Virus & Malware Cleaning Instructions

(Last Update: 06/28/2010, 02:57 PM, Version 1.028)

If you have one of those nasty Trojan viruses that tells you your Windows computer is infected (yes, it is!) and you need to buy their antivirus software, then chances are you have inadvertently downloaded a virus onto your computer from a more-than-likely malicious website. The owners of these products are unscrupulous scammers, and what they are selling will not help in any way. In fact, you will get this message even if you already have an antivirus package installed, but has not detected the problem early enough. According to Google and other web statistics, there are over 70,000 websites that serve this malicious type of code and constantly growing! So, the better thing to do is play it safe and avoid visiting all those ***free*** websites, as they are the ones that usually end up giving you these infections. Also, having a robust antivirus/antimalware product like AVG or Norton, is the best way to prevent these sorts of problems. And, backup your computer on a daily basis!

Note: This document will change continuously as new technologies need to be used to combat these problems. But, it should provide you a place to start restoring your system back to normal.

There are several items covered in these instructions. Here a few things to take into account the level of your problem(s).

- It is best to perform the instructions in *Safe Mode with Networking* for downloading items, or without networking, if just cleaning the infections. See section ***Starting Your Computer in Safe Mode with Networking***.
- If you are unable to get to any websites at all, you will either need to download and copy the necessary antivirus/antimalware files from a different computer using a CD/DVD or USB drive, or you can use section ***Resetting Internet Explorer*** to get this to work.
- If you are able to get to websites, such as http://www.msn.com, then see section ***Running Malwarebytes' Antimalware***. Under Windows Vista, you won't be able to install under *Safe Mode with Networking* as the *Windows Installer* service is disabled in all *Safe Mode*(s).
- If things look really bad, then see section ***Running BleepingComputer.Com's ComboFix*** as a second-to-last resort. It is powerful and cleans all sorts of things.
- If your computer still does not get back to normal, you may try one of those websites where you can upload *Hijack This* logs and experts help you to get back to normal. Sounds like a lot of work and requiring some tech savvy and a lot of patience!
- Sometimes, you just won't be able to get the infections off your computer easily, and the best thing to do is to attempt to backup all your data (documents, music, pictures and videos), if you are not already doing so regularly (daily?), and reinstall the Windows operating system (OS) from scratch. Some computers come with a recovery partition and it is pretty easy to restore from here. Others will require the Windows installation CD. Refer to your computer's tech support service if it is still under warranty, its user's manual, or look up your options on the manufacturer's website.
- Make sure to install either antivirus or internet security packages from a reputed vendor such as *AVG* or *Norton*. The *AVG Antivirus Free Edition* is an excellent product, but if you keep getting infected, and cannot change your behavior, then pay for and get the best product you can find! See section ***Installing AVG Antivirus or Internet Security (v9.0)***.

Starting Your Computer in Safe Mode with Networking

Use these instructions to always start your computer in *Safe Mode with Networking* while fixing these problems:

1. Shutdown the computer.
2. Restart the computer and as soon as the memory diagnostics or hardware logo (Dell, HP, Sony, Intel, AMD, etc.) appears, ***start pressing F8 repeatedly and quickly***.

Note: *If* Windows *starts loading, then you didn't start pressing* F8 *early enough. To save time, you can shut down the computer immediately by holding down the power button for 5-10 seconds. Turn it on again and repeat this step.*

3. If you interrupted the start up correctly, then the *Windows Startup Options* screen appears. Use the *Up-Down Arrow keys*, select *Safe Mode with Networking*. Press Enter.
4. You may need to select which operating system to start. Select the default *Windows XP* (*Vista*, *7*, etc.) configuration; hopefully, that is the one you always use!
5. You may also need to log in with an *Administrator-equivalent* account.
6. *Windows* may inform you that you are running in *Safe Mode*. Accept the message to continue.
7. The *Windows Desktop* will appear in 800x600 resolution, so the desktop icon locations may be messed up.

Resetting Internet Explorer

Use these instructions to reset Internet Explorers settings when you are unable to get to websites such as http:///www.msn.com:

1. Start *Internet Explorer*.
2. Open menu *Tools | Internet Options*.
3. Select tab *Connections*.
4. Click *LAN Settings*.
5. Turn ON *Automatically Detect Settings*.
6. Turn OFF *Use Automatic Configuration Script*.
7. Turn OFF *Use Proxy Server for your LAN*...
8. Click *OK*.
9. Click *Apply*.
10. Select tab *Advanced*.
11. Click *Reset*.
12. Turn ON *Delete Personal Settings*. Wait a while for it to finish.
13. Click *OK* to close *Internet Options*.

