9 things to do when detecting a computer infected with malware

Viruses everywhere! email, social networks, malicious websites and advertising popups are always potential threats. Although there are measures to prevent these threats, sometimes your computer is still infected. Here are 9 things to do when detecting that the computer is infected with malware.

Viruses everywhere like email, social networks, malicious websites and advertising popup are always potential threats. Although there are measures to prevent these threats, sometimes your computer is still infected. Here are 9 things to do when detecting that the computer is infected with malware.

How to detect a computer infected with malware:

Why do you need to know how to detect computers infected with malware while an antivirus program is available? Anti-virus programs will detect and promptly prevent threats before it causes harm. However, if the antivirus program is not updated to the latest database, it may **miss threats** . Below will be some 'symptoms' that indicate the computer is infected with malware.

1. The homepage and the search engine show signs of being hacked

Have you ever seen the default home page of a commonly used web browser redirecting to some strange website? Or does the default search engine now switch to another search engine you have never known?**These are signs that there is malware on the computer.**

2. The browser redirects itself to another website without notice

Similar to the above, another problem is that the browser takes itself to another site, potentially malicious when you click a link or type something on the site that has never happened before.

3. Popup

The browser automatically opens the continuous popup ads on the website.

4. Computer is standing

This is not a sure sign that the computer is infected with malware. But if this happens with the above symptoms it is very likely that the computer is infected.

5. A strange toolbar appears

Have you ever wondered why there is a toolbar on the browser? They are fully functional or contain only useless buttons. Almost no one uses the toolbar. But if it appears itself without notice, it may be because you regularly install free software, or it automatically installs on your computer or both.

6. The computer is slow, online or offline

The problem of connecting to the Internet is one thing, but if the computer is always running slow, whether you're online or not, this is a sign that the computer is infected with malware.

7. The browser cannot load the page

The browser still notifies you that the page is not loaded despite a good Internet connection.

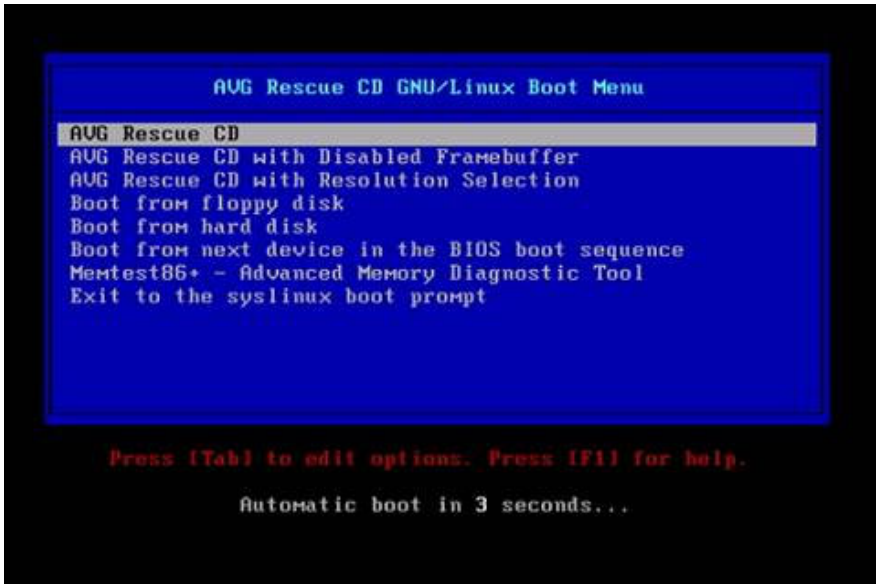
Things to do when the computer is infected with malware

1. Backup personal data

Hopefully you've ever backed up the file. But even so, you should copy individual files to another place to be safe. Secondly, you should not back up everything on your computer, because some files may be infected with malware.

