



MONMOUTH
— COLLEGE —[®]

Information Systems Center

Protecting Your Personal Computer

March 2008

Table of Contents

Introduction	1
Four Basic Steps to Protect Your Computer	1
Step 1: Keep your Windows operating system up-to-date.....	1
Step 2: Use up-to-date virus protection.	2
Step 3: Use up-to-date spyware protection.....	2
Step 4: Use firewall protection.	3
Protection Tips	4
Tip 1: If you have Windows XP, then install Service Pack 2.....	4
Tip 2: Don't open unknown e-mail attachments.....	4
Tip 3: Don't click on or open unknown links or files in instant messages.....	4
Tip 4: Don't click on buttons inside of pop-up windows.	5
Tip 5: Educate yourself about a program before downloading it.....	5
Tip 6: Don't run your computer as Administrator.	5
Tip 7: Turn off file sharing.....	5
Tip 8: Turn off third-party browser extensions in Internet Explorer.	6
Procedures	6
Create a Non-Administrator User Account.....	6
Windows XP	6
Windows Vista	7
Perform a Full Virus or Spyware Scan.....	7
Windows XP and Vista	7
Scan Your Computer for Windows Updates	8
Windows XP and Vista	8
Turn System Restore Off	8
Windows XP	8
Windows Vista	9
Turn System Restore On	9
Windows XP	9
Windows Vista	10
Turn Off File Sharing	10
Windows XP	10
Windows Vista	10
Turn Off Third-Party Browser Extensions in Internet Explorer	10
Internet Explorer 6.0	11
Internet Explorer 7.0	11

Turn On Automatic Updates	11
Windows XP	11
Windows Vista	12
Turn On the Windows Built-In Firewall	12
Windows XP	12
Windows Vista	12

Introduction

Viruses and other Internet security threats, such as hackers and spyware, can pose serious problems for anyone who owns a computer. Because of this, you should take the security of your computer seriously and do what you can to help keep it protected.

This guide explains four basic steps that you should take to help protect your computer, along with additional protection tips and step-by-step procedures.

Note: Web addresses listed in this guide may change.

Disclaimer: This document is intended for informational purposes only. Monmouth College does not endorse nor guarantee any products listed in this document. Use the techniques and software at your own risk.

Four Basic Steps to Protect Your Computer

The four basic steps that you should take to help keep your personal computer free of viruses and spyware are:

1. Keep your Windows operating system up-to-date with the latest security patches.
2. Use up-to-date virus protection and scan your computer regularly for viruses.
3. Use up-to-date spyware protection and scan your computer regularly for spyware.
4. Use firewall protection.

Step 1: Keep your Windows operating system up-to-date.

Whenever a new vulnerability (a.k.a. security hole) is discovered in the Windows operating system, Microsoft will issue a security patch (i.e., fix) for it. These security patches prevent worms and hackers from accessing your system, and they also prevent some spyware from installing on your computer.

If you are not sure whether your computer has the latest security patches, then scan it for updates. (For directions, see **Scan Your Computer for Windows Updates** on page 8.)

To ensure that your computer always has the latest security patches, you should turn on Automatic Updates. When you do this, all critical Windows updates automatically will be downloaded and installed on your computer. (For directions, see **Turn On Automatic Updates** on page 11.)

Step 2: Use up-to-date virus protection.

Using up-to-date virus protection means that you are using the latest definition files for your anti-virus software. (A virus definition file is a database of known viruses that the anti-virus software uses when it examines your computer. As new viruses are discovered, virus definition files are updated by the software providers, and this happens frequently. Therefore, it is **EXTREMELY** important to keep your anti-virus software updated. If you don't, then your computer will be vulnerable to new viruses!)

You should scan your computer for viruses at least once a week or whenever you hear of a new virus. To ensure that your computer is scanned on a regular basis, set your anti-virus software to perform automatic weekly scans.

IMPORTANT! To help ensure that all viruses are truly detected and removed from your computer, follow the instructions listed under **Perform a Full Virus or Spyware Scan** on page 7.

