



SELF HELP VIRUS CLEANING INSTRUCTIONS

Please follow these instructions completely to clean your computer of viruses and update it against further infection.

✓ **Unplug your computer from the Network**

✓ **Clean off all temporary Internet files:**

1. Open Internet Explorer and choose **Tools > Internet Options**
2. In the **Temporary Internet files** section, choose to **Delete Files**
3. When the small dialogue box opens, choose to **Delete All Offline Content**
4. Say **OK** and let this run
5. When its finished, close the Internet Options window and the browser window.

✓ **Turn OFF System restore (for Windows XP users only)**

1. Right click on **My Computer > Properties**
2. Click the **System Restore Tab**
3. Click the box **Turn off System Restore**
4. Click **OK**

✓ **Boot (restart) the computer into Safe Mode**

1. To boot into **Safe Mode**, reboot/restart your computer. As soon as it starts up, start tapping the **F8** key (you must do this prior to seeing the Windows Startup screen).
2. You will be presented with the **Windows Advanced Options menu** (on a black, command prompt style screen). Use your arrow keys to choose **Safe Mode**.
3. Once in **Windows Safe Mode**, click **OK** to accept the **Safe Mode** notice.

✓ **Obtain and Run Stinger while your computer is still in Safe Mode**

1. Run **Stinger** by accessing it from the **ResNet Resource CD (CDROM drive:\Stinger\stinger###.exe)**
2. Click the **Scan Now** button
3. Delete all Virus infected files
4. Close **Stinger (File > Close)**

✓ **Obtain and Run HijackThis while in Safe Mode (Advanced Users Only)**

1. Run HijackThis by accessing it from the the **ResNet Resource CD (CDROM drive:\Utilities\ HijackThis.exe)**
2. Click the **Scan** button
3. Tag (place a checkmark beside) the suspicious entries. These will include:
 - a. Spyware (CoolWebSearch, SearchMiracle, BullsEye, Webrebates, voltio, etc)
 - b. Adware (Blazefind-windupdates, Navisearch, Windows SA-omniscient, WinAd, etc)
 - c. Malware (Ratsou/Gayporn-svcchosts,crss32,svchosts, SDBot, Gaobot, Rbot, etc)
 - d. Browser Helper Objects (BHOs) that call executable or DLL files (examples of BHOs can be found here: <http://sysinfo.org/bhoinfo.html> - many programs now generate random named BHOs)
 - e. HKEY Current User/Run (HKCU/Run) or HKEY Local Machine/Run (HKLM/Run) registry keys that call unknown executables or DLL files and/or call them from suspicious places like c:\windows, c:\documents & settings, or no path at all
 - f. Dynamic Packet Filters (DPFs) that call executable, DLL, or CAB files or point to suspicious web sites
4. Click the **Fix Checked** button to remove the tagged entries.
5. Repeat this process until you are satisfied that nothing has returned and that everything you want to remove has been removed.

✓ **Boot (restart) your computer back into Normal Mode**

1. While in **Windows Safe Mode**, click **Start, Shutdown** and then **Restart**
2. Allow the computer to start up as normal

✓ **Ensure all other antivirus software packages are either uninstalled or inactive**

1. Use Add/remove programs to uninstall or Norton IS Removal Tool from ResNet Resource CD if applicable/necessary.
2. To make inactive, use MSCONFIG and prevent the AV software from starting up.

✓ **Obtain and Install McAfee antivirus software**

1. Install McAfee using the setup at ResNet Resource CD (CDROM drive:\Anti-Virus\- 2. Update McAfee using the DAT/SDAT file here: ResNet Resource CD (CDROM drive:\Anti-Virus\

✓ **Scan the computer to ensure it is virus-free:**

1. Right click on the **V-shield icon** that should now be present in your System Tray
2. Choose the **On Demand Scan** option
3. On the **Where** tab specify that **All fixed disks** and **Memory of running processes** should be scanned
4. Under **Scan options** ensure **Include subfolders** and **Scan boot sector** are chosen
5. Under **Advanced** tab ensure **Find potentially unwanted programs** and **Find joke programs** are chosen
6. Click on the **Scan Now** button in the right hand side of the window
7. If any infected or identified files are not automatically deleted, manually tag and delete them.
8. If any infected or identified files cannot be deleted, restart in safe mode, run scan again with the same options and delete the identified files. Reboot into normal mode when finished.

