Tell-Tale Signs that You've Been Hacked

from Ask Bob Rankin column

Sometimes the best security software in the world can't protect you from yourself. If you click on anything that moves, use trivial passwords, or download from sites that are not trustworthy, you might as well open the door and invite the bad guys in. Other times the attacks are very clever and may catch you off guard. A link in a carefully crafted "phishing" email can take you to a rogue site designed to steal your password or banking credentials.

Fake virus warning messages are almost as old as antivirus software, and they still work. When “VIRUS DETECTED! Click here to delete it NOW!” appears on-screen, people often rush to click. After all, who remembers what the real warning message of an antivirus program is supposed to look like? But when you click on the fake warning it can lead you down a rabbit hole.

Have You Been Hacked?

The super virus killer you downloaded turned out to be a Trojan Horse that enslaves your computer in a botnet, vacuums up all the sensitive account information you’ve left lying around on your hard drive, copies all your contacts, and sends the lot to some hacker in Eastern Europe.

Solution

Get familiar with your security software's warnings. Don’t follow instructions to "click and buy" or "activate" after running a scan with a hastily downloaded program.

Unexpected browser toolbars or new icons on your screen may indicate malware. Some downloads come with "foistware" that gets installed in addition to the program you're after. These sneaky extras are called PUPs (potentially unwanted programs) and may be adware, malware, or just junk you don't need. If you don’t remember deliberately installing a new program, remove it using your system’s uninstall feature and follow-up with a full anti-malware scan.

Something Is Wrong Here...

If a password you’ve typed a million times suddenly stops working, your online account may have been hacked and the password changed. This is usually caused by

weak or easily guessable passwords, but data breaches can also reveal your login credentials.

Redirected searches are another sign you've been hacked. Malware hiding on your hard drive sends your search requests to a rogue search engine instead of Google, Bing, or whatever search tool you favor. The results returned to your browser usually have little relevance to your search query; "pet meds" may return sketchy pharmaceutical sales sites.

The solution may be as *easy as checking your browser's settings to see if your default search engine has been changed*. (Settings>Apps>Default Apps). If so, change it back to your preference. If searches get redirected again, look for the "full scan or "deep scan" option in your internet security tool. When malware sneaks past your defenses, it is a sure sign that you need better protection.

If your friends start receiving spam email that appears to be from you, change your email account's password (not your username). If the problem continues, it's most likely the spammer is inserting your email address into the "from" field of spam he's sending from his own server. There's nothing you can do about that except wait.

Another red flag: Money starts trickling out of your cash and/or credit accounts, or you discover unauthorized transfers of funds. The ability to access your bank account with your smartphone is a two-edged sword. One recent story warned about a banking trojan called Octo that steals login credentials by monitoring keystrokes and initiates fraudulent transactions.

Sometimes accidental brushes against a laptop trackpad results in the cursor flying off to some odd place on the screen. But if the cursor moves on its own, opens programs and does other things that only a real person would do, either it's being controlled by malware or you have a poltergeist in your device.

What Should You Do?

Here's what to do if you think you've been hacked:

Change ALL your passwords, not just the one you think has been compromised.

If you notice any unusual activity in a financial account, contact your bank right away. Check your credit reports and consider freezing your credit files.

Do a “System Restore” on a Windows machine, rolling back your computer’s state to a time before you suspect it was hacked. Only recently installed programs will be expunged. Your documents, photos, and music will not be affected.

Run a full anti-malware scan on all of your computers.