

## Secure and Maintain Your Laptop

There are four basic steps that you can follow to secure and maintain your computer or laptop.

### **Backup Your Important Files**

A computer crash, hard drive failure or a virus can wipe out everything on your computer. Therefore, it is critical to backup your system so that you can restore your files if any disaster occurs.

You should back up regularly and back up often (at least once a week).  
Click this link to find information on [Using the Windows XP Backup Wizard](#).

### **Update Your Operating System**

Every operating system (Windows, Linux, Mac OS) has flaws. These flaws are exploited by hackers who can compromise not only the attacked computer, but every computer connected to it.

To repair security vulnerabilities and other problems, it is important to keep your operating system patched and updated. Virus protection alone will not ensure that your computer is secure.

Updating the operating system helps to ensure the integrity, confidentiality and security of electronic information on your computer and on the network.

All computers connected to the School of Law network should be updated on a regular schedule.  
Click this link to find information on how to [Update Your Computer Operating System](#).

### **Update Your AnitVirus Software**

To prevent the spread of viruses, all computers connected to the law school network must have up-to-date antivirus software installed. Antivirus software is a utility that searches your computer for viruses and removes any it finds. The search is based on definitions of known viruses. Because new and updated viruses are released continually, it is critical to update these definitions frequently to ensure that the software has the latest fixes.

It is also essential to scan your computer periodically. Most software programs have an option to set up an automatic scan at set intervals. You should also make it a practice to manually scan files you receive from an outside source before opening them.

Click this link to find more information on how to [Update Your AnitVirus Software](#).

### **Remove Adware and Spyware**

Spyware and Adware are malicious software that sends your personal information to a third party or displays advertisements, usually without your knowledge or consent.

You probably have a spyware problem if you see pop-up advertisements even when you are not on the Web, your browser does not work properly, you have a new toolbar that you did not install on your computer, your computer has slowed down significantly or your computer crashes often.

Unfortunately, spyware is extremely difficult to avoid. Most people install spyware inadvertently when they are tricked into clicking on a link that installs it; for example, by clicking a cancel button to close a dialog box. Spyware may also get installed when other software is installed.

Click this link to find information on how to [Remove Adware and Spyware](#).

## Using the Windows XP Backup Wizard

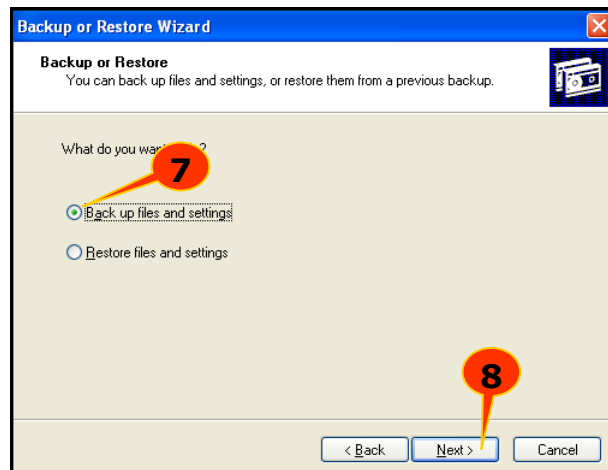
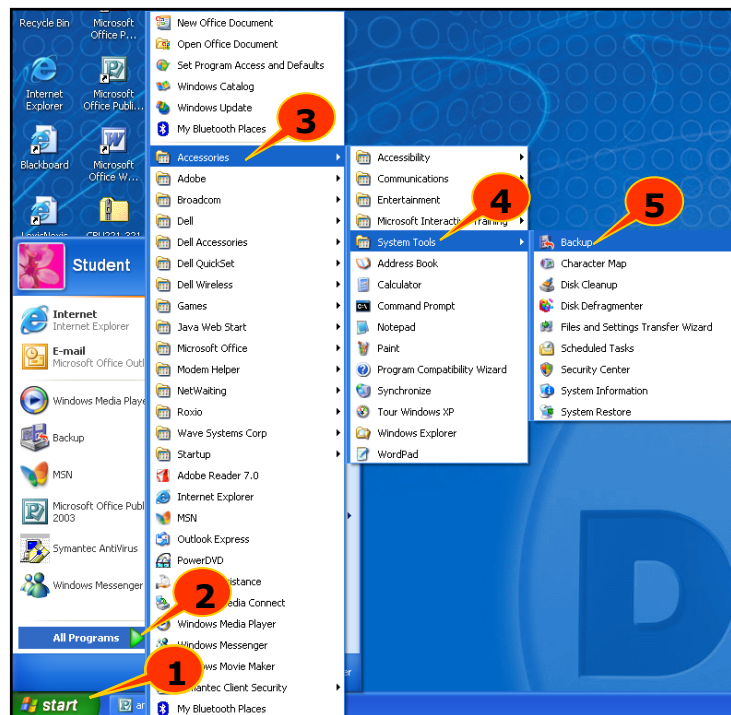
### Introduction

A computer crash, hard drive failure or a virus can wipe out everything on your computer. Therefore, it is critical to backup your system so that you can restore your files if any disaster occurs.

You should back up regularly and back up often (at least once a week).

