Volume #4 - Issue #186
November 16th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Warning Signs That You Have Been Hacked

Malware is a malicious type of virus that spies on your computer, collects data without your knowledge, or consent, and uses that information for identity theft, or to just be a nuisance to you and your computer. Malware can appear in many ways: as a fake popup or chat field while visiting a site, secretly bundled with software downloads, or even directly embedded into your computer via hackers. Probably one of the most disconcerting issues with Malware is how your computer may be infected without your

knowledge. However, there are things you can watch for the MAY indicate trouble. Computers are complicated enough that they don't always do precisely what we expect, and sometimes an unexpected behavior is just a fluke, but, this can be an outward and visible sign of an inward and terrible malware infestation. If you notice any of these security warning signs, your system may well be compromised.

Here is a list of issues that could indicate you have Malware running in your computer:
1) Suddenly reforming poorly: If your PC is running slower than it used to, or it seems to be running an awful lot of stuff in the background, malware could be the cause.

2) A security program you never installed pops up strange warnings: Creating and distributing fake antivirus programs is a lucrative business. The hackers use drive-by downloads or other sneaky techniques to get the fake antivirus onto your system, then display scary warnings about made-up threats. Naturally you have to register a payment before the fraudulent tool will "fix" the problem.

3) Standard maintenance programs don't work: Malware will often protect itself by disabling programs that might help you identify and remove it. So if programs like Windows Update, Task Manager, your antivirus program, Regedit, System Restore, or Msconfig fail to work, you have reason to be suspicious.

4) Popup ads appear even when no browser is open: While not as common as they used to be, adware programs bombard their victims with advertisements. Sometimes they're ads for legitimate products, but usually they contain links to malicious websites, sites that will attempt to drop more malware on your PC.

5) Browser navigation gets redirected: Not every site redirect is malicious, but if you find that trying to reach Google takes you to an unfamiliar search

site, you've almost certainly got a problem. For example, a fake Trojan imitating your bank might divert your browser to a fraudulent site that looks just like your bank's real site. In that case your only clue is the unfamiliar URL in the Address bar.

6) New browser home page, new toolbars and/or your browser opens unwanted websites: Did you notice your home page has been changed and you don't seem to know why? A new toolbar seems to be placed at top of your web browser? This usually happens when you visit a website and you accidentally click an online link or a pop-up window. This action triggers the download and install of a secondary software, which is not only annoying, but also malicious.

7) Your home and search pages change: This is very much like the toolbar problem. If these pages change to something you don't want, and you change them back, but your change doesn't last, something is running that you have to stop.

8) Posts you didn't write appear on your social media pages: Malware focused on Facebook and other social media sites propagates by generating fake posts and will attempt to get your friends to click the attached links. Anyone who falls for the fake and clicks the link will become the next victim.

9) Your friends say they receive strange messages or e-mails from you: Are your friends telling you that they received suspicious e-mails from you or instant messages from your social media account containing attachments or links

10) Running out of hard drive space: You should occasionally check if your physical storage space has been increasing lately or if some of your files disappeared or changed their names. This is another sign of malware activity, since there are numerous types of malicious software which use various methods to fill up all the available space in the hard drive.

How about a Smartphone? Our business deals a lot with mobile devices and we constantly have people coming in worrying about their smartphone having malware. Smartphones operating systems are built much differently than your PC's, and thus, much harder to infect (which can also be said about Mac computers).

About the only way for smartphones to get malware is through malicious apps. If you haven't downloaded any apps recently, yet your phone is operating weird, then it's probably something else like a corrupted update. If you have downloaded new apps, check your data usage and see if it's higher than normal. The malware might be sending out information about your phone or activities. You should also check to see if there are any new apps on your gadget you didn't install; a malicious app might install other apps on its own.

Thank you for subscribing to our email!