

How to Know If Your Computer Is Infected

These days 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 display annoying popups, but now malware is becoming increasingly discreet. You could be infected right now and not even know it. Also, sadly, it often seems as if the only way to make sure you're not infected is to scan your computer with numerous anti-malware programs. Doing this can be time consuming and, while scanning, may even slow your computer to a crawl. Even after that you still can't be sure you're clean. This is because scanners cannot recognize all new malware. The only other feasible option, that I know of, is to have someone else to examine your computer. Generally this would be done online via scan logs, but this is also time consuming, and not 100% reliable.

Because of these difficulties I have come up with a better method. For this method I will use multiple programs, but not to remove files, just to analyze them. Each of these programs is very effective, but they do require an active internet connection. Each will scan, and do its job, very quickly. In fact, this process is much faster, much more certain, and much easier than any other approaches I've seen. In addition to this, if each step gives you a clean bill of health, then you can be nearly 100% certain that you're not infected. I've never seen another method that could even approach this level of certainty. However, some of the methods described here may seem very difficult, or above your level of expertise. I promise that these methods are not nearly as difficult as they seem. Some may require a little bit of effort on your part, but they are certainly doable. In fact, after doing it once, the process will be much easier to do a second time. This is very useful, as most people will want to be able to ensure that their computer is clean at all times, not just once. All of this is explained in much greater detail below.

1. Use KillSwitch

The first thing I would recommend doing is downloading **Comodo Cleaning Essentials (CCE)**.

<https://forums.comodo.com/news-announcements-feedback-cce/comodo-cleaning-essentials-23219500176-released-t79476.0.html;msg569656#msg569656>

Do not delete/disable anything with this program as it can be very dangerous if used improperly. We are only using its analytical abilities. Please do not use it to try and clean up any infections or you could inadvertently harm your computer. From the link above, just select the correct version for your operating system type. After it's finished downloading, restart your computer. When it reboots do not open any programs. Just unzip the file and open the folder. Then double click on the file called KillSwitch. This will open KillSwitch, which will immediately begin analyzing all your running processes. This analysis should only take a minute or so. The reason I asked you not to open any other programs is because malware will run on system startup whether you wanted it to or not. Many legitimate programs will not. Thus we will have fewer processes to examine.

you really want to be sure that your computer is clean then I would advise using this as well. **As before, do not delete/disable anything with this program as it can be very dangerous if used improperly. We are only using its analytical abilities. Please do not use it to try and clean up any infections or you could inadvertently harm your computer.**

To use this, double click on the file for Autoruns. It will immediately start compiling the list. This process could take a couple of minutes to complete. Once it's done it will automatically begin to analyze them. Go to "View" and select "Hide Safe Entries". Now wait until all files have been analyzed. If this is the first time you have run this program, you should now close it and then open it again. I find that this often allows Comodo time to analyze some of the unknown files so that this time there will be less to check. If Autoruns now shows that "There are no items to show", then your computer passed this part of the tests. You can move on to part 3. However, if there are still entries left over, then you should start analyzing them using the same methods described in **How To Tell If A File Is Malicious**.

<http://www.techsupportalert.com/content/how-tell-if-file-malicious.htm>

To get to the files that these entries are associated with right click on an entry and select "Jump to Folder". This will open up the folder where the associated file is located, and select the file as well. Also, you will find that often a single file has numerous entries for the same file, which means that there's not nearly as much analysis to be done as it would seem.

If your analysis shows that the file is safe, then I would recommend submitting the programs that the entries belong to Comodo for analysis using the same process described above. If you report all the safe programs, then the next time you check there should not be any unknown processes for you to examine. Thus, it becomes an incredibly easy task to ensure that your computer is still clean of infections. In fact, my computer always shows a completely blank screen, after selecting the option to "Hide Safe Entries". This allows me to ensure that my system is clean in just a few minutes.

3. Check for Rootkits

If, after following the above advice, your computer shows no signs of infection, then you are probably fine. The only thing that could have slipped past you at this point are some types of rootkits. For most people, scanning with Kaspersky TDSSKiller <http://support.kaspersky.com/faq/?qid=208283363> should be sufficient to rule out this possibility. This program will scan your computer for some of the most common types of rootkits. Also, I've found it to have relatively few false positives. **As before, I would recommend you to not delete any files using this program unless you're sure that they're malicious. A false positive on the wrong file could destroy your computer, even if you're not infected.**

To use this, download the file and unzip it. Then open the file called TDSSKiller. Next select the option to "Start Scan". This scan should take less than a minute. If it does not find any rootkit activity then your computer is almost certainly clean. However, if it does find something, then I would advise that you continue on to the next step. Only if you have reason to doubt that your

computer is clean should you feel it necessary to continue on to the next step. Using this program is more difficult than what we've been doing so far.

If you are still not confident that your computer is clean, then there is one more test that you can perform. You can perform a smart scan with CCE. This is found in the same folder as KillSwitch and Autoruns. This will scan for all types of malware, but we are specifically interested in its ability to identify rootkits. The scan should not take too long to complete. **As before, I would recommend you to not delete any files using this program unless you're sure that they're malicious.** The problem with this program is that I do find it to have many false positives. This makes the results more difficult to evaluate.

After the scan is complete it will ask you to restart your computer. **Do not remove any files with this program unless you're sure they're malicious.** Once it restarts it will pop up telling you the final results. If it did not find anything, and neither did any of the above methods, then your computer is definitely clean.

As I said above, the problem with this program is that it finds many false positives. If you cannot tell, from your results, whether the entry is an infection or not you have two options. One is to navigate to the path given by CCE, and investigate the files using the methods described in **How To Tell If A File Is Malicious**. This is not always possible, depending on how well the file is hidden.

4. Cleaning Any Infections

If these methods do show that your computer is infected, then you should check out this **Malware Removal Guide for Windows**. <http://www.selectrealsecurity.com/malware-removal-guide>

Following this advice should allow you to remove almost any infection and get your computer back to working order. Once done, you should again check, using these methods, to ensure that all infections were successfully removed.