### Open the Backup Wizard

1. Open the **Start** menu.
2. Select **All Programs**.
3. Point to **Accessories**.
4. Slide right and down to select **System Tools**.
5. Slide right to select **Backup**.
6. The **Backup and Restore Wizard** opens.  
Click the **Next** button to get started.
7. Choose **Back up files and settings**.
8. Click the **Next** button.



## Decide What to Backup

Organizing your files in a logical manner is essential to backing up your documents. All files must be stored in easy-to-find locations. Windows XP makes this easy with the default **My Documents folder**.

### 1. Decide **What to Back Up**:

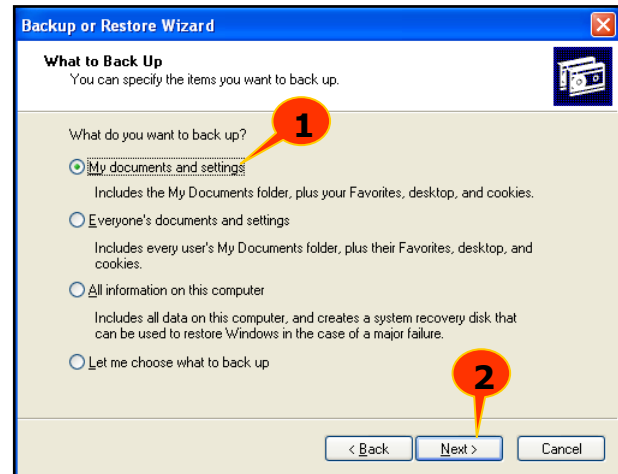
a) **My documents and settings** is usually the better choice because it will preserve your document files that are in the **My Documents** folder and the personal settings stored in the Windows registry.

b) Select **Everyone's documents and settings** if someone else shares your computer, and you want to backup their files.

c) Ordinarily you do not need to choose **All information on this computer**.

A backup of all computer information could add up to many gigabytes, and it is usually unnecessary, if not impractical. You should not choose this option if you do not have a large-capacity removable drive such as a Zip drive or if you have the disks the programs came on. Participants in the notebook program do not need to choose this option because the IT Department maintains an image of the notebook hard drive.

d) **Let me choose what to back up** allows you to select document files stored outside of your profile (My documents and settings folder) or if you have files that you don't want to back up. Browse the **My Computer** hierarchy to select files or folders for backup. If you have files stored on a Network that you would like to select, open the **My Network Places** folder.



### 2. Click the **Next** button.

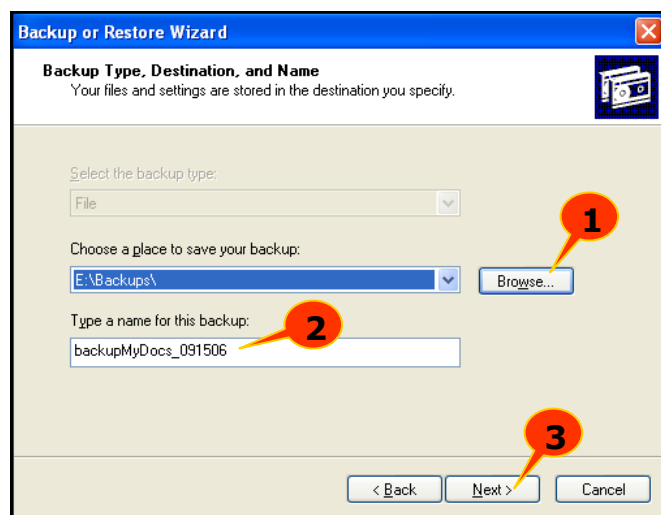
## Choose Your Backup Destination

1. Choose a place to save your backup.  
Click the **Browse** button and choose a zip drive, USB flash memory, external hard drive, a shared network drive, or you may save the backup as a file on your laptop and later write it to a CD.



**If you do save to your laptop, save it to the Desktop and then immediately write the backup file to CD or DVD.**  
Instructions on page 6.

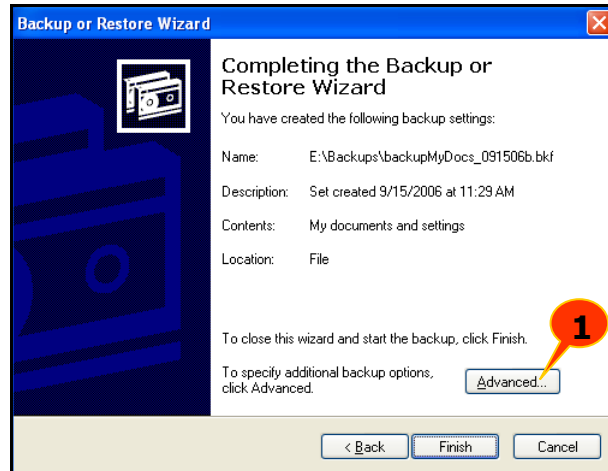
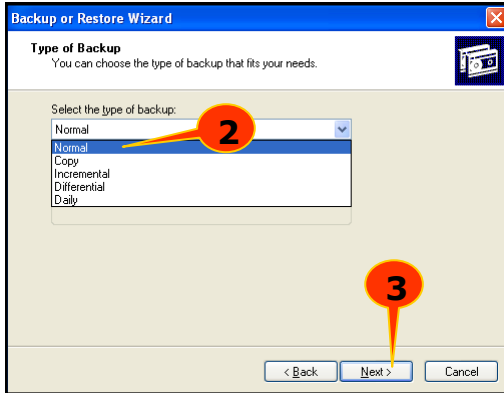
2. Enter a **Name** for your file.
3. Click the **Next** button.