If you do not have virus protection on your computer, then we recommend that you download and install **AVG Anti-Virus**, which is free and available at <http://free.grisoft.com/freeweb.php/>

Other free anti-virus programs that we recommend include:

Program	Web Address
avast! Antivirus – Scans and removes viruses	http://www.avast.com/eng/download-avast-home.html
McAfee Stinger (Stinger removes only about 38 viruses, so it should not be used as your sole means of virus protection.)	http://vil.nai.com/vil/stinger
Symantec Security Check – Scan only	http://security.symantec.com/sscv6/home.asp
McAfee FreeScan – Scan only	http://us.mcafee.com/root/mfs/

Anti-virus programs available for purchase that we recommend include:

Program	Web Address
Panda Antivirus	http://www.pandasecurity.com/homeusers/downloads/
Norton AntiVirus	http://www.symantecstore.com/
McAfee VirusScan	http://us.mcafee.com/root/package.asp?pkgid=100

IMPORTANT! Do not install more than one anti-virus program on your computer. If you have old or expired anti-virus software, then you must uninstall it before installing a new anti-virus program.

Step 3: Use up-to-date spyware protection.

Spyware programs can make your system unstable and cause other problems. They are usually unknowingly installed on your computer when you download free programs

from the Internet. They can also install automatically if you don't have your Windows operating system up-to-date with the latest security patches or when you click on buttons in pop-up windows.

You should scan your computer for spyware at least once a week using up-to-date definition files. (Like virus definition files, spyware definition files are updated as new spyware programs are discovered.)

IMPORTANT! To make sure that all spyware is truly detected and removed from your computer, follow the instructions listed under **Perform a Full Virus or Spyware Scan** on page 7.

If you do not have anti-spyware software on your computer, then we recommend that you download and install the following free programs:

Program	Web Address
Spybot Search & Destroy	http://www.safer-networking.org
Ad-Aware	http://www.lavasoftusa.com/products/ad_aware_free.php
Windows Defender	http://www.microsoft.com/athome/security/spyware/software/

Note: While you should never have or use more than one anti-virus program on your computer, you can use multiple anti-spyware programs. Just be sure to run each scan separately (i.e., do not run multiple spyware scans at the same time).

Step 4: Use firewall protection.

A firewall is software or hardware that prevents unauthorized access to your computer from hackers, worms, and other Internet security threats.

If you have Windows XP with Service Pack 2 or Vista, then you can use the built-in firewall, which is turned on by default. If you have Windows XP with Service Pack 1, then you'll need to turn on the built-in firewall. (For directions, see **Turn On the Windows Built-In Firewall** on page 12.)

If you do not have Windows XP or Vista and do not have firewall protection, then we recommend that you download and install **ZoneAlarm**, which is free and available at http://www.zonelabs.com/store/content/catalog/products/sku_list_za.jsp?lid=pdb_za1.

IMPORTANT! Unless you are familiar with how to configure multiple firewalls, do not install or use more than one firewall program on your computer. If you have Windows XP with Service Pack 2 or Windows Vista and you want to use a third-party firewall program, then be sure to turn the built-in Windows firewall off.

Protection Tips

Below are additional tips to help keep your computer protected against viruses and other Internet security threats.

1. If you have Windows XP, then install Service Pack 2.
2. Don't open unknown e-mail attachments.
3. Don't click on or open unknown links or files in instant messages.
4. Don't click on buttons inside of pop-up windows.
5. Educate yourself about a program before downloading it.
6. Don't run your computer as Administrator.
7. Turn off file sharing.
8. Disable third-party browser extensions in Internet Explorer.

Tip 1: If you have Windows XP, then install Service Pack 2.

Windows XP Service Pack 2 (SP2) provides better protection against viruses and other Internet security threats.

Note: If you are not sure whether you have Service Pack 2, then you can check by opening the **Control Panel** and double-clicking on the **System** icon.

If you don't have Service Pack 2, then you can download it from <http://windowsupdate.microsoft.com>.

Tip 2: Don't open unknown e-mail attachments.

If you receive an e-mail attachment from someone you don't know, then don't open it. The best thing to do is to just delete it. If you receive an attachment from someone you do know and you are not certain what the attachment is, then contact the person before opening it. It's much better to be safe than sorry!

Tip 3: Don't click on or open unknown links or files in instant messages.

To help keep your personal computer protected against instant message viruses, you should NEVER open an unknown file sent to you in an instant message, even if it's from someone you know. You should also be extremely cautious about clicking on links in an

instant message. If you're not absolutely certain what a file or link is, then contact person who sent it and ask before opening or clicking on it. It's much better to be safe than sorry!

Tip 4: Don't click on buttons inside of pop-up windows.

