

Protect and Clean your Computer

Windows 2000

These basic steps will remove viruses and most spyware from your computer. **Some infections are so embedded that additional expertise may be needed to remove them manually.** If after following these instructions, your computer still exhibits signs of infection, you may be required to make an appointment with IT-User Services to clean your system for a charge. Please direct questions to the IT Help Center at 831-6000.

On a computer with Internet access:

A. Print and complete ALL these instructions.

If you have any questions, please contact the IT Help Center at 831-6000.

B. Download the following files to Removable Media – a jump drive/ memory stick or a CD as follows:

Type in the web address and hit **Enter**. When the page loads, click the download link and choose **Save**, and then **Save it to Disk**. In the **Save In** window, use the arrow in the dropdown box to point to your Removable Media, and then click **Save**.

Are you an off-campus user connecting through another ISP?

- a) Go to <http://www.udel.edu/topics/virus/mcafee/> and click the link for UD community members using another ISP.
- b) Authenticate using UD's Web proxy server and then continue below.

1) UD McAfee program–

<http://www.udel.edu/topics/virus/mcafee/win/2000xp.html>

The download link “**Install VirusScan for Windows NT/2000/XP**”, appears in step 3 on this page.

File name: **vscan8.exe**

2) UD McAfee SuperDat file-

<http://www.udel.edu/topics/virus/mcafee/win/tools.html>

File name: **sdat####.exe** (where #### is the SuperDAT definition number)

3) Lavasoft's Ad-Aware SE Personal-

<http://www.lavasoftusa.com/support/download/>

Click the top-right link “**Download your free copy of Ad-Aware at Download.com**”.

On download.com, click “**Download Now**” and “**Save it to Disk**”.

File name: **aawsepersonal.exe**

4) Lavasoft's Ad-Aware SE Personal Latest Definitions File

<http://www.lavasoftusa.com/support/download/>

Click the link under “**Latest Definitions File**” next to “**Updates**”.

File name: **defs.zip**

5) **SpywareBlaster**- <http://www.javacoolsoftware.com/spywareblaster.html>

Choose the download site of **Download.com** site.

File name: **spywareblastersetup32.exe**

6) **Batch file to Disable System Services:**

<http://www.udel.edu/topics/virus/security/DisableServices.bat>

After typing in this URL address, do **File-Save**. In the Save Window point to your Removable Media and click **Save**.

File name: **DisableServices.bat**

7) **Winsock Fix to initialize TCP/IP network settings:**

<http://www.udel.edu/topics/spyware/winsockfix.html>

The download link appears in Step 1.

File name: **WinsockFix.exe**

8) **If you think you have an AIM virus, download the AIM Fix tool at:**

<http://www.jayloden.com/VirusClean.htm>

Review the Removal/Information links for specific instructions on dealing with certain AIM infections.

File name: **AIMFix.exe**

C. Verify that these files are on the Removable Media by double-clicking My Computer and then the appropriate drive:

vscan8.exe
sdat####.exe
aawsepersonal.exe
defs.zip
spywareblastersetup32.exe
DisableServices.bat
WinsockFix.exe
AIMFix.exe

On your computer, perform the following steps:

1. Use up-to-date McAfee Anti-Virus Software.

A. Remove any virus and security software.

Some software conflicts with McAfee VirusScan. If your computer has **other anti-virus software (Norton,AVG,etc)**, you should **remove that software before installing the UD-customized version of McAfee VirusScan**. You should also remove copies of McAfee VirusScan that are from **other sources** than the University of Delaware: a promotional copy that came with your computer, a copy that you purchased with a retail license, or a copy from a previous school or employer. The installation of the University of Delaware copy of McAfee

VirusScan 8 will automatically remove the UD copy of VirusScan 7 during the installation process.

