Basic Virus Removal Steps

The following are basic instructions on how to remove most virus and spyware that infect Windows XP/Vista computers. By providing these, we hope that users will be able to remove infections on their computers with minimal downtime. These steps are not a complete list.

The Technology Help Desk encourages users to read through the entire document before taking any action. It is recommended that you have copies of Operating System or Reinstall disks available. Backup all important data to your H Drive or another external media (hard drive, flash drive, CD, etc).

Finally, if you are not certain about a virus, do a Google search to find out more information. New viruses are released daily and it is impossible to keep on top of them all.

1. **Disable System Restore**
    a. XP: Click **Start – Control Panel – System - System Restore** tab.

       Vista: Click **Start – Control Panel – System – System Protection**.
    b. XP: Check **Turn Off System Restore**

       Vista: Uncheck Hard Drives if selected.

    Why?

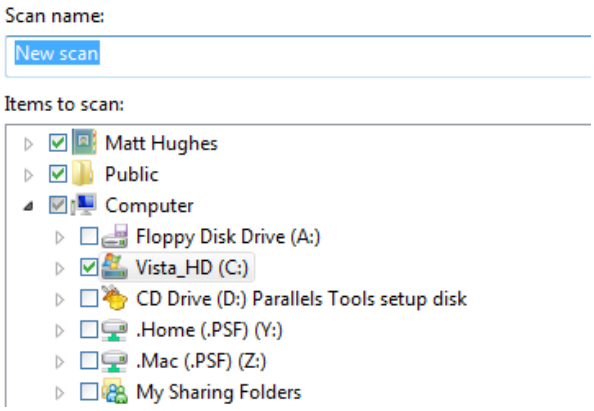
    Many viruses reside in the System Restore files which are inaccessible by most Anti-Virus and Anti-Spyware programs. Disabling System Restore will prevent the virus from running again immediately after you think you've cleaned it off.

2. **Download Windows Updates**
    a. Open Internet Explorer
    b. Go to http://windowsupdate.microsoft.com
    c. Click **Express** and **Install Updates** when prompted.

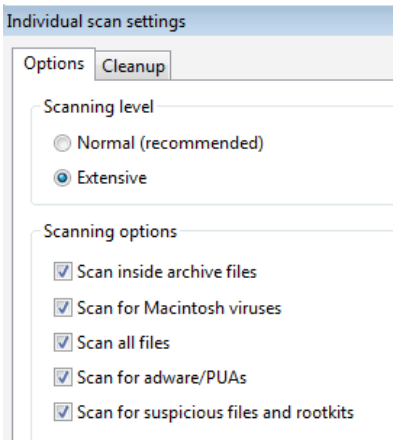
    Why?

    Most viruses and spyware get into a computer by taking advantage of a hole or exploit. Keeping it up to date with the latest patches prevents this from happening.

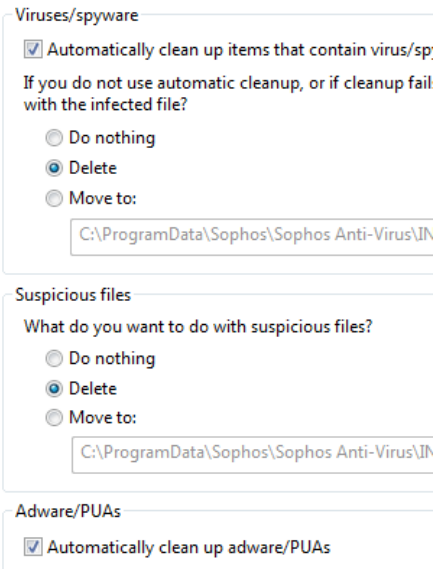
3. **Run a Complete Sophos Anti-Virus Scan**
    a. **Right Click** on the blue **Sophos Shield** on your Taskbar and select **Open Sophos Anti-Virus**.
    b. Click **Setup a new scan**.
    c. In the Scan Name field, enter a name (Complete Scan, AV Scan, etc)
    d. In **Items to Scan**, select the checkbox next to your hard drive (typically C:)



    e. Click **Configure This Scan**.
    f. In the **Individual Scan Settings**, choose the **Options** tab.
    g. Under **Scanning Level**, select **Extensive**.
    h. Under **Scanning Options**, check every box.



    i. Choose the **Cleanup** tab.
    j. Check **Automatically cleanup items that contain virus/spyware**.
    k. Check **Delete** under both **Virus/Spyware** and **Suspicious Files**.
    l. Check **Automatically cleanup Adware/PUAs**.



m. Click **OK** and then **Save and Start**

n. When the scan is complete, **reboot** your computer**.**

o. Open Sophos Anti-Virus and click on **Start** next to the scan you setup to repeat the process one more time.

Why?

An extensive Sophos scan may take several hours to complete. If you have a laptop, make sure it is plugged into the AC Adapter. The scan should find and delete most viruses and spyware that it encounters. What it cannot fix, it will throw into Quarantine. A reboot followed by a second scan makes sure no items returned.

4. Clean Up Quarantine (if necessary)

a. Open Sophos Anti-Virus and click on the **Quarantine** link.

b. Each item listed will have up to three options: Authorize (permit a file), Clean Up (attempt to disinfect), or Delete (remove from your system).

c. Attempt to **Clean Up** or **Delete** each file.

Why?

Not all viruses or spyware are moved during the scan. Some require a more extensive clean up procedure. Files in Quarantine are, in theory, harmless to your computer but you should still make every attempt to remove them.

5. **Run an Anti-Malware scan with Malwarebytes**
    a. Download and Install Malwarebytes
        i. http://www.malwarebytes.org/mbam-download.php
        ii. Or use the Norse Clean CD in the Win directory
    b. Start Malwarebytes and select the **Scanner** tab.
    c. Choose **Perform Full Scan** and click **Scan**.
    d. Select your hard drive(s) and click **Start Scan**.
    e. Malwarebytes will begin scanning. Depending on the speed of your computer, this could take up to several hours.
    f. When finished, Malwarebytes will display the results if anything is found.
    g. Place a check next to each item to be removed and click **Remove Selected**.
    h. Items will be removed and you may be prompted to restart your computer.
    i. A log file will be generated. Save it to your Desktop or another easy to remember location.

Why?

Spyware (aka Adware, Malware) is increasingly common and can present as many problems as a virus might. It can slow down a computer, cause multiple pop-ups, install other software, or even invite in more damaging viruses. Removal is highly recommended. Sophos can detect and clean up many pieces of spyware, but it is not capable of doing it to all.

6. **If viruses remains:**
    a. **Backup your data.**
        i. Viruses that remain to this stage can be deeply imbedded in your system. On occasion, these are in important files and may cause system damage in an effort to remove them. Get your data backed up to your H Drive or an external drive before continuing.
    b. Boot your computer into Safe Mode and run a Sophos scan. Some viruses are loaded when the computer starts, making them difficult to remove. Safe Mode removes this. To get into Safe Mode:
        i. Shut down your computer.

ii. Power on and press **F8** (repeatedly) after hearing the initial beep
iii. When presented with a list of options, use the arrow keys to select **Safe Mode** and press **Enter**.
iv. Click Start – Sophos Anti-Virus – Sophos Anti-Virus to open (the blue shield will not appear on the taskbar).
v. Run a Sophos scan as indicated in earlier steps

c. Note the name of the virus and visit http://www.sophos.com and enter the virus name in the Search box. This can provide information on how to better clean up the virus.
d. Google the virus name. There are many websites that have very comprehensive instructions on how to remove particular viruses plus some tools specifically designed for it.

Contact the Help Desk *only* after you have completed all of the above steps.