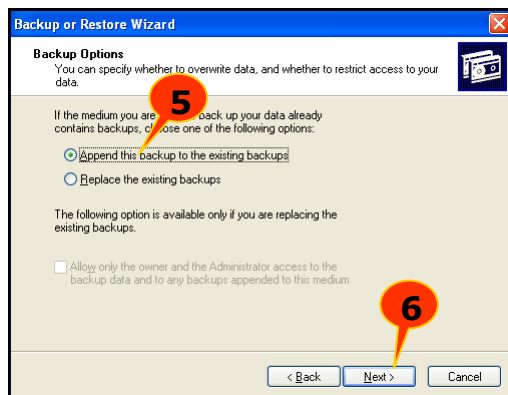
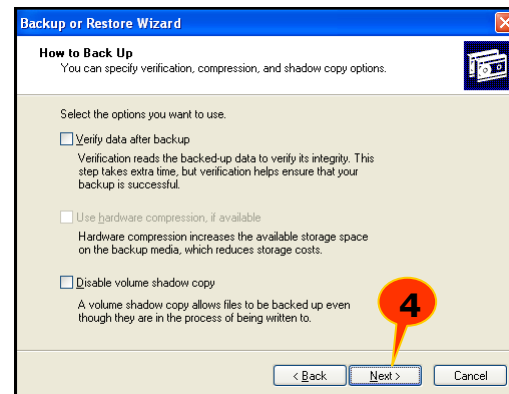
## Completing the Backup Wizard

You may define the type and method of backup, whether to append or overwrite a previous backup, or schedule automatic future backups.

1. Click the **Advanced** button.
2. Select the **Type of Backup**. **Normal** is the default and the most inclusive.
3. Click the **Next** button.



4. You may select **How to Backup**. The options to verify data, or to allow backups of open files will take more time. **You do not have to make a selection.** Click the **Next** button.
5. If you use the same filename and path to your backup file and you may select the **Append this backup to the existing backups** or to **Replace the existing backups** option.
6. Click the **Next** button.



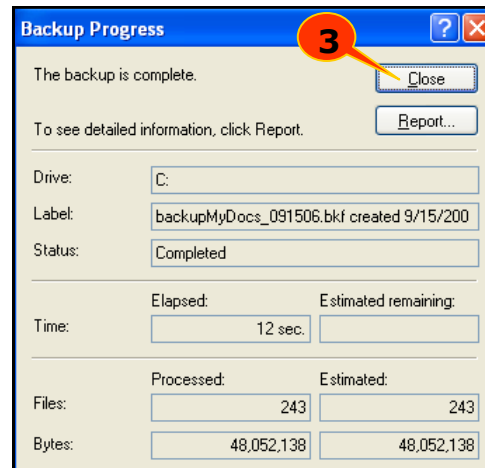
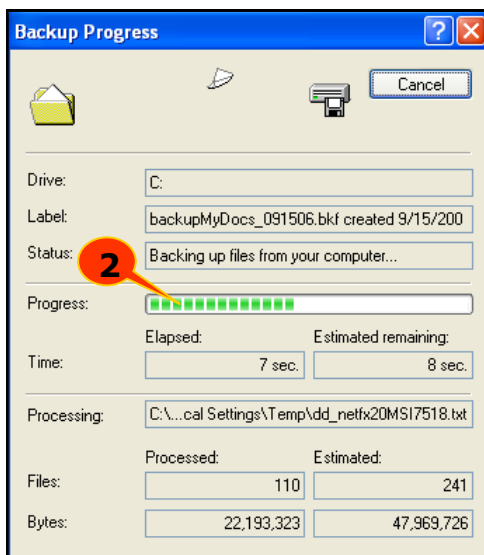
7. Select **Now** to run the backup immediately or **Later** to schedule automatic backups.
8. Click the **Next** button.



## Completing the Backup Wizard (*continued*)

All of the options that you have selected will display on the final **Completing the Backup or Restore** Wizard page.

1. Click the **Finish** button to start the backup.
2. The **Backup Progress** window opens.
3. Click the **Close** button when the backup is complete.



