How Do I Know if my PC is Infected with Malware? ©

Jim McKnight www.jimopi.net AntiMalwareHDIK.lwp revised 3-19-2013

Unless the symptoms are obvious, you cannot know 100% for sure if your PC is infected or not. Here are some common Indicators of malware infections to help you decide if you need to have your PC tested or cleaned:

1. Is your PC suddenly running very slow or erratic?
2. Is your Anti-Malware program performing strangely or not at all?
3. Does "Windows Update" fail to work? *(Start > All Programs > Windows Update)*
4. Does the "Task Manager" fail to work? *(Ctrl-Alt-Del)*
5. Does "System Restore" fail to open? *(Start > Help and Support > System Restore)*
6. Browser behavior issues:
   a. Has your Browser Homepage changed by itself?
   b. When you search on-line with Google or another search engine, do your searches come up with wierd results or do the results send you to unexpected websites?
   c. Have any new Toolbars appeared in your browser?
7. Are you suddenly being barraged with pop-up ads with or without the browser running?
8. Have new Icons, files, or folders unexpectedly appeared on the Desktop?
9. Do you have missing Icons, files, or folders?
10. Has your PC started crashing, freezing, stopping with a Blue Error Screen (BSOD), or is it rebooting by itself?
11. Is your printer acting strangely or printing wrong?
12. Have unexpected messages or unexpected windows started popping up?
13. Does the hard-drive seem to be working harder all of a sudden? *(Look at the hard-drive light)*
14. Are your friends claiming that they have received e-mails from your e-mail address that were not sent by you?

If your answer to any question above is YES, your PC could be infected. If in doubt, download and run the new Microsoft Safety Scanner from: http://www.microsoft.com/security/scanner/en-us/default.aspx

Malware commonly DISABLES all your installed Anti-Malware software. When you suspect an infection, only trust freshly installed anti-malware programs. That is why I prefer ON-LINE and PORTABLE scans to see if your PC is infected. Here are some additional online/portable scanners that you can run to see if your PC is infected or not. Run these in safe-mode if necessary.

- ESET Online Scanner (Use IE only): http://www.eset.com/us/online-scanner *(Downloads & installs an ActiveX add-on for Internet Explorer. In Windows 7, IE must be "Run as Administrator")*
- SUPERAntispyware Portable (Portable Scanner for infected PC's): Download and run. http://www.superantispyware.com/onlinescan.html
- Kaspersky Virus Removal Tool: Download and run: http://www.kaspersky.com/antivirus-removal-tool?form=1
- MBAR - MalwareBytes AntiRootkit (Free): Download, open it, do the updates, and run a scan.

WARNING: Removing malware can make your PC unbootable and should be done by a professional. If you plan to attempt it yourself, I strongly suggest you make a full image backup of the entire C drive first before removing any files. *(Also see my "HOW TO REMOVE MALWARE FROM YOUR PC" guide at www.jimopi.net)*

INDIVIDUAL FILE INFECTIONS:

If you have an individual file that you think may be infected, upload it to one of these sites where they will scan it:

- Jotti: http://virusscan.jotti.org/en
- VirusTotal: http://www.virustotal.com/

VIDEO DEMO:

To see how easy it is for your PC to get infected while browsing the Internet, check out this youtube video from Carey Holzman: http://www.youtube.com/user/CareyHolzman#p/a/u/0/XL2_NaRkpLw

SAMPLE IMAGES OF FAKE ANTI-VIRUS AND SYSTEM TOOLS:

Go to Google "Images" and search with these keywords:

fake antivirus, fake system tools, or fake system repair or fake FBI virus

These are the images that pop-up and scare you into pressing OK on the window. Once you press OK, you have given the malware permission to install itself on your PC.

WARNING - IDENTITY THEFT:

Many of the current malware infections can track your online activity including e-mails and financial transactions such as online banking and stock market transactions. You must change all your on-line passwords if your PC has been infected *(After the infection is fixed)*.