



Protecting Your Personal Computer from Malware

Protecting Your PC from Malware

What is malware?

Malware is a software program that can copy itself and infect a computer without permission or knowledge of the user. Instructions in the code within this program tell the computer to perform some task, usually a destructive one, such as deleting important files or reformatting the hard-drive. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, and other malicious and unwanted software.

How does your PC get infected?

Malware is passed from computer to computer just like a human virus is passed from person to person. Any time that you download files or put a floppy disk, zip disk or USB Pen drive into your computer you are susceptible to viruses.

Moreover, most personal computers are connected to the Internet if for nothing more than email purposes, which assists in easily spreading viruses, computer worms and Trojan horses.

Typically, a virus, worm or Trojan horse becomes active when you execute a program that contains malicious code. For instance, if you download a program from the Internet and it is infected with a virus, worm or Trojan horse it will attack your computer when you activate the program and most of the time, particularly in the case of a Trojan horse, you are unaware of the damage until days or weeks later.

How do I know if my computer has a virus?

A computer virus can do a lot of damage to your computer such as crashing your hard drive. Viruses can destroy all or some of your data. Many viruses do strange things that adversely affect your computer. The most common symptom of a computer virus is erratic behavior such as being slow to open windows or freezing up on you, etc. The destruction can happen at any rate of speed and can affect any part of the computer. If your computer begins to act strangely, the very first thing to do is to check for a virus or

spyware by running a virus can or spyware scan on your computer.

How do I protect my computer from malware?

To protect your computer from pesky and destructive malware, purchase a good virus protection program such as Norton AntiVirus. Such a program will check all files for viruses. Once installed, an anti-virus program can be set to work automatically in the background. It will check all files before they enter your computer and will alert you if a virus is detected before it contaminates your system. If a virus is detected, your antivirus program can quarantine or eliminate the problem.

What antivirus program should I purchase?

All Northwest-owned computers have Symantec AntiVirus installed on them. If you are purchasing antivirus software for a non-university owned computer, choose one that works with your computer's operating system (OS).

Keep virus Protection software updated!

New viruses inundate cyberspace everyday. Fortunately, companies like McAfee and Symantec are constantly working to create vaccines for these destructive cyber parasites.

In order to take advantage of new antivirus protections, you must update your antivirus program on a regular basis. The company that manufactured your antivirus software should provide daily and weekly updates as they discover new virus threats.

Downloading and Installing these updates are important to ensure that your computer is completely protected. Go to the Web site of your antivirus manufacturer to download new virus definitions. Some antivirus programs, such as Symantec, automatically update your antivirus protection and virus definitions when you log onto the Internet through a process called *live update*.

Removing Quarantined Viruses Using Symantec

1. Click on **Start**.
2. Click on **Programs**.
3. Click on **Symantec Client Security**.
4. Click on *Symantec Antivirus* or *Norton Antivirus*.
5. Click on **View**. (See Figure 1)
8. When items are *selected*, the **X** in the Quarantine window turns red. (See Figure 2)
9. Click the **red X** to delete the selected items.
10. Answer *yes* if the program asks again.

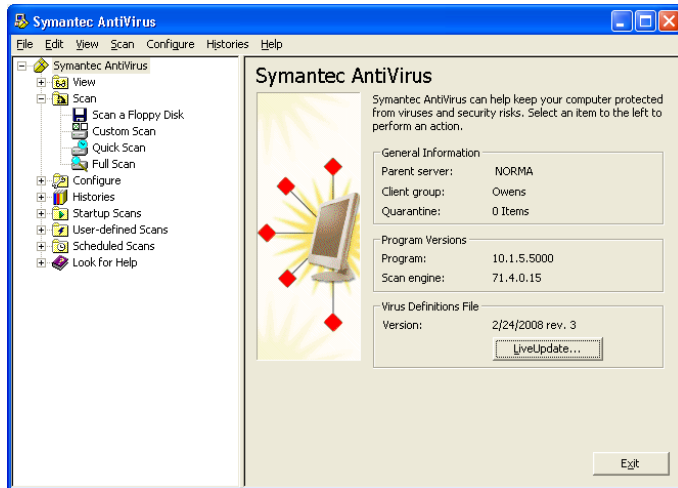


Figure 1. Symantec main window.

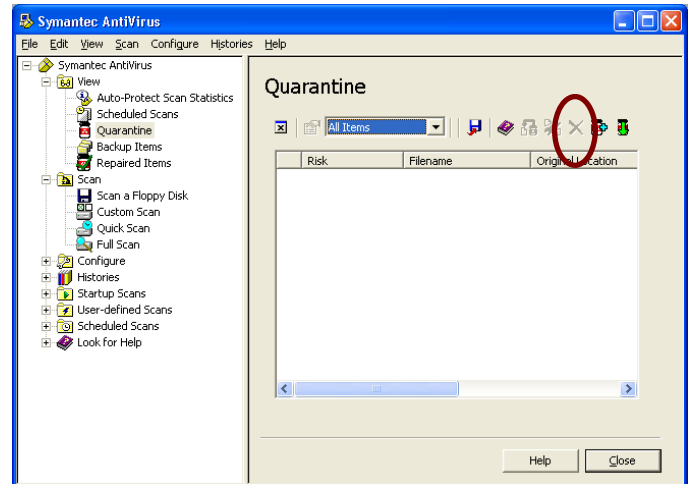


Figure 2. Quarantine view.