1. Begin at the **Start** button.
2. Choose **Settings**, then **Control Panel**.
3. Double-click the icon for **Add/Remove Programs**.
4. Highlight the name of the first program you wish to remove, then click **Add/Remove**.
5. Highlight the names of **other** programs you wish to remove, one by one, then click **Add/Remove**.
6. When you are finished, close the **Add/Remove Programs** window.
7. When you are finished removing programs, if prompted to do so, reboot your

B. Run Disk Cleanup to delete temporary files.

1. Click **Start**.
2. Click **Programs | Accessories | System Tools | Disk Cleanup**.
3. Select the drive you want to clean up. The default will be C:.
4. Disk cleanup will calculate free space, which may take a few minutes.
5. After the calculation is complete, confirm that **only** the following checkboxes are checked:
 - * **Downloaded Program Files**
 - * **Temporary Internet Files**
 - * **Recycle Bin**
 - * **Temporary Files**
6. Click **OK** and **Yes** when prompted to delete files. Disk cleanup will delete the files and close automatically when finished.

C. Install UD McAfee and SuperDAT file.

1. Open your Removable Media drive. Double-click the **vscan8.exe** program file to install McAfee.
2. When the Winzip Self-Extractor is done, it will automatically install and run the VirusScan software.

If your computer is infected with certain viruses and worms, McAfee's software will not be able to install itself until those viruses and worms are cleared using a program called **Stinger**. If you cannot install McAfee, go to <http://www.udel.edu/topics/virus/mcafee/win/2000xp.html> - step 12 for further directions.
3. When you see the message **McAfee VirusScan Setup completed successfully**, click **OK**.
4. You will see a batch screen letting you know McAfee is installing and the virus definitions are installing
5. In order to complete the McAfee installation, you will need to reboot your computer. When asked if you would like to reboot now, select **Yes**. You **must run a manual scan** after installation.
6. Open your Removable Media drive. Double-click the **sdat####.exe** program file. Click **Next** through the SuperDAT wizard to update your McAfee definitions to the latest level.

D. Scan for viruses.

This step will scan your computer's disks for infected files. Any files that can be cleaned will be retained. Any infected files that cannot be cleaned will be deleted. If for any reason you are

unable to run a scan or if McAfee cannot clean or delete an infected file, **Boot into Safe Mode** (see Appendix A at the end of this document) **and Run a Scan in Safe Mode** (See Appendix B).

1. Right-click the V-shield icon in the bottom right system tray.
2. Click (left-click) **VirusScan Console...**
3. Right-click **Scan All Fixed Disks**.
4. Click (left-click) **Start**.
5. VirusScan will take between five minutes and several hours to scan your computer's disks.
6. Close VirusScan when the scan is complete.
7. To be sure that your computer is clean, re-boot your computer, and follow steps 2-6 to scan your computer a second time.

3. Remove & protect against Spyware.

A. What is Spyware?

Applications such as spyware and malware are installed on your computer—typically without your knowledge—to gather and refer information about you to advertisers and other interested third parties. Without your knowledge, spyware and malware can be easily installed when you access certain web sites or download certain programs (e.g., Kazaa). Spyware slows down your computer, slows down our campus network, significantly increases pop-ups and can cause your browser to open to a different or undesirable web site (called "hijacking").

B. Removing Spyware

1. Double-click the Ad-Aware program file on Removable Media to install it. You will see the Ad-Aware SE Personal setup screen.
2. The screen instructions indicate that you should close all Windows applications before you begin the installation process. After you do so, click **Next**. You will see the **License Agreement** screen.
3. Click the check box near the bottom of the screen in front of **I accept the license agreement**.
4. Click **Next**. You will see the **Destination Location** dialog box.
5. Click **Next**. You will see the **Start Installation** dialog box.
6. Click **Next**. The installation process may take a few minutes depending on the speed of your computer.
7. Click **Finish**. The **Ad-Aware SE Personal** help file will open and the application will automatically begin to scan your computer for spyware.
8. Click **CANCEL** immediately to end this scan. Close the Ad-Aware program.

9. Open your Removable Media drive. Double-click the file **defs.zip**, which is the latest Ad-Aware Spyware definition file. It will unzip and create the file "**defs.ref**". Click to select this file. On the left side of the window, click "**Copy this file**". In the "Copy Items" window that appears, navigate to and click on the folder:

c:\programs\Lavasoft\Ad-Aware SE Personal

Click the **Copy** button. **If asked if you want to replace the existing file, click YES.**

10. Start the Ad-Aware program (Go to Start-All Programs-Lavasoft Ad-Aware SE Personal- Ad-Aware SE Personal).

11. Click "**Scan Now**". Select "**Perform Full System Scan**" and click **Next**.

12. If Ad-Aware detects a potential spyware application on your computer, you will hear a sound.

13. Click **Next**.

14. To delete the item(s) from your computer, **right-click in the checkbox** in front of the name of **any** of the objects listed.