✓ **Please follow these next steps to ensure you are properly protected against further infection (for Windows XP users only):**

1. Choose **Start > Control Panel > Network Connections**
2. Right click on your **Local Area Connection** (the one affiliated with ResNet if there is more than one)
3. Choose the **Properties** option from the context menu
4. Choose the **Advanced** tab on the **Local Area Connection Properties** window
5. Put a check mark in the **Internet Connection Firewall** or **Windows Firewall** selection
6. Click **OK** to close this window

✓ **Turn System restore ON again (for XP users only):**

1. Right click on **My Computer > Properties**
2. Click the **System Restore Tab**
3. Remove the check from the **Turn off System Restore** box
4. Click **OK**
5. Restart the computer

You may also wish to follow these additional steps to more fully protect your machine against further infection (recommended for Advanced Windows XP users)

✓ **Turn OFF System restore**

5. Right click on **My Computer > Properties**
6. Click the **System Restore Tab**
7. Click the box **Turn off System Restore**
8. Click **OK**

✓ **Secure user accounts**

1. In XP Pro use **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups > Users** to ensure that:
 - o Guest account is disabled
 - o Administrator account is password protected (use same password as main user account or create new one and inform client)
 - o Main user account and any other user accounts are password protected if client is amenable to that

2. In XP Home restart in safe mode, log in as Administrator and use Start > Control Panel > User Accounts to ensure that:
 - o Guest account is disabled
 - o Administrator account is password protected
 - o Main user account and any other user accounts are password protected if client is amenable to that
 - o Restart in normal mode after finished

✓ **Disable simple file sharing**

1. In XP Pro use **Start > Control Panel > Tools menu > Folder options > View tab** to ensure that **Use simple file sharing** is turned off (unchecked)
2. In XP Home use **Start > My Computer > Right-click Local drive C: > Sharing and Security** to ensure that file sharing is turned off.

✓ **Plug network cable into the computer**

1. Connect the computer to the network and reboot
2. Go online to <http://windowsupdate.microsoft.com> and scan and install the latest **Critical Updates** for the computer.
3. Do not install SP2 as we do not know if all manufacturers have guaranteed that their machines will run properly with SP2.

✓ **Turn System restore ON again (for XP users only):**

6. Right click on **My Computer > Properties**
7. Click the **System Restore Tab**
8. Remove the check from the **Turn off System Restore** box
9. Click **OK**
10. Restart the computer

✓ **Plug network cable into the computer**

3. Re-connect your computer to the network (plug in the cable) and reboot
4. Go online to <http://windowsupdate.microsoft.com> and scan and install the latest **Critical Updates** for your computer.

✓ **Install McAfee antivirus software**

3. Insert the **ResNet Resource CD**
4. An auto install window will show up or you can browse to the **Anti-virus** folder and install McAfee using the installer appropriate for your operating system (eg., install from the WindowsXP/2000 folder if you have windows XP, or the Windows98/ME folder if you have Windows 98)
5. Follow all the steps to install the McAfee VirusScan – call the CCS Help Centre if you have any difficulties at x58888.

✓ **Once VirusScan is installed, scan your computer to ensure it is virus-free:**

9. Right click on the **V-shield icon** that should now be present in your Task Manager (bottom right of your desktop)
10. Choose the **On Demand Scan** option
11. On the **Where** tab specify that **All fixed disks** and **Memory of running processes** should be scanned
12. Under **Scan options** ensure **Include subfolders** and **Scan boot sector** are chosen
13. Click on the **Scan Now** button in the right hand side of the window
14. Follow MacAfee's instructions for cleaning off any found viruses

✓ **Now turn System restore ON again (for XP Users only):**

11. Right click on **My Computer > Properties**
12. Click the **System Restore Tab**
13. Remove the check from the **Turn off System Restore** box
14. Click **OK**
15. Restart the computer

If you have any questions or difficulties understanding these instructions, please call ResNet support at x58888 option 2. If you are unsuccessful cleaning off the virus on your computer, you have the option of requesting a ResTech visit at a charge of \$35 to see if we can clean your virus for you. Call ResNet support for more details at x58888, option 2.



2004-2005