

Cleaning Your Infected Computer: Steps to Clean Your Machine

This document contains the following sections:

- Symptoms of Infection or Compromise
- Basic Steps to Clean Your Windows Computer:
- Step 1: Verify Anti-Virus
- Step 2: Boot into Safe Mode / Run Symantec Anti-Virus
- Step 3: Web-Based Scans
- Step 4: Anti-Hijacking / Anti-Spyware
- Step 5: Verify the Computer is Clean
- Step 6: Enable the Firewall
- Step 7: Establish Passwords
- Clean? Keep it that way
- Advanced Steps:
- Other Diagnostic Tools
- MSCONFIG

Symptoms of Infection or Compromise

Is your computer infected or compromised? The following is a list of symptoms you may have noticed:

- Crashing often
- Computer seems a little slower
- Running out of Windows "resources"
- Having to reboot often
- Persistently slower than usual Internet access
- Home page has changed
- More popup windows than usual
- E-mail or Internet access a lot slower

Basic Steps to Clean Your Windows Computer

Step 1: Verify your Anti-Virus is up to date

In most cases, computers are infected by trojans, viruses or worms as a result of opening an e-mail attachment. To clean your machine from these infections, follow these steps to run the antivirus software.

Note:

Step 2: Boot into Safe Mode

Follow these steps to boot your computer into Safe Mode and diagnose the problem in a safe environment.

Note: While in Safe Mode, you will only have access to very basic files and drivers, mouse, monitor, keyboard, etc. You will not have access to network connections.

Note: You will be unable to boot into Safe Mode if Windows required system files are corrupted.

1. **Important!** Be sure that you have updated the virus definitions files before following this procedure.
2. Click **Start > Shut Down**.
3. Select **Restart**.
4. Depending on whether you have multiple operating systems loaded on your machine, follow the appropriate step below:
 - If your machine offers only one operating system, begin tapping the **F8 key** before your machine reaches the Window's display screen.
 - If your machine offers multiple operating systems, select the appropriate operating system from the list, then begin tapping the **F8 key**.
5. Use your up or down arrow keys to select and highlight the appropriate safe mode option. Press **Enter**.

Note: NUM LOCK must be off before the arrow keys on the numeric keypad will function.
6. Once you have logged onto Windows in Safe Mode, launch your AntiVirus.
7. Select **Scan** to expand the drop down menu, then select **Scan Computer**.
8. The scanning process begins. This can take several minutes. Once complete, the software will display any problems that it has found and will provide further instructions.
9. Restart your computer.

Step 3: Web-Based Scans

Even if you have an updated Anti-virus running on your computer, there are instances when a Trojan will disable the anti-virus software or render it from working properly. Thus you should make it a practice to do a free web-based security and virus scan from [Symantec](#) or [Trend Micro house call](#).

Note: The web-based scan is only possible if you have internet connectivity.

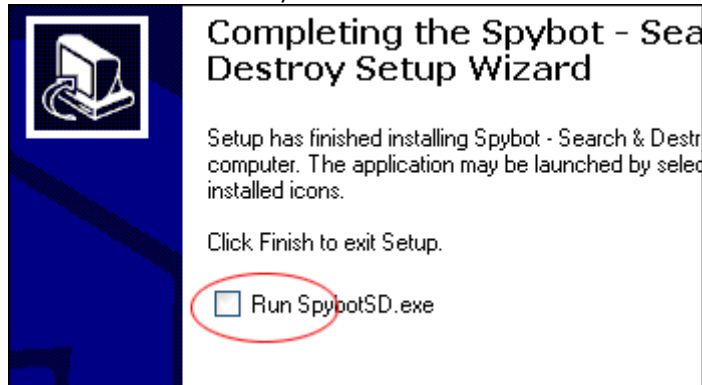
Step 4: Anti-Hijacking / Anti-Spyware

Download, install, update and run one or more of the following anti-hijacking and anti-spyware products. We recommend running at least two of these programs to ensure any malicious program is detected and removed.