6. A *drop-down* menu will appear. Click **Quarantine**.
7. If there are items listed in the right-hand box, *select* the items.

Running a Supplemental Virus Checker Using Trendmicro

1. Click on **Internet Explorer**.
2. Type in the following URL in the Address textbox: <http://www.trendmicro.com>
3. Click on **Free Online Services**.
4. Click **Learn More...** beneath the heading *HouseCall™ Free Scan*.
5. Click on **Scan Now, It's Free!**
8. Check the box for your C: drive to be scanned.
9. Please **do not** scan your Catbert (N) storage. *Information Systems* maintains security and virus updates on your Catbert (N) storage.



You might want to run the Trendmicro scan in Safe Mode if you believe you may need to remove programs. However, be aware that certain programs that you may need will not run in Safe Mode. To put your computer into Safe Mode, press the F8 Key right as windows is starting. Use your arrow key to select Safe Mode and then press Enter.

6. Once you have clicked on the **Scan Now, It's Free!** link, it will download some files to your computer.
7. If asked to accept anything, answer *yes*.



The virus check on your C: drive will take a while to run. It may find viruses and give you some information about them.

Please try and delete all that you can. If it finds viruses that cannot be deleted, notify the Information Systems Help Desk at 660-562-1634.



Spybot Search & Destroy and Ad-Aware

Spybot Search & Destroy and *Ad-Aware* are other software programs that can be downloaded and installed to protect your computer from malware and various spyware.

A brief word about Spybot Search & Destroy:

Spybot is easy to install, use and update. It is a free download and the program will eliminate most adware on your computer. Additionally, *Spybot* will block adware from coming back in the future. *Spybot* also offers real-time protection by blocking adware programs as they try to install.

Once you have downloaded *Spybot Search & Destroy*, install the program by **double**-clicking on the icon on your desktop.

The first time you run the program, it will ask you to update the program and make some back-ups. Simply follow the easy step-by-step directions provided by *Spybot's* wizard.

Once installed, run the program once a week, making sure to get all the available weekly updates first. Weekly updates can be found through the Search for Updates feature within *Spybot*. After installing updates, use the Immunize feature. The Immunize feature blocks known bad software programs. Lastly, run a scan and delete any adware or spyware *Spybot* discovers.

To download *Spybot Search & Destroy*, click the **Spybot** link on the *Viruses and Spyware* web page on the *Client Computing Online Support* web site:

http://www.nwmissouri.edu/compserv/ClientComputing/Online_Support/index.htm

OR, go directly to the *Viruses and Spyware* web page by typing the following URL:

http://www.nwmissouri.edu/compserv/ClientComputing/Online_Support/viruses_spyware.htm

A brief word about Ad-Aware:

Ad-Aware from *Lavasoft* gives you the ability to scan your RAM, Registry, hard drives, and external storage devices for known data-mining, advertising, and tracking software (spyware). Additionally, *Ad-Aware* allows you to clean your system and maintain a higher degree of privacy while surfing the Internet.

To download *Ad-Aware*, click the **Ad-Aware** link on the *Viruses and Spyware* web page on the *Client Computing Online Support* web site:

http://www.nwmissouri.edu/compserv/ClientComputing/Online_Support/index.htm

OR, go directly to the *Viruses and Spyware* web page by typing the following URL:

http://www.nwmissouri.edu/compserv/ClientComputing/Online_Support/viruses_spyware.htm

AVG Anti-Virus or Internet Security

AVG (www.grisoft.com) is designed to maintain your computer's safety while searching the Internet and downloading music, images and documents.

AVG also protects your computer when opening email or instant messaging by scanning documents, files, web pages and hyperlinks before you open them.

AVG Internet Security and Anti-Virus are available to you for a 30-day free trial period. During the trial period, you will have full access to all AVG program features and AVG's Technical Support team.

To download *either AVG Internet Security or Anti-Virus*, click the **AVG** link on the *Viruses and Spyware* web page on the *Client Computing Online Support* web site:

http://www.nwmissouri.edu/compserv/ClientComputing/Online_Support/index.htm

OR, go directly to the *Viruses and Spyware* web page by typing the following URL:

http://www.nwmissouri.edu/compserv/ClientComputing/Online_Support/viruses_spyware.htm

You can also go directly to AVG by typing the following URL:

<http://www.grisoft.com/>

Once on AVG's homepage, click on the Trial Versions tab and click **Download** on the version you want to try free for 30 days.



If you have a university-provided notebook computer, you already have Symantec Anti-Virus and do not need to download AVG.