

**CIT Client Services Safe Computing Group
Adware and Spyware: Self-help Resource**

*Safe Computing
Malware Clean-up Guide*



This guide is provided by the CIT Client Services Safe Computing Group to help UVM affiliates cope with the growing number of problems related to spyware, adware, and virus infections.

Malware Help CD Contents

.....Digital version of this help guide

..... Link to online Safe computing guide

Installers for the following freeware programs:

.....[Lava Soft Ad-aware](#) Personal Version 1.06

.....[Spybot Search & Destroy](#) version 1.4

.....[CCleaner](#) version 1.22

.....Microsoft Windows [Defender](#)

.....[Mozilla Firefox](#) version 1.0.6

.....[Gaim](#) version 1.4.0



Help-guide Booklet Contents

Malware Help CD Contents	2
Announcements	4
Dealing with Infections	6
Malware: A Closer look	7
Step by Step Cleanup	9
Preventative Steps	18
Symantec Antivirus	19
Glossary	21

** See last page for Resource CD*

CIT Announcement:

Due to the increase in time and resources spent removing spyware and viruses from individual computers and the UVM network, the following policies have been created:

Effective July 2006:

“*Walk-in Help*” at the Computer Depot in Waterman was re-named “**Computer Depot Clinic**” or “**CDC**”.

Effective August 1, 2005:

There are three options for students who need assistance with cleaning malware from a computer:

1. Attend a safe computing workshop to learn how to clean up an infected machine and maintain the cleaned condition.
 - Hands-on assistance is provided free of charge by CIT Client Services Technicians at all workshops.
 - Students may attend an unlimited number of workshops.
 - Check at The Computer Depot Clinic for the hours of the malware workshops. OR go to: www.uvm.edu/cit/safecomputing/workshop.html
2. Request a complete re-imaging (only for computers purchased through the UVM Depot) OR a re-installation of Windows XP using the student's CDs that came with any computer purchased from any vendor.
3. Drop off the computer at the Computer Depot and pay the current Depot hourly labor rate to have the computer cleaned by a CDC staff technician. Average turn around is one week, average service time is 2.5 hours.

CIT Announcement (cont'd):

Effective January 18, 2005 charges may be assessed for malware removal.

This guide is provided by the CIT Client Services' Safe Computing Group to help UVM affiliates with the growing number of problems related to spyware, adware, and virus infections.

Malware (Malicious Code) is a term that includes computer viruses (all virus forms, trojans, and worms) and Spyware (adware, spyware, key loggers) and their variations, as identified by CIT supported Antivirus software and/or other CIT supported malware/anti-spyware removal programs.

Students can use our online self-help guide posted at <http://www.uvm.edu/cit/safecomputing>

Dealing with Infections

How do I fix my infected computer?

Fixing an infected computer is an art. There is no perfect or fool-proof way to fix a computer infected with malware.

What follows is a guide which highlights many of the procedures we at CIT use every day to disinfect UVM computers. If at any point during the process you find yourself stuck, please go to CDC (in Waterman at the MCSV Depot) to get a ticket and be referred to the Malware clean-up workshops in Waterman. You can also sign up online for a Malware clean-up workshop at: www.uvm.edu/cit/safecomputing; on the left side of the page click on “Safe Computing workshop” and click “Sign-up”.

What to expect from this guide:

This guide will take you through the following steps:

- Disable System Restore and File/Printer Sharing
- Search for and remove viruses
- Search for and remove spyware

Step-by-Step Clean up

The steps that follow show how to remove a malware infection from Windows PCs ONLY. If you have an Apple computer and are interested in protecting it from an infection, all you need to do is keep your antivirus software and your software updates, current, and turn on your personal firewall in the sharing system preference. up-to-date. As of the writing of this guide, malware poses little or no known threat to Apple Computers.

Malware: A Closer Look

What is Malware?

Malware is any component installed on a computer which negatively affects the system's overall health and primarily consists of viruses, spyware, and adware. Any of which can cause numerous problems for you and others on the UVM network; these problems increase exponentially due to the 10,000+ computers on the UVM network.

