Sun City Computer Guy

Virus and Malware Removal Checklist

www.suncitycomputerguy.com scalcomputerguy@gmail.com

NOTE: Before you run this entire checklist, especially if you have had the malware/virus for just a couple hours, simply run the Malwarebytes Anti-malware program and your anti-virus program each in the "threat scan" or "full computer scan" mode. It may remove your malware/virus on the first shot. If you have had the malware/virus for days, read on…

> **WARNING: NO ONE, not even me, can guarantee that every malware or virus can be removed. If you have a virus, some or all of your data may already be lost or can be lost trying to remove the virus. This checklist will help guide you through the process of removing a virus, but NO ONE can guarantee success. Back up your data before you begin!**
>
> WARNING: I've tried my best to be sure there are no errors in this checklist. This is an outline of many of the steps I use to remove a malware/virus. The actual steps will vary according to the virus found. A mistake could stop your computer from working or you could lose your files. Please be careful. If you are not sure what you're doing, seek professional technical assistance. [Insert a really good disclaimer here…I'm not responsible for any loss…I don't want to hear from your lawyer.] I'll be glad to refer you to a professional.

NOTE: Removing a virus, trojan, and/or spyware removal is not for the impatient. Most virus removals take a minimum of four hours. The tough ones will take ten hours and longer and will have to be done several times to remove all traces of the virus. Professional in-house computer services and on-line virus removal services prices vary greatly from $80-$400. BUT, there is no need to reformat your hard drive or completely restore your software as a first choice. If you reformat, you will lose all your files. With patience, this is something you can do! If you don't feel up to it, I will do it for you. I will normally ask $90-$120.

BEFORE you start to remove a virus, send me an e-mail with the name of the virus. I will let you know of any special tips or special removal tools you may need. These special removal tools are readily available for free from the major anti-virus manufacturers.

LAST WARNING: If you are not **SURE** what you are doing, don't do it! You could lose everything. See me or a professional before you try something you aren't sure about.

In general, to remove a virus and/or spyware, you need to do the following steps, in order:

1. Run Windows Update, to ensure you have the latest updates. Repeat until there are no more updates.

2. Open your anti-virus software and update the virus signatures. If you use Windows 7, your default anti-virus program is **Microsoft Security Essentials**. It can be downloaded at http://www.microsoft.com/security_essentials. It is free. Windows 8 and 10 uses **Windows Defender** which replaces Microsoft Security Essentials. It is built in to Windows and does not have to be downloaded. Do not run any scans yet.

3. Download and install Malwarebytes Anti-Malware. It is excellent at removing malware. A link to the download site is available free on my web site at www.suncitycomputerguy.com. Do not run any scans yet.

4. Disconnect from the internet. This is very important as malware and viruses may re-infect your computer during the removal process using the internet! You may have to disconnect from your wi-fi network, or turn off your wireless card, or unplug your LAN cable.

5. Turn off **System Restore**. Viruses can frequently hide there and can reappear after you spent hours removing them. While this step is not always necessary, I recommend it if you are going to try to remove a virus yourself.

6. Restart your computer and boot into "**Safe Mode**". For Windows 7, do this by repeatedly pressing the F8 key during the BIOS self test. For Windows 8 and 10, do this by holding down the SHIFT key while you restart the computer. Safe Mode will keep many malware and virus processes from running. It is a good first step. If Windows doesn't say "Safe Mode" when you restart, try again.

7. Next run Malwarebytes Anti-Malware using a "Threat Scan". If you find any infected files, repeat the scan a second time or more. Continue running the program until no "threats" are found. Each scan will take about 20 minutes. It could take up to an hour. Be patient. You may need to restart your computer after each scan. Follow the program's instructions.

8. Next, run the anti-virus program installed on your computer. Look for a "full computer scan" mode. The default anti-virus program installed on a Windows 10 computer is called "**Windows Defender**". Search for it in the Windows 10 Search Box. You may need to restart your computer after each scan. Follow the program's instructions.

9. If viruses, trojans, or spyware still exist, you should use a different anti-virus program and a different anti-spyware program for Steps 7 and 8 above. No program is guaranteed to get everything. You may need to use more than one. See my Anti-virus Page for several suggested alternate programs. They should eventually work. As a matter of course, I will always run a different program to check my work.

10. Only after your computer completes each scan without detecting any viruses, trojans, or spyware, should you turn "**System Restore**" back on and reconnect to the internet.

NOTE: Even after this, not all viruses and malware can be removed. If you are at this point and you still have evidence of malware or viruses, you need professional help to continue using other malware removal tools. Send me an e-mail and I will get you pointed in the right direction.

11. After removing the malware or viruses, some critical Windows files may have been removed or damaged. To fix this, open a command prompt as an Administrator and run the **Windows System File Checker**. You do this by typing **SFC /SCANNOW** from the command prompt (use an elevated command prompt in Windows 7, 8, or 10). If any files need to be fixed or replaced, Windows may ask you to place your original Windows System disk in your CD/DVD drive. Files will be automatically extracted from the CD as needed. After the **Windows System File Checker** is complete, you will be returned to a Command Prompt. Read the messages carefully if the program states that some files will be repaired on the next system restart. If so, the SFC command should be re-run after the computer restart. Type **EXIT** to return to Windows.

12. One more time, run **Windows Update** to ensure you have the latest critical security updates. Repeat until there are no more critical updates. The virus removal process may have removed some files that Windows needs.

13. If all this fails, your hard drive may have to be reformatted and Windows completely reinstalled. Bummer, but this may be the only effective solution. Be more careful opening e-mails and web sites next time and you will never need this service from me or anyone else.

WHY DO PEOPLE MAKE VIRUS', TROJANS, AND SPYWARE?

In the old days, it was a matter of conquest. Think of it as electronic graffiti, "Kilroy was Here." Some other programs wanted to steal your personal information and passwords. Now most virus', trojans, and spyware, want to put your computer to work sending thousands of spam e-mails for them. Once they infect your computer, they own it - along with thousands others - and will send out e-mails around the world advertising porn, some worthless product, or a scam of some sort. Since it looks like the e-mail is coming from you, it gives it an air of credibility. They also try to cripple your anti-virus software and disable the Windows Update program. They still can steal your personal information. They can change your computer to make it nearly impossible to remove the virus, trojan, or spyware.

Malware and viruses are **bad stuff.** You need to practice safer computing. Find out how by taking my free classes or by browsing the free help on my web site at http://www.suncitycomputerguy.com. Feel free to come to my free Computer Clinic on Thursday mornings at the Community Center.