OUCH! February 2021

SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for You

I'm Hacked. Now What?

Have I Been Hacked?

No matter how secure you are, sooner or later you may have an accident and become hacked. Below are clues you might have been hacked and if so, what to do.

Your Online Accounts

- Family or friends say they are receiving unusual messages or invites from you that you know you did not send.
- Your password to an account no longer works, even though you know the password is correct.
- You receive notifications from websites that someone has logged into your account when you know you did not log in yourself. Do not click on any links in such notifications to check your account; instead, type the website address yourself into your browser, use your previously saved bookmark, or access your account from a mobile app.

Your Computer or Mobile Device

- Your antivirus program generates an alert that your system is infected. Make sure it is your antivirus software generating the alert and not a random pop-up window from a website trying to fool you into calling a number or installing something else. Not sure? Open and check your antivirus program to confirm if your computer is truly infected.
- You get a pop-up window saying your computer has been encrypted and you have to pay a ransom to get your files back.
- Applications seem to be crashing randomly or are loading very slowly.
- While browsing the web, you are often redirected to pages you did not want to visit or new, unwanted pages appear.

Financial

- There are suspicious or unknown charges to your credit card or bank account that you know you did not make.

Now What? - How to Take Back Control

If you suspect you have been hacked, stay calm; you will get through this. If the hack is work-related, do not try to fix the problem yourself; report it immediately. If it is a personal system or account that has been hacked, here are some steps you can take:

- **Recovering Your Online Accounts:** If you still have access to your account, log in from a trusted computer that you are confident is not infected and reset your password. Once you log in, make sure to set a new, unique and strong password, the longer the better. Remember, each of your accounts should have a different password. If you can't keep track of all of them, we recommend using a password manager. Also, if it is an option, enable Multi-Factor Authentication (MFA) for your accounts, helping ensure the cyber attackers cannot get back in. If you no longer have access to your account, contact the website and inform them your account has been taken over.
- **Recovering Your Personal Computer or Device:** If your antivirus program is unable to fix an infected computer or you want to be more certain your system is safe, consider reinstalling the operating system and rebuilding the computer. This often requires erasing or replacing the disk drive and then reinstalling and updating the operating system. Do not reinstall the operating system from backups. 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 time to purchase a new one.
- **Recovering Your Financial Accounts:** For issues with your credit card or any financial accounts, call your bank or credit card company right away. Call them using a trusted phone number, such as the phone number listed on the back of your bank card, the number printed on your financial statements, or visit their website. Monitor your statements and credit reports frequently. In addition, consider putting a credit freeze on your credit files.

If you have suffered financial harm or feel in any way threatened, report the incident to local law enforcement.

Guest Editor

Maxim Deweerdt (Twitter @alfasec) is a Certified Instructor at the SANS Institute, mainly teaching Cyber Defense courses. He is also a principal consultant at NVISO, where he focuses on Threat Hunting, Incident Response and SOC maturity projects.

Resources

The Power of Updating: https://www.sans.org/security-awareness-training/resources/power-updating
Got Backups: https://www.sans.org/security-awareness-training/resources/got-backups
Making Passwords Simple: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Ransomware: https://www.sans.org/security-awareness-training/resources/ransomware
Report Identity Theft: https://www.identitytheft.gov
Credit Freezes: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/