How does Malware get on my computer?

Some web sites may "hijack" your web browser when you visit them, altering its home page, search page, bookmarks, and other settings.

Spyware and Adware are downloaded along with "Free Music Download" or peer-to-peer file sharing (P2P) programs. Some examples include KaZaa, eMule, Morpheus, LimeWire, WinMX, Blubster and BearShare. CIT technicians tested KaZaa, Blubster, and Limewire; approximately 1,000 spyware/adware components were detected after each installation.

Viruses can come via email attachments, images (.jpg files), file sharing software, external media (CDs, DVDs, USB-Drives), or through flaws in Microsoft Windows. Additionally, your computer is more likely to become infected if you have not set an administrator password.

Note: *Using peer-to-peer file sharing software will eventually cause problems for you and possibly the entire UVM network. Not only do you run the risk of allowing your computer to be infected with something terrible, you also run the risk of clogging the network to such an extent that it causes slow connections for everyone else.*

There may be legal complaints from owners of copyrights for downloaded material on your hard drive - for which you are personally liable, even if someone else put it there.

How do I know if Malware is on my computer?

- Your computer slows down
- You can no longer get online
- Your web browser brings you to sites you never visited or intended to.
- Frequent “pop-up” windows and error messages

What do I do to control Viruses, Spyware, and Adware?

- Keep your operating system updated - "Windows Updates" for a Windows PC, and "Software Updates" for an Apple machine.
- Keep your antivirus software **AND** definitions updated as much as possible.
- For Windows users, make sure to run malware scanning software, such as Lavasoft's Ad-Aware.

Step-by-Step Cleanup

Step I: *Getting into safe mode:*

What is safe mode?

Safe mode is a diagnostic mode of Windows which allows for more effective troubleshooting capabilities than in a normal Windows mode. This allows for a more effective removal of most malware.

Getting into safe mode:

There are a few different ways to enter safe mode with networking. Only one will be discussed here for the sake of simplicity. The process goes as follows:

1. If you are currently logged into Windows, go to the “Start” menu and select "Turn off computer," then click "Restart" and proceed to step 3.
If the machine is off, proceed to step 2.
2. Turn on the computer.
3. As soon as the computer starts up, you will see a black screen with your computer’s make appearing in large letters for example “Dell” or “Compaq”. Begin tapping the F8 key on your keyboard as soon as you see it. Do not hold F8 down. Continue tapping the F8 key until you see a screen that gives you the option of selecting, "Safe Mode with Networking". Move down using your arrow keys, then hit enter.
4. If prompted, choose your operating system from the menu.
5. Log into the machine as you normally would.
6. A few seconds to a few minutes will pass (it's different for every computer), and then you will be presented with a screen asking if you want to continue to start up the computer in safe mode; click “Yes”.

You will then be working in safe mode. Do not be alarmed if everything looks strange (large & grainy)– since safe mode doesn't load video drivers.

Step II: Disabling System Restore

What is System Restore?

System Restore is a feature built into Microsoft Windows that backs up configuration settings routinely. This comes in handy in various situations, such as when a piece of software is installed and it causes the computer to start up improperly. Ideally, System Restore would give you the option to choose a point in the past when your computer worked well and you can restore your computer to this state.

It sounds useful, why do we want to disable it?

System Restore backs a number of settings up, even if they have been created by malware. This means that if a malware scan is run and viruses/malware are removed, there is still a good chance that the malware will re-infect the computer the next time a System Restore is performed. When the computer boots up, if a virus was stored in the system restore directory, it is still present on your computer. System Restore must be disabled prior to running a malware scan.

How to disable System Restore:

1. Find and right-click once on your "My Computer" icon. It can be found either on your desktop or in the Start menu.
2. Click on "Properties".
3. In the window that presents itself, click on the tab labeled "System Restore".
4. Check the box labeled "Disable System Restore".
5. Click "OK"

Step III: Disabling File and Printer Sharing

What is File and Printer Sharing?

