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

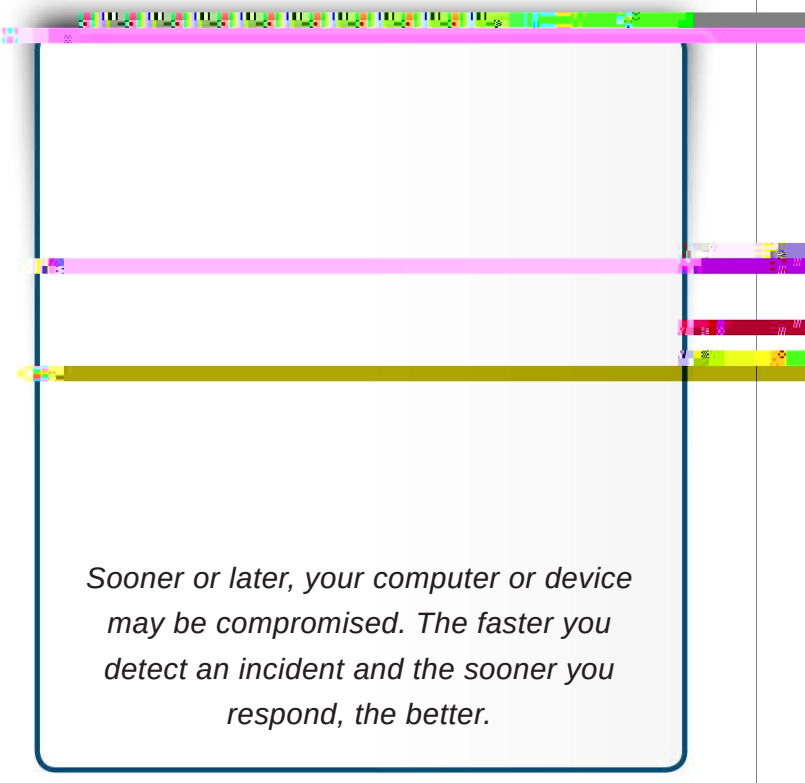
Samantha Davison (@sam_e_davison) is the Security Awareness and Education Program Manager at Uber, educating their employees in over 350 cities around the globe.

Clues You Have Been Hacked

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
- 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 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

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

being hacked.

- Law Enforcement: If you feel in any way threatened, report the incident to local law enforcement.

Tip of the Day

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
	https://securingthehuman.sans.org/ouch/2016#january2016