Be sure to download the Detection Updates before running either of these programs. Follow these steps:

Spybot Search & Destroy

1. Download Spybot Search & Destroy and save it to your desktop.
2. **Double-click** on the icon to install the program. Through the installation, click **Next** to accept the default responses.
3. At the end of the installation, **be sure to DESELECT** the checkbox to Run



4. Spybot.
4. Download Updates for Spybot - Search & Destroy.
5. **Double-click** the Spybot Search & Destroy Installer icon (not the Detection Update) to launch the program.
6. At the prompt to **Create registry backup**, click **Next**. This is not necessary.
7. Click **Search for Updates**.
8. If updates are found, click **Download All Available Updates**.
9. Click **Next**.
10. Click **Immunize this System**.
11. Click **Next**.
12. Click **Start Using the program**.
13. From the Spybot S&D window, click **Search & Destroy**.
14. Click **Check for Problems**.
15. If problems are found, they are selected and listed at the bottom of the window. Click **Fix Selected Problems**.
16. When the recovery is complete, close Spybot.

Ad-aware

1. Ad-aware
2. Download Detection Update for Ad-Aware (After downloading, copy this file into the C:\Program Files\Lavasoft\Ad-Aware SE Personal folder. Overwrite the old file when prompted.)
3. Run Ad-aware.

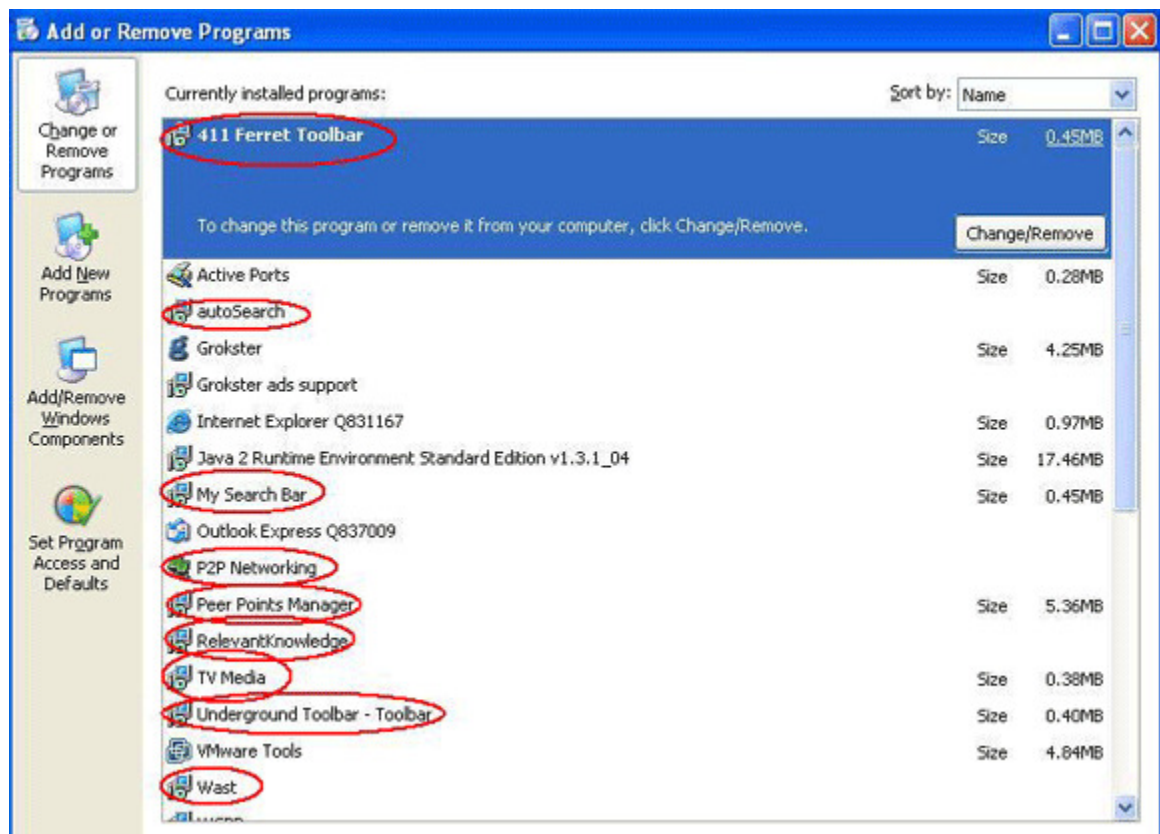
Step 5: Verify the Computer is Clean

Once you've successfully run the anti-hijacking / anti-spyware program, you should verify that the software on your computer is indeed software that you installed. Hackers and unscrupulous websites often install "legitimate" spyware/adware software, and because the server software is legitimate it will not show up in a virus scan.

Follow these steps to remove unwanted software:

1. Select **Start > Control Panel > Add Remove Programs**.
2. Search the list for software that you did not install.

Note: Look for items such as Toolbar Software, Casino Software, Rebate Software and Shopping Software. The illustration below shows some circled software that will cause random pop-up windows, user tracking, slowdowns, lockups and other problems. While this problematic software can be uninstalled here, to ensure it's fully removed you will need to run Adware and Spyware removal software as outlined above.



3. Look for listening and connected ports on your machine. A listening port or connected port indicates your machine is connected, or awaiting a connection, to an external computer. Follow these steps:
4. Download and install the **Active Ports** program (do NOT run the program; proceed to the following step).
5. Close ALL programs that may use a network or Internet connection. This includes web browsers, e-mail programs, chat programs and file sharing programs.
6. Run the **Active Port** program.

- If you notice an established connection to other machines even when your browser and e-mail programs are closed, your computer could still be compromised. Contact someone for further advice.

In the example below, the computer indicates NO active connections and no hidden programs that are establishing connections to other computers.

Process		Local IP	Local Port	Remote IP	Remote Port	State	Protocol	Path
UDP System	4	192.168.141.1	138			LISTEN	UDP	
UDP System	4	192.168.141.1	137			LISTEN	UDP	
UDP System	4	0.0.0.0	445			LISTEN	UDP	
TCP System	4	192.168.141.1	139			LISTEN	TCP	
TCP System	4	0.0.0.0	445			LISTEN	TCP	
UDP lsass.exe	360	0.0.0.0	4500			LISTEN	UDP	C:\WINDOWS\system32\lsas
UDP lsass.exe	360	0.0.0.0	500			LISTEN	UDP	C:\WINDOWS\system32\lsas
TCP svchost.exe	596	0.0.0.0	135			LISTEN	TCP	C:\WINDOWS\system32\sv
TCP alg.exe	1020	127.0.0.1	1026			LISTEN	TCP	C:\WINDOWS\System32\alg
UDP svchost.exe	1264	192.168.141.1	123			LISTEN	UDP	C:\WINDOWS\System32\sv
UDP svchost.exe	1324	0.0.0.0	1025			LISTEN	UDP	C:\WINDOWS\System32\sv
UDP Rtvscan.exe	1480	0.0.0.0	2967			LISTEN	UDP	C:\Program Files\Symantec A

In the example below, this computer indicates an active connection to "Unknown". In this case, the user should run further removal software to determine what is on the computer.

Process		Local IP	Local Port	Remote IP	Remote Port	State	Protocol	Path
TCP Unknown	0	128.2.125.58	1062	207.68.171.245	80	TIME_WAIT	TCP	
TCP Unknown	0	128.2.125.58	1058	128.2.14.3	139	TIME_WAIT	TCP	
UDP System	4	128.2.125.58	138			LISTEN	UDP	
UDP System	4	128.2.125.58	137			LISTEN	UDP	
UDP System	4	0.0.0.0	445			LISTEN	UDP	
TCP System	4	128.2.125.58	139			LISTEN	TCP	
TCP System	4	0.0.0.0	445			LISTEN	TCP	
UDP lsass.exe	668	0.0.0.0	500			LISTEN	UDP	C:\WINDOWS\system32\lsa
TCP svchost.exe	836	0.0.0.0	135			LISTEN	TCP	C:\WINDOWS\system32\sv
UDP svchost.exe	936	128.2.125.58	123			LISTEN	UDP	C:\WINDOWS\System32\sv
TCP svchost.exe	936	0.0.0.0	1025			LISTEN	TCP	C:\WINDOWS\System32\sv
UDP svchost.exe	1112	0.0.0.0	1030			LISTEN	UDP	C:\WINDOWS\System32\sv
UDP svchost.exe	1124	128.2.125.58	1900			LISTEN	UDP	C:\WINDOWS\System32\sv
TCP svchost.exe	1124	0.0.0.0	5000			LISTEN	TCP	C:\WINDOWS\System32\sv

Step 6: Enable the Firewall

A firewall is a system designed to reinforce the Security of the data flowing between two networks, the internal network and the outside network, such as the Internet. All messages entering or leaving pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. Firewalls can also make your computer "invisible" to the outside world so that it doesn't become an easy target for an attacker.

Follow these steps to enable the Windows XP Internet Connection Firewall (ICF):

1. Click **Start -> Control Panel**.
2. Double-click **Network Connections**.
3. Right-click the connection on which you would like to enable ICF (i.e., Local Area Connection, Wireless connection) then click **Properties**.
4. On the **Advanced** tab, click the box to select the option to **Protect my computer or network**.
5. If you want to enable the use of some applications and services through the firewall, click the **Settings** button, and then select the program(s), protocol(s), and service(s) to be enabled for the ICF configuration.

Step 7: Establish Passwords

After your computer has been cleaned you should change passwords on the computer and verify that an Administrator account and password has been established.

1. Click **Start > Control Panel > User Accounts**.
2. Check for any User Accounts you didn't add. This may indicate a hacker has accessed your system.
3. Ensure the **Guest account** is disabled.
4. Click your **User Account** and the **Administrator User Account** (if applicable), and reset the password for each respective account.

Advanced Section

Other Diagnostic Tools

There are many built-in Windows diagnostic programs you can run to determine what is exactly happening on your computer. Unless otherwise noted these programs are run at the command prompt. Follow these steps:

1. Click **Start > Run**.
2. Type **CMD**. A command shell window appears.
Note: You can also find advanced diagnostic utilities on this page.
3. Enter one of the following at the command prompt:
 - **netstat** - Shows all listening ports and all current connections to those ports. Common Port list; Common "Trojan" Port list;
 - **nbtstat** - Lists all current and recent NetBIOS connections.
 - **arp** - Shows MAC addresses that the computer has been communicating with.
 - **eventvwr.msc** - Shows system, application and security logging information for the computer. (Be sure to type the .msc after the typing eventvwr).

- **fsmgmt.msc** - Shows shared folders and files and connected users on the computer. (Be sure to type the .msc after the typing fsmgmt).
- **at** - Shows scheduled jobs on the computer. This is a common ploy by attackers to run programs such as Trojans. A typical computer shouldn't have any scheduled jobs.
- **msconfig** - For Windows XP computers, displays system settings. Of notable interest is the "Startup" tab. Contact us if you have questions about suspicious startup items. Click [here](#) for additional technical details.

MSCONFIG

Windows XP users can also run MSCONFIG. Follow these steps:

1. Click **Start > Run**.
2. In the text box, type **MSCONFIG**.

Of notable interest is the **Startup** tab. Many trojans will place programs here that run when the computer starts up.

Note: Many legitimate programs will be installed here so disable programs with caution. If in doubt call or ask someone who will know if the program is necessary.