File and Printer sharing is a feature built into Microsoft Windows that allows computers on a network to share printers and files with one another. It is by default turned on.

Why do we want to disable it?

Malware can take advantage of the file and printer sharing. Most users do not require this functionality so it wise to turn it off and reduce the risk of infection. If you **MUST** share printers or files from your machine, you may skip this step.

How to disable File and Printer Sharing:

1. Click the Start Menu and then select "Control Panel".
2. When the Control Panel opens double-click "Network Connections".
3. A window will open and you should see at least one icon labeled, "Local Area Connection". If you see more than one, do the remaining steps for each one. Right-click once on a connection and select "Properties".
4. In the Components list click on "File and Printer Sharing for Microsoft Networks" and click "Uninstall". Choose Yes when prompted to confirm.
5. Close all open windows.

Step IV: Installing, Updating, and Running Lavasoft's Ad-Aware

What is Ad-Aware?

Ad-Aware is a program provided by Lavasoft that removes malware components. It needs to be updated often to be effective. Ad-Aware is also free and extremely easy to use (personal use only refer to their license agreement for more details).

Installing Ad-Aware:

1. You may download Ad-Aware from www.download.com or if you have the Resource CD: Double-click the file "aawpersonal.exe". In the window that comes up, check the license agreement box and click "Next".
2. If you already have a previously existing installation of Ad-Aware, it will ask you if you would like to uninstall it. Select "Yes". and click "Next".
3. The next window that comes up will ask you where you want to install Ad-Aware. Choose an alternate location if you wish to do so, then click "Next".
4. A window will come up asking who you would like to give access to Ad-Aware. Typically, the default selection of "Anyone who uses this computer" will do fine. Click "Next".
5. When it completes, uncheck "Open the Help File Now" and click "Finish".

Updating Ad-Aware:

1. Open up Ad-Aware (the shortcut can usually be found on your desktop after it has been installed).
2. Click "Check for updates now" on the lower right-hand

side of the window.

3. On the following window click "Connect".
4. Let the update complete and click "Finish".

Running an Ad-Aware Scan

1. Open Ad-Aware (the shortcut can usually be found on your desktop after it has been installed).
2. Make sure Ad-Aware is updated. (Refer to previous section)
3. Click "Start".
4. Select "Next" on the following pane.
5. Let the scan run, which can take a while. When it finishes, click "Next".
6. On the next pane you will see a list of all the components Ad-Aware found during the scan. Right-click once on one of the components and select "Select All Objects". Click "Next" to begin the removal process.

You are done with Ad-Aware for now, but as you have seen you can update it and use it to fight malware in the future.

Step V: Installing, Updating, and Running Spybot Search & Destroy

What is Spybot Search & Destroy?

Spybot S&D is another spyware scanner/remover, similar to Ad-Aware. When run in combination with Ad-Aware, Spybot S&D effectively reduces the number of malware components on an infected computer. Since neither Ad-Aware or Spybot S&D are perfect at removing every single malware component, running both ensures the highest level of success.

Installing Spybot Search and Destroy:

1. You can download Spybot from www.download.com or if you have the Resource CD double-click the file labeled, "spybotsd14.exe" and choose your language (English if you're reading this). Click "OK" then click "Next" on the installation window that appears.
2. On the next window, click "I accept the agreement" and click "Next". On the next window, choose a specific download directory or leave it as is and click "Next". Click "Next" on the next several windows that appear, and choose "Install" on the last window.
3. When the install finishes, click "Finish". Spybot S&D should automatically launch. If it does not, go to your desktop and double-click the "Spybot Search and Destroy" icon.
4. Spybot S&D will now prompt you to backup the registry. Choose "Next" in the window. On the next window, click "Search for updates". On the window that follows, check all the boxes listed and click "Download Updates".

Updating Spybot S&D:

Note: If you just installed Spybot S&D then you've probably already installed the updates. These directions are for updating them on a periodic basis. Move to the next section if you've already done this.