Clicking on any type of button in a pop-up window (e.g., an OK or Cancel button) may cause spyware to install on your computer. Always close a pop-up window by clicking on the **Close** (X) button in the upper-right corner of the window or by clicking on its taskbar button and selecting **Close**.

Tip 5: Educate yourself about a program before downloading it.

Before you download a program, conduct a Google search on it to see if any other programs, such as spyware, come bundled with it.

Also, read the program's licensing agreement or Read Me files before downloading it. The licensing agreement or Read Me files often contain information about other programs that may be bundled with the software. (Be aware, however, that not all software provides information regarding bundled programs!)

Tip 6: Don't run your computer as Administrator.

Running your computer as Administrator is risky because important areas of the file system and registry database are left unprotected and vulnerable to damage from viruses.

You should only use the Administrator account to perform special tasks that require you to do so (e.g., turning on Automatic Updates and installing software).

For directions on how to create a non-administrator user account, see **Create a Non-Administrator User Account** on page 6.

Tip 7: Turn off file sharing.

Your computer may be set to allow other computers to access your hard drive in order to share files. This can put you at risk for becoming infected or hacked.

For directions on how to turn off file sharing on your computer, see **Turn Off File Sharing** on page 10.

Tip 8: Turn off third-party browser extensions in Internet Explorer.

Turning off third-party browser extensions in Internet Explorer will prevent some spyware programs from installing on your computer.

Note: Some legitimate toolbars (e.g., the Google, eBay, and Yahoo toolbars) may be disabled by this step.

For directions on how to turn off third-party browser extensions, see **Turn Off Third-Party Browser Extensions in Internet Explorer** on page 10.

Procedures

Create a Non-Administrator User Account

Windows XP

1. Click on the **Start** button and select **Control Panel**.
2. If necessary, click on **Switch to Classic View**.
3. Double-click on **User Accounts**.
4. Under **Pick a task**, select **Create a new account**.
5. Enter a name for the account.
6. Click on the **Next** button.
7. Under **Pick an account type**, select **Limited**.
8. Click on the **Create Account** button. The account appears listed under **Pick an account to change**.
9. Click on the account icon.
10. Under **What do you want to change...**, click on **Change the password**.
11. In the **Type a new password** field, enter a password for the account.
12. In the **Type the new password again to confirm** field, enter the password again.

13. In the **Type a word or phrase to use as a password hint** field, enter a password hint.
14. Click on the **Create Password** button.
15. Log off and log back on using the new account.

Windows Vista

1. Log on as Administrator.
2. Click on the **Start** button and select **Control Panel**.
3. Click on **User Accounts and Family Safety**.
4. Click on **User Accounts**.
5. Click on **Manage another account**.
6. Click **Create a new account**.
7. Enter the name for the user account.
8. Click on **Standard user**.
9. Click **Create Account**.
10. Select the new account to configure it.
11. Click on **Create a Password**.
12. Enter the password.
13. Click on **Create**.
14. Log off and log back on using the new account.

Perform a Full Virus or Spyware Scan

Windows XP and Vista

Note: The procedure below should be followed when your computer is infected with viruses or spyware or when you think that it might be infected.

1. Make sure that your virus or spyware definition files are up-to-date.

2. Physically disconnect the computer from your Internet service (i.e., unplug the data or phone cable).
3. Turn off System Restore. (For directions, see **Turn System Restore Off** on page 8.)
4. Perform a full system scan and remove any virus or spyware programs that are found.
5. Reboot the computer.
6. Perform another scan and remove any more virus or spyware programs that are found.
7. Repeat steps 5 and 6 until no virus or spyware programs are found.
8. Turn on System Restore. (For directions, see **Turn System Restore On** on page 9.)
9. Reconnect the computer to your Internet service (i.e., plug the data or phone cable back in).

Scan Your Computer for Windows Updates

Windows XP and Vista

1. Log on as Administrator.
2. Open your Web browser and go to <http://windowsupdate.microsoft.com>.
3. Click on **Scan for updates**.
4. Download and install all of the items listed under **Critical Updates**.

Turn System Restore Off

Windows XP

1. Click on the **Start** button and select **Control Panel**.
2. If necessary, click on **Switch to Classic View**.
3. Double-click on the **System** icon.
4. Click on the **System Restore** tab.

