EINPRESSWIRE

How to check if your PC has been hacked, and what to do next

DUBAI, DUBAI, UNITED ARAB EMIRATES, August 25, 2022 /EINPresswire.com/ -- Phil Muncaster, guest writer at ESET explains that even if your PC been hacked? Whatever happens, don't panic. Read on for ten signs your PC has been hacked and handy tips on how to fix it.

Global cybercriminals make trillions of dollars each year. Much of their success comes from exploiting the mistakes that we make—by clicking on phishing links, forgetting to update critical software, and failing to use multi-factor authentication (MFA). There are many attack vectors available to them, an endless supply of stolen identity data to use, and countless cybercrime sites on which to trade stolen data, tooling, and cybercrime services.

The sooner you find out about a compromise the better. The longer it goes on, the more damage the bad guys could do and the more expensive the fallout may be. So getting on the front foot with a few proactive checks makes sense. Over 847,000 businesses and consumers reported a cybercrime to the FBI last year, with incidents costing almost $7bn. Don't wait to take action until it's too late.

Ten signs your PC may have been hacked
Hackers will usually not broadcast their attacks. Staying covert is the name of the game, because the longer the victim is kept in the dark, the longer attackers have to monetize network access and online accounts.

Keep an eye on these telltale signs to spot early on if you've unwittingly become a cybercrime victim:

You get a ransomware message
Let's start with the most obvious. If you boot up the PC only to find a ransom message rather

than the usual start-up screen, there’s a very good chance you’ve become a victim of ransomware. It will typically give a short timeframe in which to pay up, along with instructions on how to pay in digital currency. The bad news is that even if you follow these to the letter, there’s a one-in-three chance you won’t regain access to those encrypted files.

A slow-running computer

When malware — including Trojans, worms, and cryptocurrency miners — are installed on a PC, they often slow the machine down. This is especially true of cryptojacking attacks, which use excessive processing power and energy to mine for digital currency. Slow-running machines can be the result of non-malicious factors, such as poor PC hygiene, but it’s best to check to see if there’s anything untoward going on.

The webcam turns on by itself

Some spyware installed by hackers is designed not only to harvest data from your PC but also secretly switch the webcam and mic on. Doing so could enable cybercriminals to record and steal video of you and your family, potentially for use in blackmail attempts. Keep an eye on the webcam light to check if it becomes operational independently. Better still, disable it completely by sticking a Band-Aid over it.

Your friends receive unsolicited messages from your accounts

Another sure-fire indicator that your PC has been compromised is if friends and contacts start complaining of spam coming from your email or social media accounts. A classic phishing tactic is to hijack victims’ accounts and then use them to spam or phish all of their friends. This is a threat that can be easily mitigated by ensuring all accounts are protected by MFA.

There are way more pop-up ads on screen

Adware typically makes the attacker money by exposing victims to excessive ad volumes. So if your machine is being flooded with pop-up advertising, it’s a good indicator that there may be some malicious code or potentially Unwanted Software installed somewhere.

New toolbars appear on the browser

Malware may also install additional toolbars on your browser. If you spot any that you don’t recognize or can’t remember downloading, it could means your PC has been hacked. It may be necessary to restore your PC back to its factory settings in order to remove them if you are facing a malware attack by an APT group. Simple PUA may not require such a drastic approach. Deleting the app and toolbar could be sufficient in this case.

Random icons start appearing

When malware is installed on a compromised PC, new desktop icons will often appear. These can be easily spotted, as long as the desktop itself is neatly arranged into a small number of files, folders and programs. Consider doing a little light tidying up in order to better keep track of the icons on your PC.

Passwords/logins stop working

If hackers have managed to compromise your PC, they may have hijacked various online accounts, such as your email, and changed the passwords in order to lock you out. Dealing with the fallout from this can be one of the most stressful parts of any cyberattack. It will require a fair amount of back-and-forth with the various online providers whose clients, partners or employees' accounts have been hijacked.

Data and logins are circulating on the dark web

If you ever receive a data breach notice from a company you do business with, always take it seriously and independently try to verify it. Sites like HaveIBeenPwned? provide third-party confirmation of any breaches. Dark web monitoring tools can also go searching for your data on cybercrime and other forums, to provide a more proactive way to stay informed. If you act quickly, by changing passwords and/or freezing credit cards, you can mitigate the risk before the bad guys have even been able to monetize an attack.

You get a warning from your security software

Warnings from anti-malware tools should also be taken seriously, although fake computer security software pop-ups are a persistent threat. Check the message is coming from your legitimate computer security software vendor and then follow the instructions to try to find and delete the malicious files on your PC. Don't assume that the warning means the security software tool will automatically purge the PC of that specific threat.

What happens next?

Whatever happens, don't panic. If your PC has been compromised, run an anti-malware tool from a reputable company to try and find and remove any malicious code from it. Then consider:

- Resetting all password to any accounts accessed from that PC
- Downloading an MFA app to mitigate further risk of account compromise
- Investing in a dark web monitoring tool to check what data has been stolen/exposed
- Setting up a credit freeze so that hackers/fraudsters can't obtain new lines of credit in your name
- Monitoring all accounts for suspicious activity, especially bank accounts

If you're not confident that the PC has been fully cleaned, consider doing password resets from an alternative device. Contact your security software vendor or bank for further advice.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here