Microsoft Office. Windows Update only updates the operating system while Microsoft Update updates both the operating system and Microsoft applications. Microsoft Update does not, however, update non-Microsoft applications.

To enable Microsoft Update:

1. Launch Internet Explorer.
2. Go to <http://update.microsoft.com/microsoftupdate>.
3. Click **Start Now** and follow the instructions.

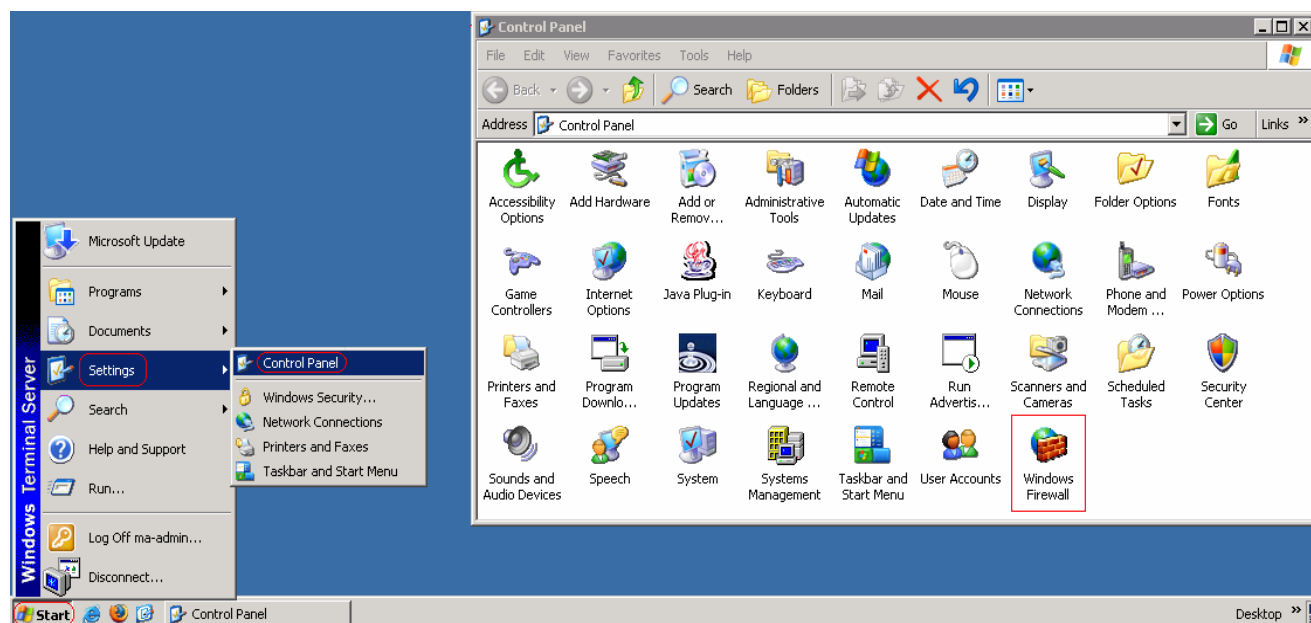
Note: If you see an "Express" and a "Custom" button instead of a "Start Now" button, then your machine is already configured to use Microsoft Update instead of Windows Update.

Requirement 2: Use a Host-Based Firewall

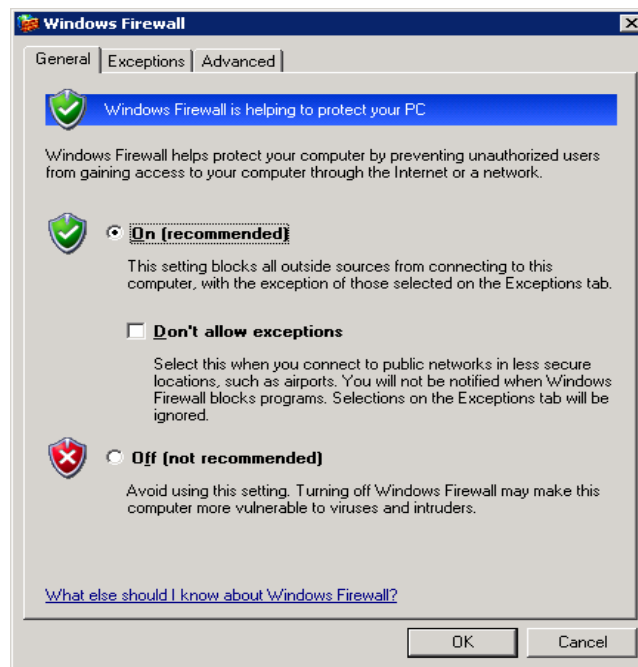
A host-based firewall is a firewall that is running on the computer itself. This is in contrast to an external firewall that may exist on your network between your machine and the Internet.

To use the built-in Windows Firewall:

1. Click **Start** and select **Settings > Control Panel**.
2. In the **Control Panel** window, double-click **Windows Firewall**.



3. If prompted, click **Yes** to start the Windows Firewall/Internet Connection Sharing Service.
4. Turn on the **On (recommended)** button, and click **OK**:



Example of Your Firewall Working

After enabling the firewall, if you run a program such as instant messaging or a multi-player network game that needs to accept information from the Internet, the firewall may ask if you want to block or unblock (allow) the connection.

For example, here is a pop-up that results from launching AOL Instant Messenger:



If you choose to unblock the connection, Windows Firewall will create an exception or "hole" within the firewall so that the pop-up does not occur every time that program is run. Having too many holes in your firewall is detrimental. To learn more about managing firewall exceptions, see:

http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfexceptions.msp.

Requirement 3: Install Anti-Virus Software

For anti-virus information at the University of Michigan, visit <http://virusbusters.itcs.umich.edu>. The University of Michigan maintains a license for members of the University community to use anti-virus software for non-commercial use on their personal and work computers.

As of late 2006, Windows users at U-M can install McAfee's VirusScan product. U-M's installation package keeps the anti-virus software updated automatically and also includes an anti-spyware component.

Remember to Monitor

Now that you've put the automatic update, firewall and anti-virus software into place, remember to periodically monitor their status.

When you log in and use your computer as an administrator you can inadvertently disable the essential security software described here. Periodically check the status of these protection mechanisms by using the Security Center control panel applet.

To check your protection status:

1. Click **Start** and select **Settings > Control Panel**.
2. In the **Control Panel** window, double-click **Security Center**. The Security Center window displays.



This window displays the status of each security measure. In this case, notice that the Firewall and Automatic Updates are enabled, while the VirusScan Anti-Virus software is installed but not running. You can click on the Recommendations button for help in remedying the situation.