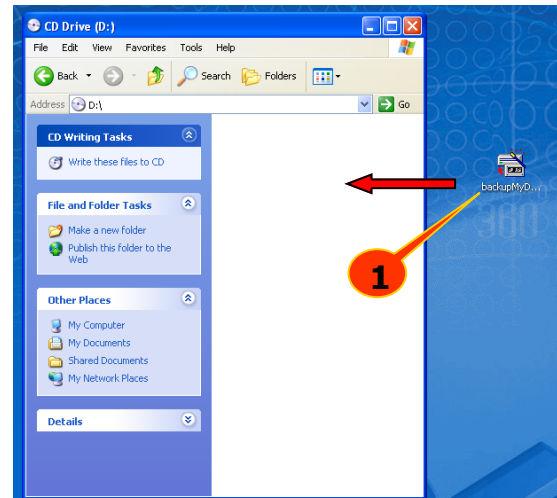
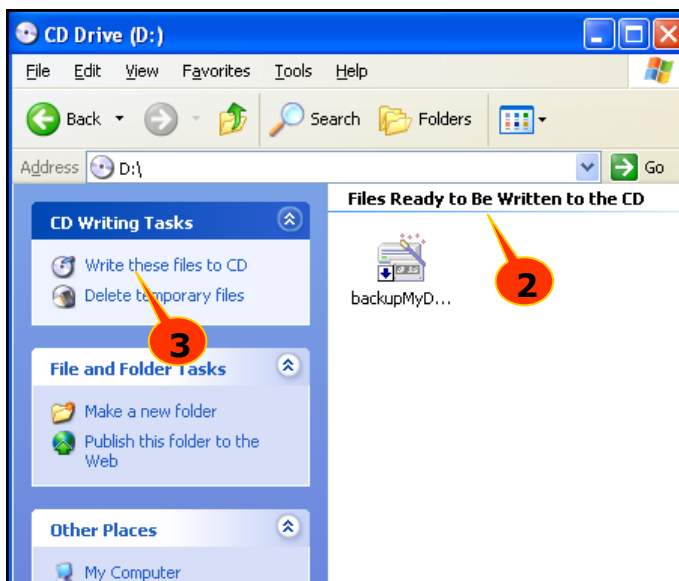
**For information on scheduling your backup please see the Microsoft site:**

<http://www.microsoft.com/windowsxp/using/setup/maintain/backupfiles.msp>

## Copy Your Backup to a CD or DVD

You may use the Windows XP **CD Writing Utility** to transfer a backup that was saved to the laptop. Insert a blank **CD-R** or **DVD-R** and open **My Computer** or **Windows Explorer** and select the disk drive letter for your system.

1. Find your backup and drag it into the window displaying the contents of your **CD/DVD** drive.
2. You will see the message, **Files Ready to Be Written**.
3. Select the option **Write these files to CD**.



4. By default Windows will name the CD using the current date. You may accept or change the name.
5. Click the **Next** button.



**Clearly label your CD or DVD and store it in a safe place.**



## Update Your Computer Operating System

### Introduction

Every operating system (Windows, Linux, Mac OS) has flaws. These flaws are exploited by hackers who can compromise not only the attacked computer, but every computer connected to it.

To repair security vulnerabilities and other problems, it is important to keep your operating system patched and updated. Virus protection alone will not ensure that your computer is secure.

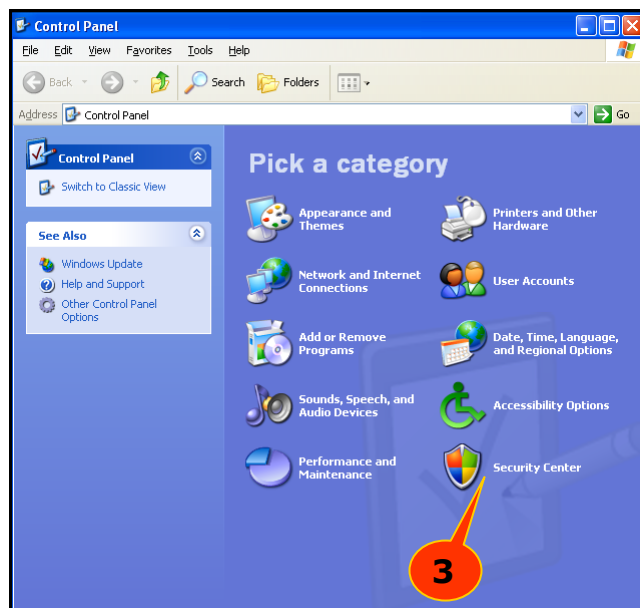
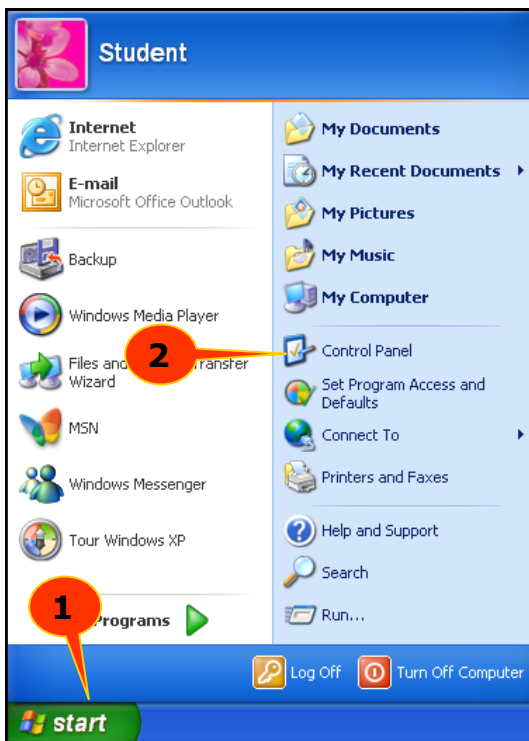
Updating the operating system helps to ensure the integrity, confidentiality and security of electronic information on your computer and on the network.

All computers connected to the School of Law network should be updated on a regular schedule.

### Windows Security Center

You can ensure that your home computer is protected by activating the automated security updates in the Windows Security Center. The Security Center will check to make sure you have an up-to-date software firewall, an up-to-date antivirus program, and that automatic updates are set to download and install automatically.

