SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for You

Am I Hacked?

Overview

Just like driving a car, sooner or later you may have an accident no matter how secure you are. Below are clues to help figure out if you have been hacked and, if so, what to do. The sooner you identify something bad has happened, the more likely you can fix the problem.

Clues You Have Been Hacked

- Your anti-virus program generates an alert that your system is infected. Make sure it is your anti-virus software generating the alert, and not a pop-up window from a website trying to fool you into calling a number or installing something else. Not sure? Open your anti-virus program.
- You get a pop-up window saying your computer has been encrypted and you have to pay a ransom to get your files back.
- Your browser is taking you to all sorts of websites that you did not want to go to.
- Your computer or applications are constantly crashing or there are icons for unknown apps or strange windows popping up.
- Your password no longer works even though you know it is correct.
- Friends ask you why you are spamming them with emails that you know you never sent.
- There are charges to your credit card or withdrawals from your bank account you never made.

How to Respond

If you suspect you have been hacked, the sooner you act the better. If the hack is work related, do not try to fix the problem yourself; instead, report it immediately. If it is a personal system or account that has been hacked, here are some steps you can take:

Change Your Passwords: This includes not only changing the passwords on your computers and mobile devices, but for your online accounts. Do not use the hacked computer to change your passwords; use a different system that you know is secure. If you have a lot of accounts, start with the most important ones first. Can't keep track of all your passwords? Use a password manager.

Financial: For issues with your credit card or any financial accounts, call your bank or credit card company right away. Use a trusted phone number to call them, such as from the back of your bank card, your financial statements, or visit their website from a trusted computer. In addition, consider putting a credit freeze on your credit files.

Anti-virus: If your anti-virus software informs you of an infected file, follow the actions it recommends. Most anti-virus software will have links you can follow to learn more about the specific infection.

Reinstalling: If you are unable to fix an infected computer or you want to be surer your system is safe, reinstall the operating system. Do not reinstall from backups; instead, backups should only be used for recovering your personal files. If you feel uncomfortable rebuilding, consider using a professional service to help you. Or, if your computer or device is old, it may be easier to purchase a new one. Finally, once you have rebuilt your system or purchased a new one, make sure it is updated and enable automatic updating whenever possible.

Backups: A key step to protecting yourself is to prepare ahead of time with regular backups. Many solutions will automatically back up your files daily or hourly. Regardless of which solution you use, periodically check that you are able to restore those files. Quite often, recovering your data backups is the only way you can recover from being hacked.

Law Enforcement: If you feel in any way threatened, report the incident to local law enforcement. If you are the victim of identity theft and are based in the United States, then visit https://www.identitytheft.gov.

Subscribe to OUCH! and receive the latest security tips in your email every month - www.sans.org/security-awareness/ouch-newsletter.

Guest Editor

Dr. Johannes Ullrich *(@johullrich) is the Dean of Research for the SANS Technology Institute, the Director of the SANS Internet Storm Center, and a SANS Fellow. He created the DShield collaborative sensor network and hosts the Internet Storm Center's daily network security news podcast.*

Resources

Backups:	https://www.sans.org/u/JGP
Passphrases:	https://www.sans.org/u/JGU
Password Managers:	https://www.sans.org/u/JGZ
What Is Malware:	https://www.sans.org/u/JH4
Credit Freeze:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/