Volume #4 - Issue #163
June 8th, 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.

Signs You Have Been Hacked

Smart hackers don't get caught. They break into your device, steal everything they can, and finish without a trace. Sometimes they leave a trail of destruction in their wake – malware, weird ads, confused relatives, and even a drained bank account or stolen identity.

Computers, phones, routers, and down to the innocent webcam are vulnerable to these hackers. So what if they've already broken in, yet you

don’t even know they’re there? Here are clear-cut signs that you've been hacked.

1. Your gadget suddenly slows down

One of the side-effects of malicious software is a slow gadget. Software gets sluggish, or constantly freezes, or even crashes. If you start noticing some of these symptoms, your gadget may very well be infected with viruses, trojans or worms. Malicious software usually runs in the background, secretly eating up your gadget's resources while it's active.

Here are tools you can use to pinpoint those nasty applications. If an application that you don't recognize is hogging your computer resources, it's likely a virus.

PC: Use Task Manager

There are a few ways to see what processes your computer is running. The easiest is to bring up Windows' built-in Task Manager. Just use the keyboard shortcut CTRL + SHIFT + ESC and go to the Processes tab. Put simply, the Task Manager lists all of your computer’s current tasks and how much processing power they’re using, measured in Central Processing Units (CPUs). Open up Task Manager and check the CPU and memory columns for each process. You might find one process is using 100 percent - or close to it - of your CPU. Open up the program associated with the process and see what it's doing. Restart the task and monitor it, but this program might be the culprit.

Mac: Use Activity Monitor

The Mac equivalent to Task Manager is its built-in Activity Monitor. The quickest way to access the Activity Monitor is by using Spotlight Search. Click the magnifying glass on the right side of the menu bar at the top of your screen, or press Command + Spacebar to open a Spotlight window and start typing the first few letters to auto-complete "Activity Monitor." Just press Enter to access the tool. Similar to Window's Task Manager, Mac's

Activity Monitor displays a list of all your open processes with tabs for CPU, Threads, Idle Wake Ups and Network usage.

If this happens when you are on an iPhone, try a soft reset by holding the power and the home button until it reboots with the Apple logo. This step can clear out frozen apps that can be hogging your memory.

2. Videos are suddenly buffer and webpages take forever to load
When a streaming video suddenly freezes, and your device appears to be “thinking,” this is called buffering. This annoyance often happens, especially if you play a lot of videos are your Wi-Fi connection is weak. If it’s happening a lot, or videos fail to play at all, you’re wise to suspect neighbors are piggy-backing on your connection. Click here for steps on how to check for Wi-Fi thieves.

Then again, malware can also slow down your internet traffic is by DNS hijacking. In short, hackers can redirect your internet traffic to unsafe servers instead of the secure servers. This will not only slow down your browsing experience; it's also a serious security risk. For example, if your router's DNS settings have been hijacked, each time you visit your online bank's website, you'll be redirected to a phishing website instead.
To check your router's DNS settings, you can use an online tool like F-Secure Router.

3. Programs and apps start crashing
Now, here is a clear sign that your system has been infected. If your antivirus software and task manager are either crashing or disabled, a nasty virus has likely taken hold of your critical system files.
You may not be able to click on once-reliable apps. In the worst case scenario, ransomware may prevent you from opening favorite files.
You can try and fix the problem by booting your gadget in Safe Mode. With Safe Mode, your computer will be running with just the bare essentials. This way, you can safely delete and uninstall any programs and files that you can't during normal operation.

Windows:
On Windows, search for System Configuration then open it >> select Boot tab then tick off Safe Boot >>check Minimal (this is enough for most cases) >> click on OK to confirm >> Restart your computer.

macOS:
On a Mac, press and hold down the Shift key while restarting your computer. Keep holding the key through the Apple logo and release when you see the login screen.

Android:
Android also has its own version of Safe Mode but there are different ways to activate it, depending on your phone model. Click here to learn how.

iOS:
Stock iOS doesn't have a Safe Mode but you can try a soft reset to fix most issues. To do this, press and hold both your iPhone's Home button and the Sleep button at the same time, wait for it to restart then let go of the buttons when the Apple logo is displayed.

The iPhone X doesn't have a Home button so the process is a bit different. Press and quickly release the volume up button, press and quickly release the volume down button then press and hold the side button and release when the Apple logo appears.

4. You start seeing pop-up ads
Malware can also add bookmarks that you don't want, website shortcuts to your home screen that you didn't create, and spammy messages that entice you to click through. Apart from slowing down your gadget and eating away at your data, these intrusive notifications can also install more malware on your system. Criminals can also use DNS hijacking to modify the ads that you see while browsing. Instead of the regular ads that you

should be getting, they can be replaced with inappropriate or malicious ones.

On Windows, clean out adware with SpyBot Search & Destroy. On a Mac, use Malwarebytes for Mac.

No one is immune to hacks, you can be extremely carefully and have the best online security available, and you will still get tricked into downloading malware. Hopefully, the above tips can help you correct the mistake and get up and running again.

Thank you for subscribing to our email!