2. Disconnect the Internet

The virus will automatically perform Internet connections to download additional infected files.**Disconnecting from the Internet is one of the first things you should do to reduce the performance of malware.** If you use a desktop computer, the easy way to do it is to unplug the Ethernet cable. If using a laptop, you can disconnect from the Internet by unplugging the Ethernet cable, or if you're using Wi-Fi, **just use the shortcut to turn off the connection or use the WiFi network icon in the Taskbar.**



3. Boot in Safe Mode or use a rescue disk

By booting in **Safe Mode** , you can prevent unnecessary components from starting, which prevents malware activity. To do so, restart the computer, press and hold the F8 key while the computer is booting. The first option, 'Safe Mode' should be selected, otherwise you can use the arrow keys to select other appropriate options, then press Enter. Once in Safe Mode, you can continue the malware removal process. If Windows cannot boot, you can use the antivirus rescue disk. They are mostly free and come from many companies like Kaspersky, Avira, AVG, etc. Or you can use Linux Live CD.

Reference: 10 most effective antivirus software for Windows 2017

4. Using other computers with Internet access

You should use a trusted computer and access websites to resolve malware. This is necessary because it is necessary to study the problems and symptoms infected with the malicious code. If you don't have another computer, you can talk to a trusted friend or family member. Of course, if you're studying at a college or university, or if you have access to a computer at the library, you can use a public computer to do this.

When downloading any computer program from a clean computer, you need to find a way to safely transfer them to an infected computer. It is best to use USB that contains unimportant files. You can also use SD memory card or portable hard drive for this.

5. Identify malware and find ways to remove it

Usually when malware infects a computer, it is not just a normal virus. But if it is a specific type of malicious code, it can be removed with certain procedures. There are many articles and forums that provide information to remove certain types of malware. Look for basic information about that type of malware. For example, if it is a fake antivirus program, what is its name? Once you have the information, you can search and gather what information you need to do. Ideally, you will find instructions from beginning to end to remove malware.

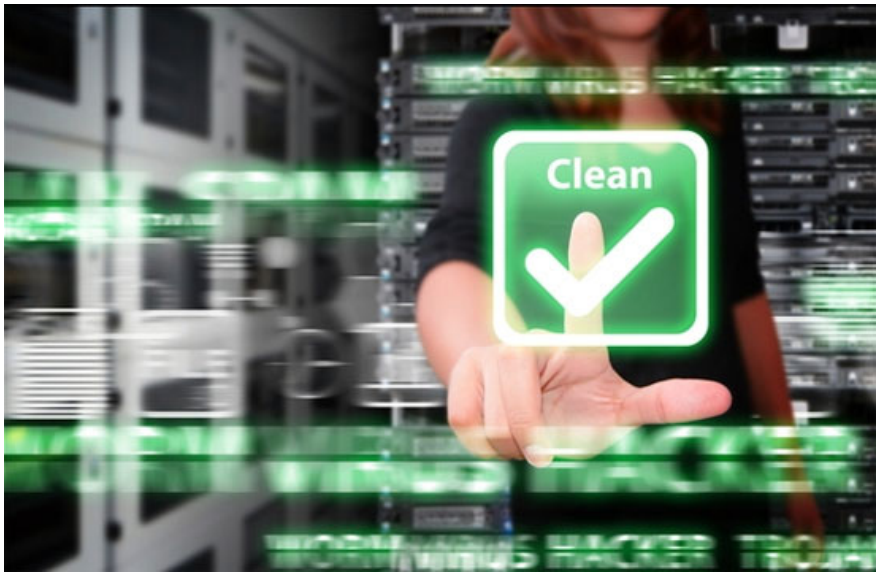
6. Scan with multiple programs until there is no malware

There are a variety of tools that can be used to remove malware. These tools range from antivirus to rootkit, adware, spyware. Some tools that users should use are Kaspersky TDSSKiller for removing rootkits. Malwarebytes Anti-Malware and HitmanPro to remove all types of malware, and AdwCleaner to remove adware. All of these tools are free and usable in combination.

