How to Know if Your Computer is Infected

Malicious software is becoming an epidemic: it seems like it's everywhere. Also, sadly, there's been a change in the way malware acts. It used to be that it would slow down your computer or constantly display annoying popups, but it has now become even more discreet. In fact, you could be infected right now and not even have the slightest idea.

Luckily, there's a way out of this quagmire that's quicker, more thorough and much easier than any other method. **Simply follow this user-friendly 3-step guide to help render your computer malware-free.**

Note: In order to ensure that your computer is not infected, you must follow each step in order.

It often seems that the only way to check your computer for malware is to scan it using numerous anti-malware programs. This can be very time consuming and can bring your computer to a complete standstill. Even after the scan has finished, you cannot be totally sure that your computer is malware free, because scanners cannot.

A better method for checking for malware uses multiple programs, not to remove files, but to analyse the computer. Every program used in this method is very effective and simple to use. Furthermore, they will not cause your computer to slow down as they are only running when you're using them. However, they do require an internet connection to work properly. No active malware can escape detection using this process.

STEP 1: Check for Rootkits

It's important to make sure that there are no active rootkits on your computer. To do this you can first scan your computer with Kaspersky TDSSKiller (it can be downloaded from this page). While it is downloading, download the zip file Comodo Cleaning Essentials from this page.

Please make sure to select the correct version for your operating system. If you do not know whether your computer is running a 32 or 64 bit operating system then please have a look at this FAQ.

If for some reason, you are having trouble downloading these programs, or your internet connection is acting up, you should download them on another computer and transfer them to the infected one using a flash drive. As the malware may actually infect the flash drive when you plug it into your computer, it's best not to plug it into any other electrical device after using it to transfer these programs.

Kaspersky TDSSKiller will scan the computer for some of the most common types of rootkits – this program has a very high detection rate. To use it, simply open the file named TDSSKiller and then select the option "Start Scan". All in all, this scan should take less than one minute.

If it does find something, then it is highly likely that your computer is infected. However, if no rootkits are found then you should go ahead and check your computer using Comodo Cleaning Essentials (CCE).
Unzip the folder for CCE – to do this simply locate the folder, right click, click Extract All, and follow the simple instructions. Once you have done this, double click on the file named CCE – this will open the main program for CCE. If, for some reason, CCE refuses to open then hold down the shift key and, while still holding it, double click on the CCE file.

If the file successfully opens, you can let go of the shift key. Holding down the shift key kills any unnecessary processes which could be interfering with its launch. If this does not work, then download and run a program called Rkill (can be downloaded from this page). This program will terminate any malicious processes and, as a result, CCE should open fine.

When it has opened, do a smart scan with CCE. It will download all the recent virus databases (may take a while to complete). Once this download has finished, the scan will begin and your computer will be checked for all types of malware. This scan should not take too long to complete. CCE also scans for system changes which may have been caused by malware. After the scan is complete you will be asked to restart your computer. Once your computer has restarted you will be given the final results.

STEP 2: Use KillSwitch

If the aforementioned procedure did not reveal any malware activity, then you should open CCE again. However, this time, go to "Tools" and select "Open KillSwitch". KillSwitch will then begin analyzing all of your running processes. This scan should only take a few minutes at most. Without waiting for the analysis to finish you can go to "View" and select "Hide Safe Processes" – this will hide all processes that are deemed to be safe by Comodo.

Therefore, once the scan is finished, all that is left are those files which are believed to be dangerous or are not on Comodo's whitelist. The latter is denoted as FLS.Unknown. Please note that unknown does not mean that the file is dangerous – it just means it hasn't been whitelisted by Comodo yet.

If after the scan, KillSwitch shows that "There are no items to show", then your computer has passed this part of the test. However, if there are files remaining then you should investigate them.

In order to do this, you must first navigate to the files. To do this simply right click on the process in question and select "Jump to Folder". This will open up the folder where the associated file is located and will select the file as well. In order to check whether a file is indeed malicious, you can upload it to a program such as Virustotal.

STEP 3: Use Comodo Autoruns

Once again, go to the tools menu on the CCE. This time select "Open Autorun analyzer" – this program will analyze the registry and show you the files associated with each item. Since all malware writes to the registry, this program is capable of identifying malware and unknown files, even if they aren't running.

One downside to this program is that it will potentially give you more files to check than the aforementioned methods. However, if you want to be sure that your computer is 100% clean then this step is necessary.

After you open Comodo Autoruns it will immediately begin compiling a list – this process can take a few minutes to complete. Once again, without waiting for the scan to finish, you can go to "View" and select "Hide Safe Entries" so that you will have less files to look at once the scan has completed.

If Autoruns says "There are no items to show" then your computer has passed this test. If your computer has also passed the previous steps, then there is definitely no active malware on your computer.