OUCH! | April 2016

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

I'm Hacked, Now What?

Overview

We know you care about protecting your computer and mobile devices and take steps to secure them. However, no matter how securely you use technology, you may eventually be hacked or "compromised." In this newsletter, you will learn how to determine if your computer or mobile device has been hacked and, if so, what you can do about it. Ultimately, the quicker you detect something is wrong and the faster you respond, the more likely you can reduce the harm a cyber attacker can cause.

Guest Editor

Samantha Davison (**@sam_e_davison**) is the Security Awareness and Education Program Manager at Uber, educating their employees in over 350 cities around the globe.

Clues You Have Been Hacked

It can be hard to determine if you have been hacked, as there is often no single way you can figure it out. Instead, hackers usually leave several clues, often called indicators. The closer your system matches any of these clues, the more likely it has been hacked:

- Your anti-virus program has triggered an alert that your system is infected, particularly if it says that it was unable to remove or quarantine the affected files.
- Your browser's homepage has unexpectedly changed or your browser is taking you to websites that you did not want to go to.
- There are new accounts on your computer or device that you did not create, or new programs running that you did not install.
- Your computer or applications are constantly crashing, there are icons for unknown apps, or strange windows keep popping up.
- A program requests your authorization to make changes to your system, though you're not actively installing or updating any of your applications.

- Your password no longer works when you try to log into your system or an online account, even though you know your password is correct.
- Friends ask you why you are spamming them with emails that you know you never sent.
- Your mobile device is causing unauthorized charges to premium SMS numbers.
- Your mobile device suddenly has unexplained very high data or battery usage.

Sooner or later, your computer or device may be compromised. The faster you detect an incident and the sooner you respond, the better.

How to Respond

If you believe your computer or device has been hacked, the sooner you respond the better. If the computer or device was provided to you by your employer or is used for work, do not try to fix the problem yourself. Not only can you cause more harm than good, but you could also destroy valuable evidence that can be used for an investigation. Instead, report the incident to your employer right away, usually by contacting your help desk, security team, or supervisor. If for some reason you cannot contact your organization, or you are concerned about a delay, disconnect your computer or device from the network and then put it in sleep, suspend, or airplane mode. Even if you are not sure if you have been hacked, it is far better to report it just in case. If the computer or device is your own for personal use, 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 all of your online accounts. Be sure you do not use the hacked computer to change the passwords. Instead, use a different computer or device that you know is secure to change the passwords.
- Anti-Virus: If your anti-virus software informs you of an infected file, you can follow the actions it recommends. This usually can include quarantining the file, cleaning the file, or deleting the file. Most anti-virus software will have links you can follow to learn more about the specific infection. When in doubt, quarantine the file. If that is not possible, then delete it.
- Rebuilding: If you are unable to fix the infection or you want to be absolutely sure your system is fixed, a more secure option is to rebuild it. For computers, follow your system manufacturer’s instructions. In most cases, this will mean using the built-in utilities to reinstall the operating system. If these utilities are missing, corrupted,

or infected, then contact your manufacturer for guidance or visit their website. Do not reinstall the operating system from backups; they may have the same vulnerabilities that allowed the hacker to originally gain access. Backups should only be used for recovering your data. For mobile devices, follow the instructions from your device manufacturer or service provider, these should be on their website. In many cases, this may be as simple as restoring your mobile device to factory default. If you feel uncomfortable with the rebuilding process, consider using a professional service to help you. Or, if your computer or device is old, it may be easier and even cheaper to purchase a new one. Finally, once you have rebuilt your computer or device (or purchased a new one) make sure it is fully updated and current and enable automatic updating whenever possible.

- Backups: The most important step you can take to protecting yourself is to prepare ahead of time with regular backups. The more often you back up, the better. Some solutions will automatically back up any new or changed files every hour. Regardless of which backup solution you use, periodically check that you are able to restore those files. Quite often, recovering your data from backup 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.

Tip of the Day

Looking for more advice on making the most of technology while staying secure online? Check out SANS Tip of the Day. A new security tip is posted every day. https://www.sans.org/tip-of-the-day

Resources

Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
What Is Malware?:	https://securingthehuman.sans.org/ouch/2016#march2016
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

License

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus