9 cybersecurity tips for the mildly paranoid (plus 4 for the truly anxious)

Elizabeth Weise , **USATODAY** Published 7:53 p.m. ET March 9, 2017 | **Updated 5:45 p.m. ET March 10, 2017**

(Photo: Shutterstock)

SAN FRANCISCO – So it looks as if the CIA could potentially break into most smart phone or computer networks, at least according to the stolen documents released by WikiLeaks (www.usatoday.com/story/news/nation/2017/03/07/wikileaks-says-has-published-cia-hacking-codes/98844256/) on Tuesday.

Whether you have anything to hide or not, it's a good reminder that in a digital age, keeping your life private requires some work.

Here's a list of nine things everyone should be doing already to keep their information relatively confidential, plus four more for the truly paranoid.

Don't get phished

The most common way the CIA's cyber tools, and hackers for that matter, get into your devices are via phishing emails (www.usatoday.com/story/tech/2016/12/15/how-prevent-phishing-scams/95446030/) or texts. These are created to look like they're from a friend or trusted sender (say your bank or a software company) and contain a link they try to trick you into clicking on.

Doing so loads software onto your computer, tablet or smartphone that allows the spies, or hackers, in. Once there, they can install any number of programs that allow them to spy on you and steal data. The CIA documents describe programs that can search through emails, contacts, texts and photos and send them from your device without your knowing it.

All of this is why you want to be very careful about what emails you open and what links you click. Hackers, and presumably the CIA, are very good at creating realistic-looking emails that entice you to click on dangerous links. Double and triple check before you click on links sent via email or texts. When in doubt, don't click on the link but instead go to the actual website it claims to be from.

Turn on two-factor authentication

This is that annoying step that comes after typing in your password. It sends a code to your smart phone or a landline or sometimes email. You input the code – the second factor in the authentication process — and you're good to go.

While it seems like a hassle, it's actually an extremely powerful way to keep anyone but you from getting into your accounts. They'd have to not only have stolen your ID and login but also your phone.

You should turn two-factor authentication on for every app, program and device for which it's available. It's a small hoop for you to jump through but an enormous wall for hackers, and would-be spies, to overcome.

These steps will help you stay safe online (http://www.usatoday.com/videos/tech/columnist/komando/2017/01/13/these-steps-help-you-stay-safe-online/96536108/)

Only use secure web browsers

Look for websites that use the secure version of the web protocol. You can tell by looking at the URL, which should start with HTTPS rather than simply HTTP. It stands for Hypertext Transfer Protocol Secure and keeps malicious third parties from inserting code onto the site.

Use strong passwords

There are weak passwords and then there are crazy weak passwords. According to a survey by Keeper, which makes password management software, 17% of users have 123456 as their password, followed by 123456789 and qwerty. At least put up a fight! Choose strong passwords or sign up for a password management program that will create them for you.

Password manager apps keep you safe (http://www.usatoday.com/videos/tech/personal/2014/05/22/9440051/)

Install a modern operating system

Many of the vulnerabilities detailed in the WikiLeaks documents are older and target dated systems. It's entirely possible that the CIA has newer tools for newer programs, but we don't know. What we do know is that the longer an operating system or program is around, the more vulnerabilities in it that are found and exploited. So use the most recent version of whatever operating system you prefer (Microsoft, Apple or Linux generally) and when a new one comes out, don't wait forever to switch.

Install security updates and patches

When you get a new phone or computer or install a new system, set it up to automatically update with security patches. If there's no automatic update available, check periodically to see if anything new is available.

Use a security program

There are many out there, from free to ones you pay for. While it's unlikely they'd keep the CIA out of your system, they'll do a good job of keeping run-of-the-mill hackers away, and might make it a little harder for spies to get to you.

What about Alexa?

Many have noted that Amazon's popular voice-activated digital assistant Alexa, and the Echo speaker/microphone it lives in, are not mentioned in the WikiLeak documents. That could mean that WikiLeaks simply hasn't gotten to the portion of the documents that talk about Alexa. It could also be the data dump, which seems to date mostly from 2014 and 2015, is from a time when Alexa was not really on the radar as a potential security risk.

That said, Amazon told USA TODAY that Echo's design precludes snooping (www.usatoday.com/story/tech/news/2016/03/02/voice-privacy-computers-listening-rsa-echo-siri-hey-google-cortana/81134864/). The Echo keep less than 60 seconds of recorded sound in its storage buffer (/story/tech/news/2016/03/02/how-voice-activated-devices-listen-you-and-how-turn-them-off/81187578/). As new sound is recorded, the old is erased. So there's no audio record made of what went on in a room where an Echo sits.

Use encrypted messaging software

There's no evidence the CIA was using the tools described in the WikiLeaks documents to spy on Americans, which would be illegal under U.S. law as the CIA can't operate within the United States. That said, if you really want to keep your life confidential, here are a few more things you can do.

Popular programs include Signal, Telegram and WhatsApp. The WikiLeaks documents claimed that the CIA had a program that allowed it to see what users were typing on certain phones running the Android operating system, but they hadn't been able to break the encryption of the programs themselves.

Install a camera cover on your computer and phone

This keeps anyone from being able to surreptitiously turn on your camera and use it to record you. At hacker conferences it's common to see little bits of paper taped over computer cameras, or little plastic sliding covers that allow them to close off the lens when they're not using it. It's a low-tech fix for a high-tech problem.

Use a landline

While it's relatively trivial to bug someone's phone, there are strong legal protections around doing so in the United States, including the requirement that those doing the bugging get a court order. So making a call on a land line is more secure, or at least more legally protected, than making a call on a cell phone. It also doesn't leave a digital trail as texts or email do.

A telephone from the 1940s. *(Photo: Elizabeth Weise)*

Unplug and turn off your devices

For the truly paranoid, the best way to make sure the devices that surround you aren't spying on you is to unplug them or turn them off.

Finally, think about what you're giving away for free

All of this raises a simple question — how much information do you voluntarily turn over to websites, apps and online services every day? Remember that No is always an option, though it sometimes means foregoing convenience for privacy.

CIA London

hacking

Read or Share this story: http://usat.ly/2mrjY9z