15. From the list, click **Select All Objects**. Ad-Aware will indicate how many spyware objects it detected. You will see a dialog box confirming the number of objects to delete and whether you want to continue.

16. Click **OK** to delete the spyware item(s) from your computer.

17. If you see a dialog box that one or more of the objects cannot be deleted immediately, click **OK** in the dialog box to have those objects deleted at reboot.

Having problems connecting after removing all spyware?

Try the **Winsock Fix** to initialize your TCP/IP network settings and restore your connection:

- a. Copy **WinsockFix.exe** from your removable media to your desktop.
- b. Double-click **WinsockFix.exe** to execute.
- c. Click the **Fix** button
- d. Restart your computer.

C. Preventing Spyware

SpywareBlaster, a freeware program produced by Javacool, will help prevent much of the spyware from being installed on your computer.

1. Double-click the SpywareBlaster setup file to begin installation. You will see the **Welcome** screen.

2. Click **Next**. You will see the **License Agreement** dialog box.

3. Click in the radio button in front of **I accept the agreement**. You will see the **Select Destination** Location dialog box.

4. Click **Next**. You will see the **Select Additional Tasks** dialog box.

5. Click **Next**. You will see the **Ready to Install** dialog box.

6. Click **Install**. You will see the **Completing the Setup Wizard** screen.

7. Click **Finish**. You will see the **Getting Started—Enabling Protection** dialog box.

8. Click **Next**. You will see the **Getting Started—Keeping Up-to-Date** dialog box.

9. Click **Next**. You will see the **Getting Started—Thank you** dialog box.

10. Click **Finish**. You will see the **SpywareBlaster Protection** dialog box.

If your computer CANNOT access the Internet,

Under **Quick Tasks** (in the bottom half of the dialog box), click **Enable All Protection**.

When your Internet access is restored, complete the steps below.

If your computer CAN access the Internet,

a. Under **Quick Tasks** (in the bottom half of the dialog box), click the **Download Latest Protection Updates** link.

b. Click the **Check for Updates** button.

c. If updates are provided, click the **Enable All Protection for Unprotected Items** link.

11. Close SpywareBlaster. On your computer's desktop, you will see the SpywareBlaster desktop icon.

D. Think you have an AIM virus?

1. Run the free AIM Fix tool downloaded from <http://www.jayloden.com/VirusClean.htm>. Review the Removal/Information links for specific instructions on dealing with certain AIM infections.
2. This tool may fix problems associated with AIM but may NOT fix all problems caused by the infection. Some AIM bots disable security settings, leaving your system vulnerable to attacks.
3. Be sure to complete all items on this *Protect & Clean your Computer* checklist to keep your computer protected.
4. You may need to re-install your operating system to completely remove this infection and restore your system settings

4. Update Windows / Microsoft software and configure future automatic updating.

Download/install critical updates that Microsoft has released for the Windows operating system and configure future automatic updating.

If your computer CAN access the Internet, go to <http://www.udel.edu/topics/windowsxp/XPupdate.html> and complete ALL steps.

If your computer CANNOT access the Internet

1. **Go to Start – Control Panel – System.**

If the control panel is displayed in Category View, you can either select Switch to Classic View and then select System, or you can select the Performance and Maintenance category, then select System, and then select the Automatic Updates tab.

2. In the dialog window, make sure there is a check in the box next to "**Keep my computer up to date. With this setting enabled, Windows Update software may be automatically updated prior to applying any other updates.**"

3. In the **Settings** pane, select the third option. (**Automatically download the updates, and install them on the schedule that I specify.**) Choose a time of day when your computer is generally turned on. Your computer will automatically check for updates at that time every day and install them as necessary. **This is the recommended method.**

4. Click **OK** when you are finished.

5. *As soon as you have Internet access,*

Go to <http://www.udel.edu/topics/windowsxp/XPupdate.html> and complete Steps 1-14 to manually update your computer with the latest Microsoft Critical Updates.