1. Open the **Start** menu.
2. Select the **Control Panel**.
3. Select the **Security Center** icon or text.

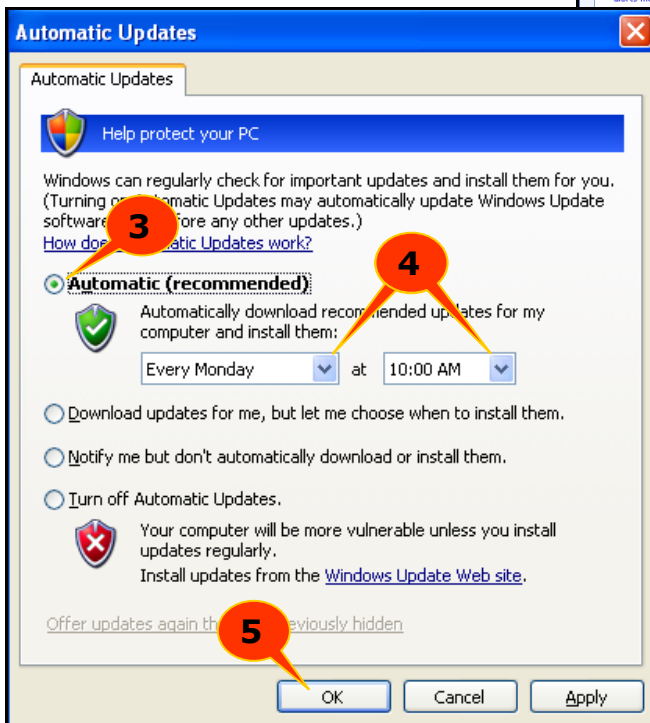


## Windows Security Center (*continued*)

Windows Security Center lets you automatically verify the status of the major security functions: Firewall, Automatic Updates, and Virus Protection. When a problem is detected, you receive notification and a list of recommended steps that may help secure your computer.

### ***Verify that Automatic Updates is turned ON.***

1. If you find the function turned **OFF**, select the **Turn on Automatic Updates** button.
2. Select the **Automatic Updates** icon or text from the **Manage security settings** section to define how and when you want updates processed.
3. Select the **Automatic (recommended)** option.
4. Use the drop-down menus to set a time when you will most likely have your system on and connected to the Internet.
5. Click the **OK** button.



## Non-Windows Operating Systems

Macintosh (OS X) users may request updates at any time or schedule their Mac OS X to check for updates using the automatic Software Update feature from System Preferences.



For Red Hat Enterprise Linux or Fedora, visit the RHEL (<http://www.redhat.com/software/rhel/>) or Fedora (<http://fedora.redhat.com/>) Web sites.

## Update Your AntiVirus Software

### Introduction

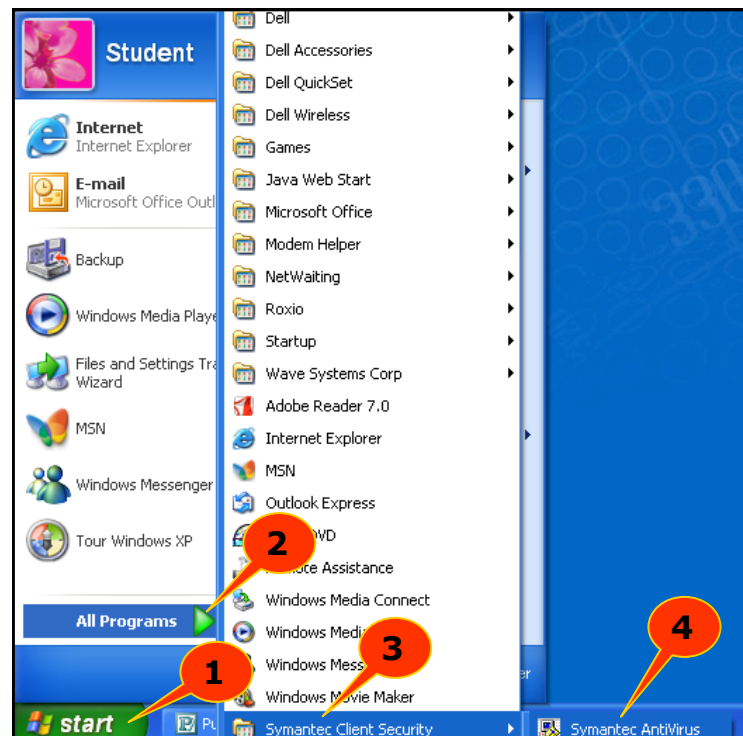
Computer viruses, worms and Trojan Horses are malicious software programs designed to corrupt, delete or record data and interfere with your computer operations without your permission or knowledge. Some can even allow users to control your computer remotely, compromising confidential or personal information. They spread themselves, often by email, to other computers and throughout the Internet.

To prevent the spread of viruses, all computers connected to the law school network must have up-to-date antivirus software installed. Antivirus software is a utility that searches your computer for viruses and removes any it finds. The search is based on definitions of known viruses. Because new and updated viruses are released continually, it is critical to update these definitions frequently to ensure that the software has the latest fixes.

It is also essential to scan your computer periodically. Most software programs have an option to set up an automatic scan at set intervals. You should also make it a practice to manually scan files you receive from an outside source before opening them.

