apnews.com

Turn off, turn on: Simple step can thwart top phone hackers

By ALAN SUDERMAN

6-8 minutes

RICHMOND, Va. (AP) — As a member of the secretive Senate Intelligence Committee, Sen. Angus King has reason to worry about hackers. At a briefing by security staff this year, he said he got some advice on how to help keep his cellphone secure.

Step One: Turn off phone.

Step Two: Turn it back on.

That's it. At a time of widespread digital insecurity it turns out that the oldest and simplest computer fix there is — turning a device off then back on again — can thwart hackers from stealing information from smartphones.

Regularly rebooting phones won't stop the army of cybercriminals or spy-for-hire firms that have sowed chaos and doubt about the ability to keep any information safe and private in our digital lives. But it can make even the most sophisticated hackers work harder to maintain access and steal data from a phone.

"This is all about imposing cost on these malicious actors," said Neal Ziring, technical director of the National Security Agency's cybersecurity directorate.

The NSA issued a "best practices" guide for mobile device security last year in which it recommends rebooting a phone every week as a way to stop hacking.

King, an independent from Maine, says rebooting his phone is now part of his routine.

"I'd say probably once a week, whenever I think of it," he said.

Almost always in arm's reach, rarely turned off and holding huge stores of personal and sensitive data, cellphones have become top targets for hackers looking to steal text messages, contacts and photos, as well as track users' locations and even secretly turn on their video and microphones.

"I always think of phones as like our digital soul," said Patrick Wardle, a security expert and former NSA researcher.

The number of people whose phones are hacked each year is unknowable, but evidence suggests it's significant. A recent investigation into phone hacking by a global media consortium has caused political uproars in France, India, Hungary and elsewhere after researchers found scores of journalists, human rights activists and politicians on a leaked list of what were believed to be potential targets of an Israeli hacker-for-hire company.

The advice to periodically reboot a phone reflects, in part, a change in how top hackers are gaining access to mobile devices and the rise of so-called "zero-click" exploits that work without any user interaction instead of trying to get users to open something that's secretly infected.

"There's been this evolution away from having a target click on a dodgy link," said Bill Marczak, a senior researcher at Citizen Lab, an internet civil rights watchdog at the University of Toronto.

Typically, once hackers gain access to a device or network, they look for ways to persist in the system by installing malicious software to a computer's root file system. But that's become more difficult as phone manufacturers such as Apple and Google have strong security to block malware from core operating systems, Ziring said.

"It's very difficult for an attacker to burrow into that layer in order to gain persistence," he said.

That encourages hackers to opt for "in-memory payloads" that are harder to detect and trace back to whoever sent them. Such hacks can't survive a reboot, but often don't need to since many people rarely turn their phones off.

"Adversaries came to the realization they don't need to persist," Wardle said. "If they could do a one-time pull and exfiltrate all your chat messages and your contact and your passwords, it's almost game over anyways, right?"

A robust market currently exists for hacking tools that can break into phones. Some companies like Zerodium and Crowdfence publicly offer millions of dollars for zero-click exploits.

And hacker-for-hire companies that sell mobile-device hacking services to governments and law enforcement agencies have proliferated in recent years. The most well known is the Israeli-based NSO Group, whose spyware researchers say has been used around the world to break into the phones of human rights activists, journalists, and even members of the Catholic clergy.

NSO Group is the focus of the recent exposés by a media consortium that reported the company's spyware tool Pegasus was used in 37 instances of successful or attempted phone hacks of business executives, human rights activists and others, according to The Washington Post.

The company is also being sued in the U.S. by Facebook for allegedly targeting some 1,400 users of its encrypted messaging service WhatsApp with a zero-click exploit.

NSO Group has said it only sells its spyware to “vetted government agencies” for use against terrorists and major criminals. The company did not respond to a request for comment.

The persistence of NSO’s spyware used to be a selling point of the company. Several years ago its U.S.-based subsidy pitched law enforcement agencies a phone hacking tool that would survive even a factory reset of a phone, according to documents obtained by Vice News.

But Marczak, who has tracked NSO Group’s activists closely for years, said it looks like the company first starting using zero-click exploits that forgo persistence around 2019.

He said victims in the WhatsApp case would see an incoming call for a few rings before the spyware was installed. In 2020, Marczak and Citizen Lab exposed another zero-click hack attributed to NSO Group that targeted several journalists at Al Jazeera. In that case, the hackers used Apple’s iMessage texting service.

“There was nothing that any of the targets reported seeing on their screen. So that one was both completely invisible as well as not requiring any user interaction,” Marczak said.

With such a powerful tool at their disposal, Marczak said rebooting your phone won’t do much to stop determined hackers. Once you reboot, they could simply send another zero-click.

“It’s sort of just a different model, it’s persistence through reinfection,” he said.

The NSA’s guide also acknowledges that rebooting a phone works only sometimes. The agency’s guide for mobile devices has an even simpler piece of advice to really make sure hackers aren’t secretly turning on your phone’s camera or microphone to record you: don’t carry it with you.