5. Check the **Turn off System Restore** checkbox.
6. Click on the **OK** button.
7. Restart the computer.

Windows Vista

1. Click on the **Start** button and select **Control Panel**.
2. Click on **System and Maintenance**.
3. Click on **System**.
4. Click on **System Protection** in the left-hand task list.
5. Uncheck the checkboxes next to each hard drive listed under the **Create restore points automatically on the selected disks:** section.
6. Click on the **Turn System Protection Off** button for each disk that you uncheck.
7. Click on the **Apply** button.
8. Click on the **OK** button.

Turn System Restore On

Windows XP

1. Click on the **Start** button and select **Control Panel**.
2. If necessary, click on **Switch to Classic View**.
3. Double-click on **System**.
4. Click on the **System Restore** tab.
5. Uncheck the **Turn off System Restore** checkbox.
6. Click on the **OK** button.
7. Restart the computer.

Windows Vista

1. Click on the **Start** button and select **Control Panel**.
2. Click on **System and Maintenance**.
3. Click on **System**.
4. Click on **System Protection** in the left-hand task list.
5. Check the checkboxes next to each hard drive listed under the **Create restore points automatically on the selected disks:** section.
6. Click on the **Apply** button.
7. Click on the **OK** button.

Turn Off File Sharing

Windows XP

1. Click on the **Start** button and select **Control Panel**.
2. Double-click on **Network Connections**.
3. Right-click on **Local Area Connection** and select **Properties**.
4. Uncheck the **File and Printer Sharing for Microsoft Networks** checkbox.
5. Click on the **OK** button.

Windows Vista

1. Log on as Administrator.
2. Click on the **Start** button and select **Control Panel**.
3. Double-click on **Network and Sharing**.
4. Under **File Sharing**, click on **Turn off file sharing**.
5. Click on the **Apply** button.

Turn Off Third-Party Browser Extensions in Internet Explorer

Note: Some legitimate toolbars (e.g., the Google, eBay, and Yahoo toolbars) may be disabled by this step.

Internet Explorer 6.0

1. Open **Internet Explorer**.
2. Click on the **Tools** menu and select **Internet Options**.
3. Click on the **Advanced** tab.
4. Under **Browsing**, uncheck the **Enable third-party browser extensions (requires restart)**, **Enable Install On Demand (Internet Explorer)**, and **Enable Install On Demand (Other)** checkboxes.
5. Click on the **OK** button.

Internet Explorer 7.0

1. Open **Internet Explorer**.
2. Click on the **Tools** menu and select **Internet Options**.
3. Click on the **Advanced** tab.
4. Under **Browsing**, uncheck the **Enable third-party browser extensions** checkbox.
5. Click on the **OK** button.
6. Restart the computer.

Turn On Automatic Updates

Windows XP

1. Log on as Administrator.
2. Click on the **Start** button and select **Control Panel**.
3. If necessary, click on **Switch to Classic View**.
4. Double-click on the **Automatic Updates** icon.
5. If you have Service Pack 1, then click on the **Keep my computer up to date** checkbox, click on the **Automatically download the updates...** button, and specify the day and time that you want the updates downloaded and installed.

If you have Service Pack 2, then click on the **Automatic** button and select the day and time that you want the updates downloaded and installed.

6. Click on the **OK** button.

Windows Vista

1. Log on as Administrator.
2. Click on the **Start** button and select **Control Panel**.
3. Double-click on **Security**.
4. Click on **Turn automatic updating on or off**.
5. Specify when you want updates installed.
6. Click on the **OK** button.

Turn On the Windows Built-In Firewall

Windows XP

IMPORTANT! If you are using a third-party firewall, then **DO NOT** use the built-in Windows firewall. (Unless you are familiar with how to configure multiple firewalls, you should not install or use more than one firewall program on your computer.)

Note: If you have Service Pack 2, then the built-in firewall is already turned on by default.

1. Click on the **Start** button and select **Control Panel**.
2. If necessary, click on **Switch to Classic View**.
3. Double-click on the **Windows Firewall** icon.
4. On the **General** tab, click on the **On** button.
5. Click on the **OK** button.

Windows Vista

IMPORTANT! If you are using a third-party firewall, then **DO NOT** use the built-in Windows firewall. (Unless you are familiar with how to configure multiple firewalls, you should not install or use more than one firewall program on your computer.)

Note: The built-in firewall should already be turned on by default.

1. Click on the **Start** button and select **Control Panel**.

2. Click on **Security**.
3. Click on **Windows Firewall**.
4. Click on **Turn Windows Firewall On or Off**.
5. Click on **On (recommended)**.
6. Click on the **OK** button.