1. Remove root malware (malware) on Windows 10 computers

Again, you need to download them from a clean computer with an Internet connection and transfer the files to the infected computer. Programs like Malwarebytes Anti-Malware need an Internet connection to download the latest virus database.

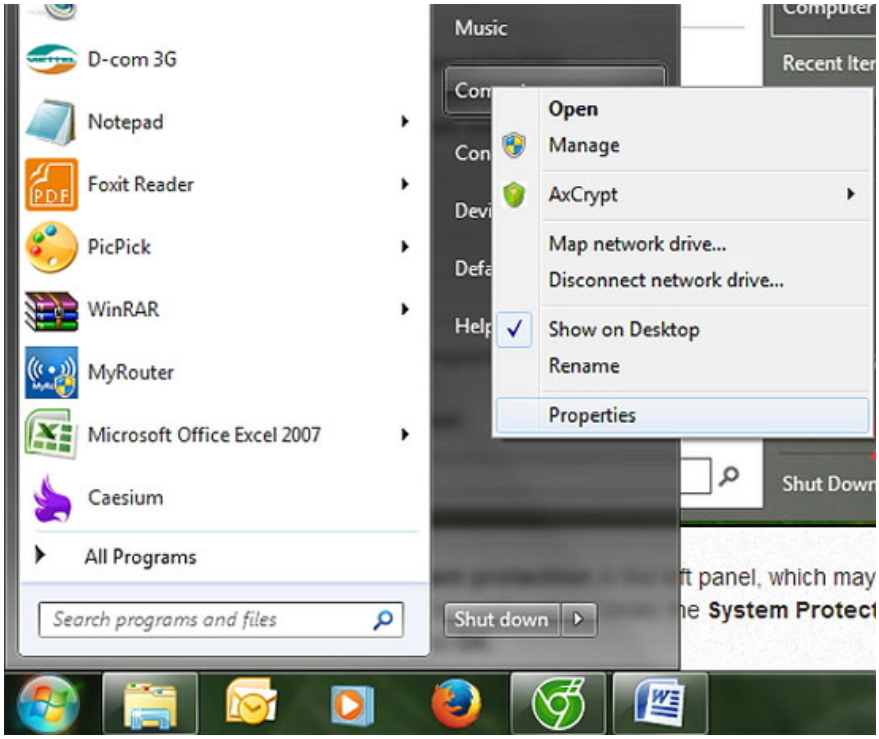
Note: although many programs may be used to remove malware, it is not possible to use multiple antivirus programs at the same time, as it may cause conflicts.



7. Delete temporary files and unnecessary programs

Once malware has been removed, now is the time to clean up the remaining files. The recommended program to do this is CCleaner. It is not considered a security program, but it can help in this process. However, CCleaner is not the only choice. Advanced SystemCare 6 Free, System Ninja, as well as DriveTidy are good alternatives.