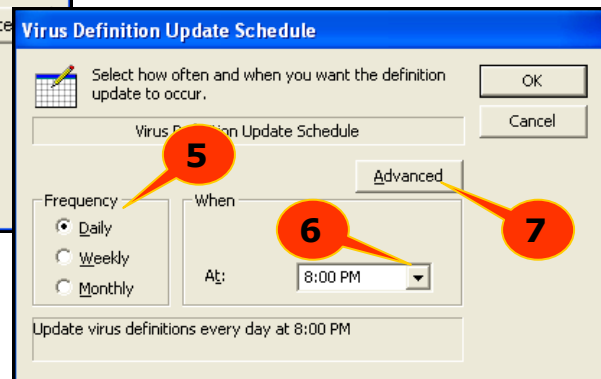
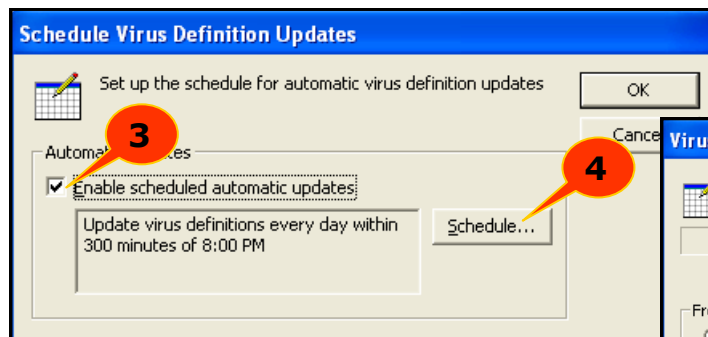
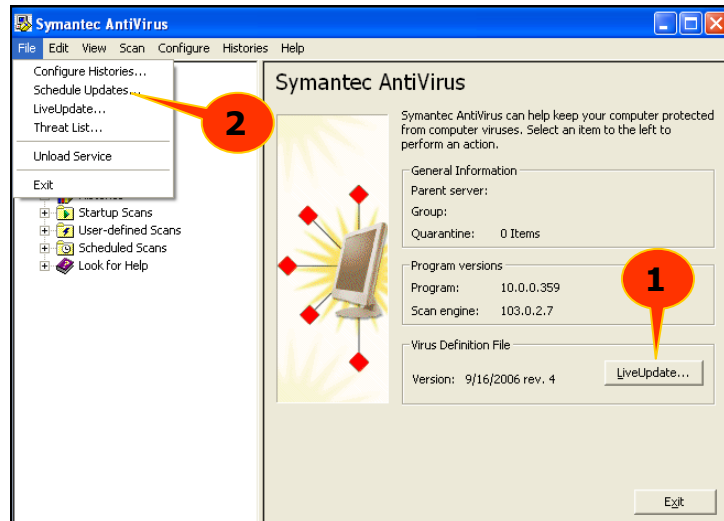
### Open the Symantec AntiVirus Program

1. Open the **Start** menu.
2. Select **All Programs**.
3. Point to **Symantec Client Security**.
4. Slide right to select **Symantec AntiVirus**.

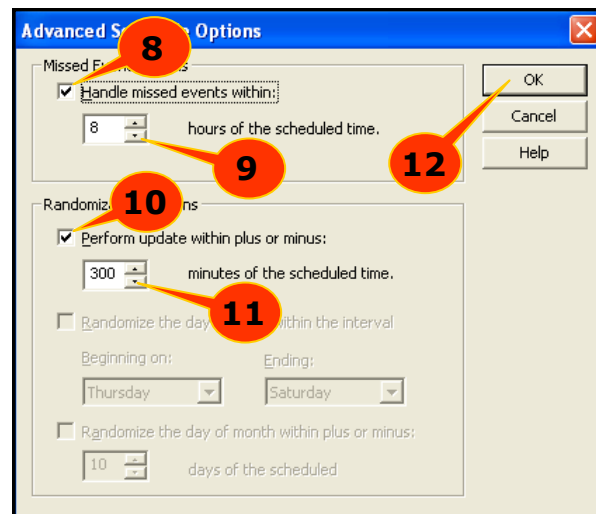


## Updates - Live and Scheduled

1. Click the **LiveUpdate** button at any time to update the protection files on demand.
2. To schedule an update, open the drop-down **File** menu and select **Schedule Updates**.
3. Check the box for **Enable scheduled automatic updates**.
4. Click the **Schedule** button.
5. Select the **Frequency: Daily, Weekly, or Monthly**.
6. Use the drop-down menu to select a time **When** you would like the update to occur.
7. Click the **Advanced** button to add more schedule options to ensure that the protection files are updated in case of a missed scheduled time.



