ISSUE: January YEAR: 2019

Security Awareness Newsletter

"Technology in renewable energy has already led to many innovations in business models, products, and solutions."

LOYOLA UNIVERSITY CHICAGO

Preparing people to lead extraordinary lives

Signs of Being Hacked

Giovanni Salinas

Technology is constantly on the move, and it can be difficult to identify when one has indeed been hacked or if your equipment is simply outdated and running poorly. Cyber thieves and hackers have become more sophisticated in the methods they use to obtain personal information. For these reasons, it's imperative to understand when an individual has truly been hacked.

One clear sign that you've been hacked is if your device slows down. Malicious software is notorious slowing down your device due to consuming additional system resources. Such software could also cause an infected device to crash or perhaps freeze sporadically. If you notice these symptoms, your device may be infected with a virus, trojan, worm, or similar malware. These types of malicious software are known to run in the background, which is why your device may start to perform poorly.

Another sign that you may have been hacked is if your videos and webpages are taking an unusual amount of time to load. Hackers can install malware which can slow down your internet traffic. One example of this is called DNS hijacking. This allows hackers to simply redirect your traffic to their servers where they can obtain your information. For example, if DNS hijacking took place you might get redirected to a phishing website when attempting to access a trusted site like Facebook.

While we love surfing the web, it's vital to keep track of your online activity. Hackers are eager to gain any credentials available. With your credentials they can easily access your bank accounts, social media profiles, and other services/sites you may have access to. They may even open new accounts or take other unwanted actions using your identity. Make sure to understand your daily activity and what you browse to. If you start noticing emails and even Facebook posts that you don't recall creating, it's more than likely that you've been compromised. Be sure to regularly check your accounts (bank accounts, social media, streaming services, etc.) to ensure there is no unusual behavior.

Here are some sites that can help you to identify whether some of your accounts have been hacked:

https://haveibeenpwned.com/
https://haveibeenpwned.com/Passwords
https://breachalarm.com/

Sources

https://www.komando.com/columns/456930/7-clear-cut-signs-youve-been-hacked
https://www.forbes.com/sites/adamtanner/2014/04/14/these-sites-tell-which-of-your-accounts-have-been-hacked/#530f1f403763

University Information Security Office

Email: DataSecurity@luc.edu
Telephone: (773) 508-7373
Hours: M-F 8AM-5PM

LUC.edu/its/uiso/

How to Respond When You Are Hacked

Yuyang Zhao

If you have been hacked, had an account compromised, or even suspect something of that nature may have occurred, the first thing you should do is reset your passwords using a trusted device. We recommend starting with your email account, followed by financial and other critical accounts.

For most people, changing passwords is the first thing that comes to mind when they find out they are hacked. That is a good first step, but it may often not be enough.

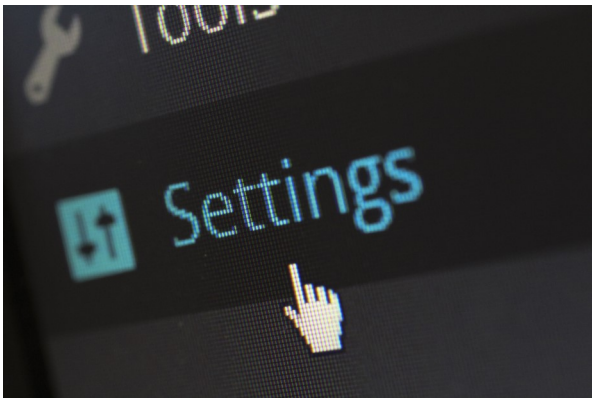
After resetting passwords using a trusted device, the next thing you should do is update and scan any devices that you suspect of being infected. Almost all malware is installed by the victims themselves, unknowingly. If malicious software has been installed on your computer, you need to get it off before you start any recovery process. Ensure you are running the latest patches available for your operating system, then run a full system scan using your main antivirus software (some antivirus software examples are available here: LUC.edu/its/uiso/resources/antivirus.shtml). One antivirus product may not catch everything, so we recommend using a second product to conduct another scan and increase the odds of complete detection.

If you already have backups of your data from before the compromise took place, reinstalling the operating system is an effective way to destroy the vast majority of infections.

Finally, it is beneficial to ask yourself why you have been hacked. Knowing why you were successfully targeted can often help you understand how to protect yourself against similar attacks in the future.

Sources

https://www.wired.com/2013/03/what-to-do-after-youve-been-hacked/
https://whatismyipaddress.com/hacked



What is Phishing

Richard Mahmud Okhai

Over the past ten years or more, phishing attacks have consistently been one of the most prevalent attack types across the globe. A large part of why this style of attack continues to be so successful is a combination of user curiosity and a lack of awareness.

A phishing attack is a process in which a cyber attacker tries to manipulate you into opening a malicious link/ attachment or take other unwanted actions. This could result in a computer virus, malware, or a lead you to a website that attempts to trick victims into disclosing sensitive information.

Are you interested in fighting this type of crime and protecting our cyberspace? You can start by getting better at detecting phishing email messages. Look out for spelling errors, poor grammar, strange URLs (e.g. zxxyzzy.loyola.weebly.com), an unprofessional writing style, and unusual requests.

We all make mistakes, and hackers put considerable effort into creating email messages that are designed to exploit that fact. By applying these basic detection techniques throughout our day-to-day work and personal lives, we can all help to defend against these types of attacks.

Sources

(Palmer, D. (2017, September 28).) Link: https://www.zdnet.com/article/watch-out-these-phishing-emails-claiming-to-be-a-secure-message-from-your-bank/