Whenever you see an '**Updates are ready for your computer**' balloon in the lower right corner of your screen, always **install the updates immediately.**

5. Setup Desktop Security.

A. Password-protect all accounts on your computer.

Change your Account Password:

1. After logging on, press the CTRL + ALT + DEL keys together.
2. Click the Change Password button in the dialog box that appears.
3. Type your old password and the new password twice, as indicated.

4. After completing this successfully, use this new password every time you logon to your computer. After logging on,

Change the Administrator Account password and check for any other accounts:

1. Go to the **Start** menu and choose **Settings** and then **Control Panel**.
2. Double-click the **Users & Groups** icon.
3. Highlight the username **Administrator** in the white box and click **Set Password**.
4. You may need to verify the old password and supply a new password (twice) for the Administrator account.
5. Repeat this step for any other accounts on your computer.

B. Disable the Windows 2000 Guest account.

This prevents users without an account on your computer from logging in remotely or locally.

1. Go to the **Start** menu and choose **Control Panel**
(or Settings-Control Panel if the Classic Start Menu is used).
2. Select **User Accounts**.
3. If the Guest Account is turned on, select **Guest Account**.
4. Select **Turn off the Guest Account**.
5. Exit out of User Accounts.

C. Disable unnecessary System services.

1. Copy [DisableServices.bat](#) from your Removable Media to your desktop.
2. Double-click DisableServices.bat to execute.
3. Hit any key to continue as prompted.
4. The window will close automatically.
5. Restart the computer.

D. Reset Internet Explorer browser security settings to default.

1. Open the Internet Explorer browser.
2. Go to **Tools-Internet Options**.
3. Click on the **Security** tab.
4. Click on the **Internet Zone** icon to highlight it.
Click on the **Default Level** button if it is not grayed out.
5. Repeat this step for **Local Intranet**, **Trusted Sites** and **Restricted Zones**.
6. Click on the **Advanced Tab** and click **Restore Defaults**.
7. Click **OK** to close the window.

E. Disable File and Print Sharing.

1. Open the Network Control Panel.
2. Choose the "Local Area Connection" - Right-click on it and select "Properties".
3. Uninstall or Disable the "File and Print Sharing" Service.

Ongoing Protect & Clean Maintenance Tasks -

= <http://www.udel.edu/security/protect/win2000.html>

After cleaning your computer, the following tasks should be completed **WEEKLY** to KEEP your computer clean.

- * [Run Disk Cleanup](#).
- * Remove & protect against Spyware.
 - [Run Ad-Aware SE Personal](#)
 - [Run SpywareBlaster](#)
- * [Backup Important Data](#).

The following tasks are now set to run automatically:

- * Windows Operating System Updates.
- * UD McAfee will update daily and scan weekly for viruses.

See **Application Critical Security Updates –**

<http://www.udel.edu/security/secchkwin.html#appupdate> for how to obtain critical security updates for popular programs like Firefox, and other UD-supported software.

Appendix A: How to Boot into Safe Mode

1. If the computer is on, from the Start menu (in the lower-left corner of the screen), shut down Windows.
2. Turn the computer off.
3. Turn the computer on. The computer will begin processing a set of instructions known as the "Basic Input/Output System (BIOS)." What you see on the monitor depends on the BIOS manufacturer. Some computers display a progress bar that refers to the word BIOS, while others may not display any indication that this process is happening.
4. As soon as the BIOS has finished processing, begin tapping the F8 key on your keyboard. Continue to do so until the Windows Advanced Options menu appears.

NOTE

If you begin tapping the F8 key too soon, some computers display a "keyboard error" message. To resolve this problem, restart the computer and try again.

5. Use the arrow keys on the keyboard to scroll through the menu options, and then select the Safe mode menu option.
6. Press ENTER.

Appendix B: How to Run a McAfee Scan in Safe Mode

1. Make sure your computer is running in Safe mode.
2. From the Start menu, select All Programs | Network Associates | VirusScan On-Demand Scan.
3. All Local Drives should be highlighted. Click Start to begin the scan.
4. VirusScan will take between 5 minutes and several hours to scan your computer's hard drive(s), depending on how much data is stored on your hard drive(s).
5. Close VirusScan when the scan is complete.
6. Reboot your computer into regular mode.