1. Open Spybot Search and Destroy and click "Search for Updates".
2. Put checks in all the boxes that are listed and click "Download Updates".
3. Once this is complete select the "Immunize" button. Spybot will tell you how many programs it immunizes against. You will need to hit another immunize button located near the top left of the Spybot window. As of the writing of this guide the number of malware immunized against was in the 11,000s

Running a Spybot S&D Scan:

1. Open Spybot Search & Destroy and click "Check for Problems". Allow the scan to run, it can take anywhere from 5 minutes to an hour depending on the amount of files on the computer. **WARNING:** If the scan completes in only a few seconds and says that it found no malware, you need to close and reopen Spybot and start the scan again.
2. When the scan completes, make sure each item listed is checked and click "Fix Selected Problems". Click "Yes" in the window asking you permission.

Step VI: Cleaning Temporary Files

Why bother cleaning temporary files?

Viruses and other malware components often root themselves in folders designed to store temporary files. Every time you load a web page on your computer, all the images and extra features are stored on your computer to make browsing quicker. This results in very messy, very large temporary folders. Questionable software likes to store itself here because it's easy to hide amongst all the junk.

What are the consequences of deleting temporary files?

Temporary files are just that, temporary. It is safe to remove them.

How to remove temporary files:

Make these temporary folders visible.

1. Find your "My Computer" icon and double-click it (you can find it on your desktop or in the Start menu).
2. In the window that opens, click "Tools" at the top, and then select "Folder Options".
3. On the next window click the tab labeled, "View".
4. In the "Advanced Settings" frame, scroll down until you see the category "Hidden Files and Folders".
5. In the category, put a check in the box next to "Show hidden files and folders".
6. Click "OK" to close the window.

Remove the files...

1. Open "My Computer" if it is not open.
2. Double-click on "Local Disk C:".
3. Double-click on the folder labeled, "Documents and Settings".

Perform the following steps for any folder named "Administrator," "Default User," or any user name found in the "Documents and Settings" folder.

1. Double-click on the folder and open the "Local Settings" folder.
2. Double-click on the folder named "temp".
3. Hold down the "Ctrl" key on your keyboard and press the letter "A". This will select everything in the folder.
4. Find the Delete key on your keyboard and press it. If you are prompted for confirmation, click "Yes".
5. Click Back one folder so that you see the "Local Settings Folder".
6. Open the "Temporary Internet Files" folder, hold down "Ctrl" and press "A" to select all the files, then press the "Delete" key to remove them.

Preventing Further Infections

What can I do to keep my computer from getting an infection in the future?

- **Keep your Computer Up-to-Date!**
The single most important step is to keep your computer's software up-to-date, specifically Microsoft Windows itself. To do this, make sure to perform Windows updates on a regular basis. On many machines, Windows will alert you when new updates are ready to download or install. Click the "Start" menu, select "All Programs", and select "Windows Update" follow the on screen instructions, if you have the resource cd, double-click on the Windows Update icon on the CD folder to begin updating Windows.
- **Run and Update Antivirus Software.**
Keeping antivirus software current is also crucial. UVM recommends the use of the Symantec Anti-Virus software to protect machines from malware infections. This program is effective at stopping viruses before they are able to do any major damage to a computer. Directions for installing and running a Symantec virus scan can be found in the next section of this guide.
- **Perform Regular Spyware/Adware Scans.**
It is important to run both Spybot S&D and Ad-Aware on a weekly or bi-weekly basis to ensure that your computer stays malware-free in the future. Remember to update both of these programs before each scan (instructions on how to do so can be found in the previous section of this guide).
- **Set a Password.**
Setting a password for your Windows computer is also crucial. There are a number of viruses that take advantage of a machine with out a password . Select Start menu, Control Panel, User Accounts. Select each account by clicking on them and choosing the "create password" option. Choose a password that is easy for you to remember but hard for others to guess.

Installing and Running Symantec Antivirus Corporate Edition

What is Symantec Antivirus?