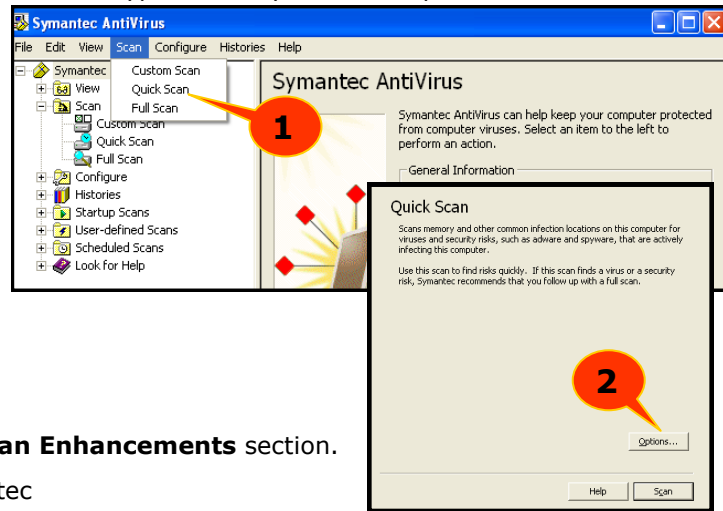
8. Check the box to **Handle missed events within:**
9. Use the drop-down menu to select the hours.
10. Check the box to **Perform update within plus or minus:**
11. Use the drop-down menu to select the minutes.
12. Click the OK button to process any changes that you made.



## Run a Scan

1. Open the drop-down Scan menu and select the type of scan you want to perform:

- Custom Scan:** Allows you to select which folders or files to scan.
- Quick Scan:** Use this scan to find risks quickly.
- Full Scan:** Scans the boot sector, programs loaded into memory, and all files and folders.



2. Click on the **Options** button

3. Select to scan **All file types**.

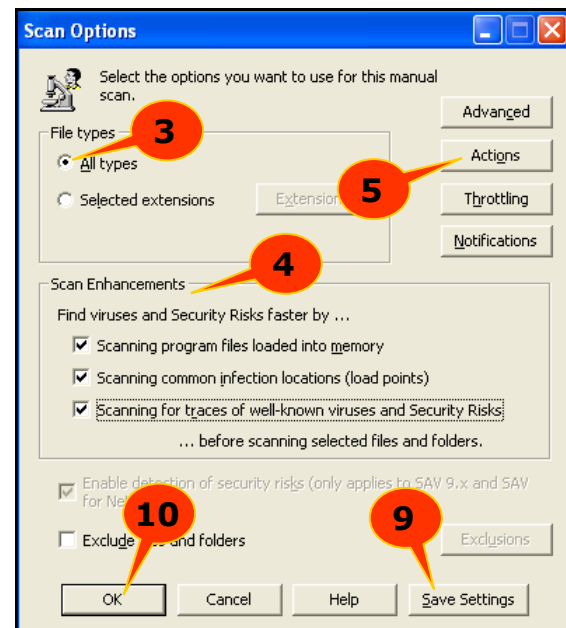
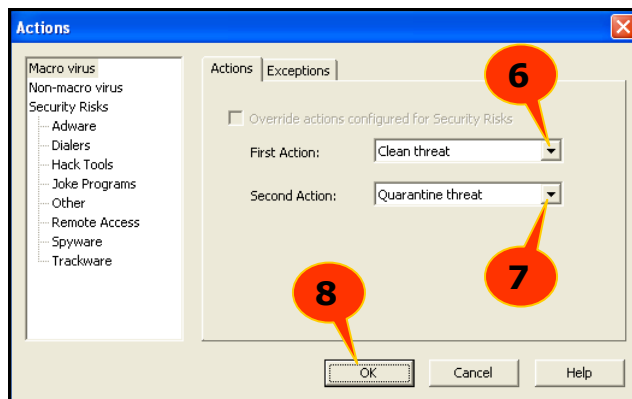
4. Select all of the check boxes in the **Scan Enhancements** section.

5. Click on **Actions** button to tell Symantec what to do if it finds an infected file.

6. Use the drop-down menu to select **Clean threat** as the first action.

7. Use the drop-down menu to select **Quarantine threat** as the second action.

8. Click **OK** to accept the options.



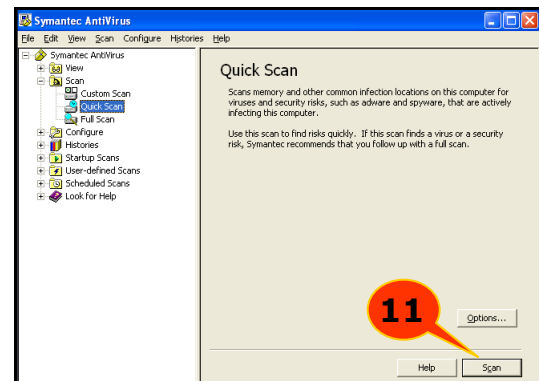
9. Click on **Save Settings** to save the selected options.

10. Click **OK** to return to the selected scan.

11. Click **Scan** to start the selected scan.

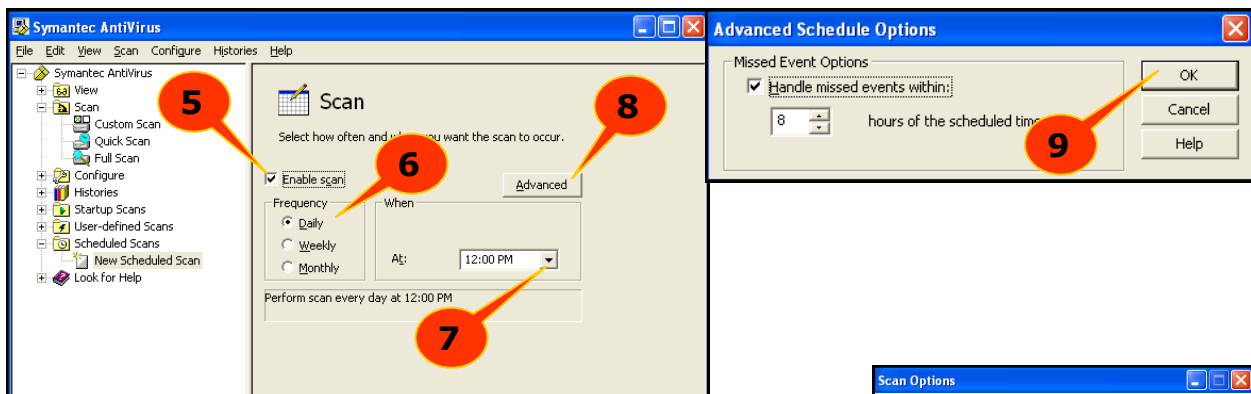
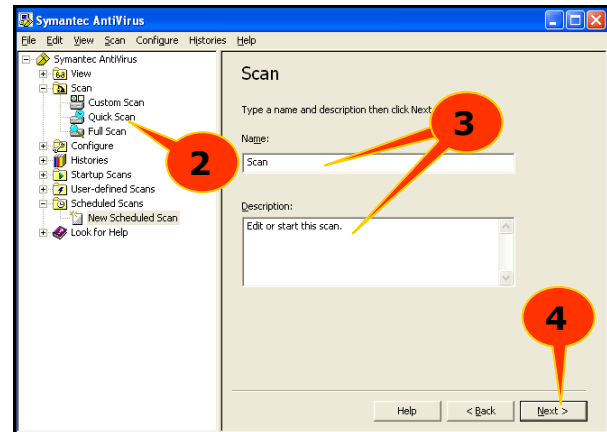
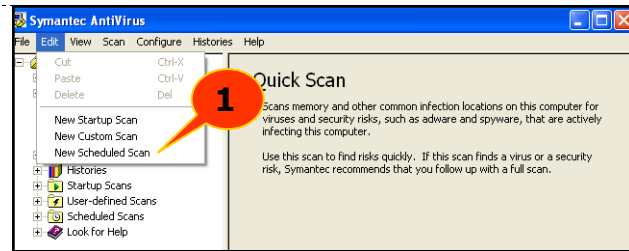


**A window will open showing the progress of the scan and any threats found.**

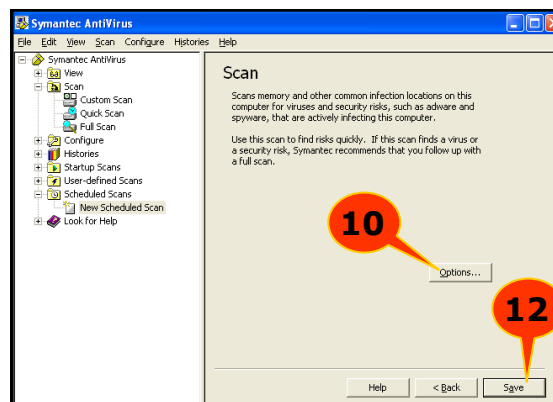


## Schedule an Automatic Scan

1. Open the drop-down **Edit** menu and select **New Scheduled Scan**.
2. You have a choice of **Quick Scan**, **Full Scan**, or **Custom Scan**.
3. You may change the scan **Name** and **Description** or accept the defaults.
4. After making your selection, click the **Next** button.
5. Make sure that the **Enable scan** check box is checked, it is by default.
6. Select the **Frequency: Daily, Weekly, or Monthly**.
7. Define **When** to scan by selecting a time from the drop-down menu.
8. Click **Advanced** to define the Missed Event Options.
9. Click **OK** to accept the Advanced Schedule Options.



10. Click **Options** to review or change the default options.
11. If you do change the **Options**, click the **Save Settings** button.
12. Click the **Save** button to save your new scheduled scan.



## Removing Adware and Spyware

### Introduction

Spyware and Adware are malicious software that sends your personal information to a third party or displays advertisements, usually without your knowledge or consent.

You probably have a spyware problem if you see pop-up advertisements even when you are not on the Web, your browser does not work properly, you have a new toolbar that you did not install on your computer, your computer has slowed down significantly or your computer crashes often.

Unfortunately, spyware is extremely difficult to avoid. Most people install spyware inadvertently when they are tricked into clicking on a link that installs it; for example, by clicking a cancel button to close a dialog box. Spyware may also get installed when other software is installed.

That is why it is important to read all disclosures, including the privacy statement and license agreement, before installing any software. Spyware can also be installed with music and video downloads.

To avoid spyware, make sure you only download programs from Web sites you trust. Read all security warnings, license agreements and privacy statements. Never click **Agree** or **OK** to close a window; instead click the red **X** in the corner or use **Alt+F4** to close the window. Better yet, avoid pop-up windows altogether by using a pop-up blocker. Be careful with free music or music-sharing programs. Investigate free software by searching Google for the name of the program and the keywords **adware** or **spyware**.

The following programs are free for personal use and have proven to be safe and reliable to use.

### Download Removal Tools

Since there are so many free removal tools to choose from we have provided links to our favorite trusted sites.

1. The original software download site, Tucows.com, earned its name early on for being the first to provide software on a "freeware" or "shareware" basis.  
<http://www.tucows.com/>
2. CNET Downloads is the trusted, safe, and secure resource for software and game downloads.  
<http://www.download.com>