Running Malwarebytes' Antimalware

Use these instructions as a first step to clean out a malicious virus infection. Make sure to start your computer in *Safe Mode with Networking*, or have downloaded and copied the necessary files in these instructions from a different computer:

1. Start *Internet Explorer*, or any other browser like *Firefox*, *Chrome*, or *Safari*.
2. Download *Malwarebytes' Antimalware* from: http://download.cnet.com/Malwarebytes-Anti-Malware/3000-8022_4-10804572.html?part=dl-10804572&subj=dl&tag=button
3. Save the file (e.g., *mbam-setup-1.46.exe*, depending on the currently published version) on your computer to a folder where you can locate it.
4. Open/Run/Launch the file and click *Run* when the *Window's* warning message appears.
5. The installation program will proceed. Select affirmative responses like *Next*, *I Agree*, *Yes*, *Continue*, etc.
6. Select *Update Malwarebytes' Antimalware* and *Run Malwarebytes' Antimalware.* This will first update to the latest virus signatures, and then run the program as well.
7. On the *Scanner* tab, select *Perform Full Scan*, and click *Scan* to continue.
8. Allow the program to run its scan. It may take 20-40 minutes or more, depending on what all they have installed on their computer, hard drive size, processor speed, personal files, etc. Hopefully, it will find any infections.
9. When it is done, you will be notified to click *Show Results*. Please do so.
10. You will be presented with a checked list of potential infections. Make sure they are checked and click *Remove Selected*. You may be prompted to restart your computer.
11. Restart the computer, and try to run *Internet Explorer* and see if things have stabilized.
12. You may wish to run *Malwarebytes* again just to make sure the infections have not returned.

Note: If the infections have returned, then try ***Running ComboFix****.*

Running BleepingComputer.Com's ComboFix

If you tried *Malwarebytes*, and the infections keep returning, then you have a more serious case, which requires a more brute-force method of cleaning. Use *ComboFix* to do this:

1. Start *Internet Explorer*, or any other browser like *Firefox*, *Chrome*, or *Safari*.
2. Open: http://www.bleepingcomputer.com/combofix/how-to-use-combofix
3. In the *Using ComboFix* section, click the download link for **BleepingComputer.Com**. It may change, but it is usually: http://download.bleepingcomputer.com/sUBs/ComboFix.exe.
4. Save the file to a location such as *C:\ComboFix*.

Note: If your antivirus/antimalware software is running and you are unable to disable it temporarily (AVG makes it very hard to do this!), then just select Allow *when you get warning messages about allowing malicious software to run once you have started* ComboFix*. Do not use* Allow *at other times unless you know the program you are running wants to access the internet, etc.*

5. As instructed, you may print out the page and follow the instructions. Eventually, you will just be running the program to fix the problem.
6. Open the folder you selected in the earlier step and double-click *ComboFix.exe* to run it.
7. It does not have an installation program, but you may be prompted to install Microsoft Windows Recovery Console package. Please allow it to do so by selecting affirmative responses like *Next*, *I Agree*, *Yes*, *Continue*, etc.

8. Once it starts running, it may take quite a while to finish its work. At the time of writing, it had over 50 step, so be patient. It may tell you to reboot at least once. Please do so.
9. You may wish to run *ComboFix* again just to make sure the infections have not returned.

Note; If the infections have returned and you do not want to diagnose this further, then reinstall the Windows OS from scratch or use your computer's recovery partition to restore the manufacturer's original system configuration.

Installing AVG Antivirus or Internet Security (v9.0)

Use these instructions to download and install *AVG*'s *Antivirus* (free/paid) or *Internet Security* packages. This is a very good free product, or an excellent paid version that is recommended if you tend to go to a lot problem websites. It is recommended that you use just the *Antivirus* package for a home-based computer, such as a desktop or laptop that does not leave the house and your own network. Purchase and install the *Internet Security* package, if you frequent other networks such as internet cafes. Here are some brief instructions to get you going:

1. Restart the computer without interrupting it.
2. Start *Internet Explorer*, or any other browser like *Firefox*, *Chrome*, or *Safari*.
3. Download the latest version of *AVG* from:

Antivirus Free:	http://free.avg.com/us-en/download-avg-anti-virus-free
Antivirus Paid:	http://www.avg.com/us-en/buy-avg-antivirus
Internet Security:	http://free.avg.com/us-en/download-avg-internet-security

Note: These links are constantly changing and could be out of date, so it may take a few clicks on http://www.avg.com to locate the free antivirus download.

4. Run the installation program. Select affirmative responses like *Next*, *I Agree*, *Yes*, *Continue*, etc. Use the recommended settings for *Custom* with *All* components selected, and a *DAILY* (not weekly) full system scan at *4 AM*.
5. Let it update and then allow it to run the *Optimization Scan* and then a *Full System Scan*.

Installing Windows Updates

It is recommended to apply all *Windows/Microsoft Updates* to your computer. These are usually weekly security and product updates released by *Microsoft* for your *Windows* computer. The following instructions are provided in brief, but a more detailed version can be found at:

http://sunnysolutions.biz/Documents/WindowsUpdateComV6.pdf

1. Start *Internet Explorer* (only works from *IE*, no other browser can be used to do *Windows Updates*!)
2. Open http://www.WindowsUpdate.Com.
3. Install all *Critical/High* updates repeatedly.
4. Restart the computer if requested to do so.
5. You may need to run this several times, before all updates have been installed.
6. You may install *Software* updates.
7. Do not install *Windows Search*, unless you have a fast computer and really need this feature; it is a resource hog.
8. Do not install *Hardware* updates, including printer drivers, unless you know what you are doing!