Symantec Antivirus is the university-recommended antivirus software for UVM affiliates. Symantec is useful to install because it performs active scanning, meaning that it is always on the lookout for malware.

Installing Symantec Antivirus:

Warning: remove any other version of antivirus software before beginning this step, unless the installed software is an older version of Symantec antivirus.

1. Open your web browser and go to www.uvm.edu/software then login with your UVM Net ID and password.
2. On the page that comes up, choose "Windows 2000/XP"
3. On the page that follows, look for the Antivirus listing. If you are on campus, download the on-campus software by clicking on the green download button just below the listing. If you are off-campus, download the off-campus software.
4. When the program begins to download, it will ask you to save or open the file. Choose "Save to disk" and choose an appropriate location for the file. It is recommended that you put it on your desktop so it will be easy to find.
5. Go to your desktop and double-click on the install file beginning with "SAV" and click "Setup" on the window that follows.
6. Wait for the program to install. This step may take several minutes. If the installer prompts you to restart, choose "No".
7. When the Live Update displays, click the "Next" button.

8. Wait for the updates to install and then select "Finish" when it finishes.
9. Reboot your computer to finalize the install.

Running a Scan:

(before running a scan make sure you have run "Live Update" while connected to the internet. Otherwise your scan will be a waste of time.

1. Double-click on the yellow shield on the bottom right-hand side of your screen or go to Start, All Programs, Symantec Client Security, Symantec Antivirus
2. Click on "Scan" in the list on the right and then choose "Scan Computer". On the right hand side of the window, select your hard drives and then click the "Scan" button.

Glossary

Adware: Anything which installs itself on a computer (often without permission) that advertises products or services. One of the most prominent forms of this type of infection is “pop-up” windows occurring mostly, in a web browser. Another feature of this infection might be hijacked browsers. I.E. having homepages changed to unwanted sites, or being redirected to a different page when attempting to reach another.

Hijack: Hijack is a term used to describe what happens to a web browser after a malware infection. A hijacked browser will often load an unwanted page when the browser is first run. Sometimes a hijacked browser will even prevent a browser from reaching pages they want to go. For example, trying to access www.uvm.edu and being redirected to www.yaymalware.com.

Another symptom of a hijacked browser is the occurrence of unwanted toolbars/search bars on the web browser window. This type of behavior is very common with an infected version of the popular web browser, Microsoft Internet Explorer.

Pop-ups: Pop-ups are windows which appear on top of other web pages used primarily for the purposes of advertising. There are a few different kinds of pop-ups. First, there is the harmless and sometimes useful type.

The second kind of pop-up appears when you enter certain web sites which knowingly incorporated the pop-up ad to increase revenue. These are annoying but at least somewhat legitimate.

The third type of pop-up is the worst - they pop up over pages which have no affiliation with the advertised product, and of-

ten display several windows at a time.

Pop-ups (cont'd):

For example, pop-ups advertise while you browse UVM's page. Sometimes these pop-ups even come up when you are not browsing the web! If you have this kind of pop-up on your machine, perform a malware scan immediately - this is typically a good indicator of such an infection.

Spyware: Anything installed on your computer which collects various information. Spyware is typically installed without the user knowing and secretly collects/sends the collected data out for someone to retrieve. Anything from web browsing habits to passwords - even credit card numbers - can be collected by spyware components.

Also known as: **Data-miners & Scumware**

Viruses:

A **computer virus** is a self-replicating computer program that spreads by inserting copies of itself into other executable code or documents. A computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. Extending the analogy, the insertion of a virus into the program is termed as an "infection", and the infected file, or executable code that is not part of a file, is called a "host". Viruses are one of the several types of malicious software or malware.

Machines that are not kept up to date (i.e. Microsoft Windows Updates) are more susceptible to infection. Certain viruses are categorized as Trojans. Trojans open up secret back doors on a computer which allow hackers to log into your machine and have as much control as a person sitting in front of it.

This page left intentionally blank.