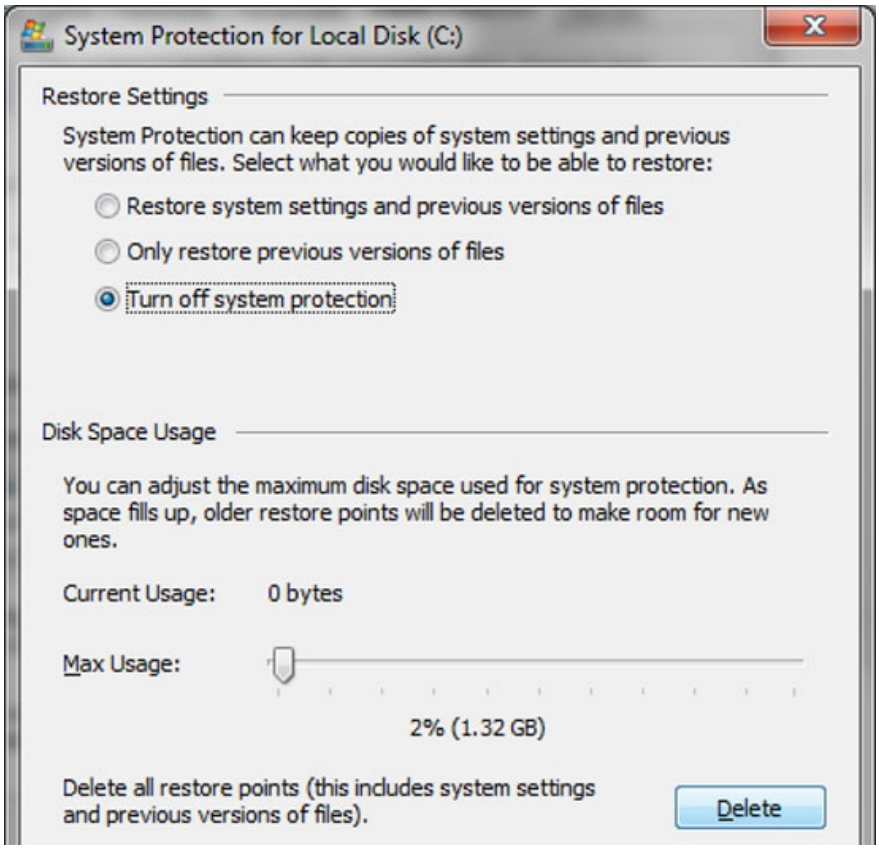
Next, review the list of installed programs to remove unnecessary or potentially risking software from sneaking into your computer by using GeekUninstaller software.



8. Remove System Restore system restore points

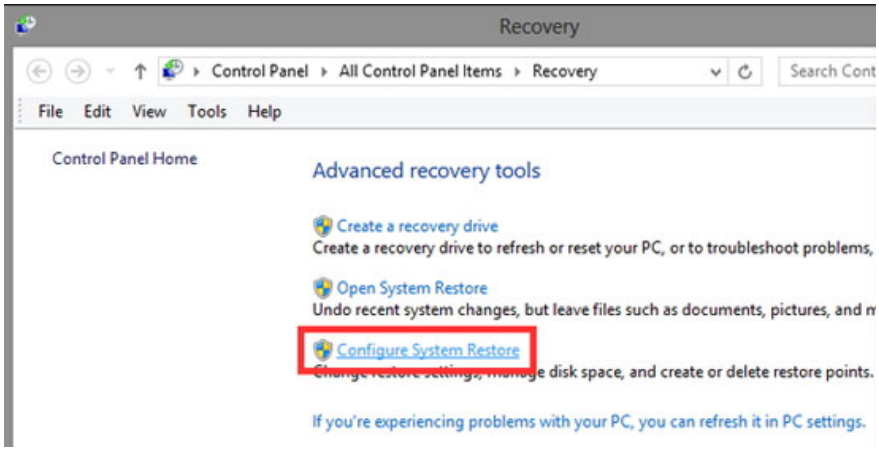
Although Windows' System Restore feature is useful, restore points are likely to contain malware, so you should delete them to make sure that the malware is removed from your computer. If you know which system restore point contains malware, remove that restore point. However, to be safe, you should remove all.

To do this in Windows Vista and Windows 7 (and Windows 8 if you have a Start Menu tool like **Classic Shell, click the Start button, right-click Computer, and then Properties.**



Click System protection in the left pane, and then you can enter an administrator password or confirm. Under **System Protection** tab, **click Configure, then press Delete and OK** .

If you're using Windows 8 and don't have the **Start Menu** tool **,** move the mouse pointer to the lower right corner to display the Charms bar. **Press Search (magnifying glass), type 'recovery' and click Settings** .



Once done, you will see the **Recovery** window. Click the **Configure System Restore link** and follow the same instructions as above.

9. Change password

Finally, you should change your password to ensure no confidential information is collected during the computer being infected with malware. If the information is collected, the malware can use it against you and cause more damage.

You should use a password management program to create and remember passwords easily and create strong passwords.

You finished reading the article "**9 things to do when detecting a computer infected with malware**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com