Top US Official, Senators Warn Americans to Use Encrypted Apps Amid Chinese Threats

'Encryption is your friend,' CISA official Jeff Greene says.

A woman uses her iPhone in a file photo. Jack Guez/AFP via Getty Images

By Jack Phillips

12/4/2024 Updated: 12/4/2024

A top U.S. cybersecurity official and two senators have advised Americans and government agencies to use encryption when messaging one another in the midst of recent Chinese cyberattacks and intrusions.

Speaking with reporters Tuesday, U.S. Cybersecurity and Infrastructure Security Agency (CISA) Executive Assistant Director for Cybersecurity Jeff Greene said Americans should know that “our advice is to avoid using plaintext.”

Share

Plaintext refers to readable data that is not encrypted, encoded, or otherwise obfuscated.

“Our suggestion, what we have told folks internally, is not new here: encryption is your friend, whether it’s on text messaging or if you have the capacity to use encrypted voice communication. Even if the adversary is able to intercept the data, if it is encrypted, it will make it impossible,” Greene told several media outlets.

Greene’s comment on encrypted calls and messaging—offered by Signal and Meta Platform’s WhatsApp—suggests that Chinese hackers could remain lurking in telecom companies’ networks for some time in the future.

When he was asked about a timeline for when Chinese hackers could be booted from U.S. telecom networks, Greene said, “It would be impossible for us to predict when we'll have full eviction.”

The warnings also come as both Democratic and Republican senators issued a letter to the Department of Defense (DOD) on Wednesday, urging the agency to investigate Chinese-led espionage attempts targeting American telecom companies. These hackers, the FBI said, stole information from private communications from “a limited number of individuals” involved in politics.

Those targeted individuals allegedly include President-elect Donald Trump, Vice President-elect JD Vance, and Senate Majority Leader

Chuck Schumer, said Sens. Ron Wyden (D-Ore.) and Eric Schmitt (R-Mo.) in their letter.

In their message to the DOD, they also sounded the alarm on the Pentagon's "continued use" of non-secure platforms such as Microsoft Teams and "unencrypted landline phones" in the agency. They also recommended encrypted platforms such as Signal, WhatsApp, and iPhone FaceTime.

Although it is not the first time senior American officials have endorsed encryption, a data-scrambling technique that helps protect communications from snoopers, it is a stark break with previous government messaging.

Only a few years ago, FBI Director Chris Wray criticized strong encryption as "an urgent public safety issue" because his bureau and other law enforcement agencies could not access devices that are encrypted.

"Let me be clear: The FBI supports information security measures, including strong encryption. But information security programs need to be thoughtfully designed so they don't undermine the lawful tools we need to keep this country safe," Wray said at an event in 2018.

Tech companies and cyber security experts have stated that measures allowing law enforcement authorities to access data from encrypted devices and programs would weaken cyber security for all users.

Greene's comments come as U.S. government agencies on Dec. 3 issued guidance for combating Chinese intrusions into U.S. telecoms. Washington has voiced increasing concern over Beijing's efforts to burrow deep into American telecommunications companies, including T-Mobile, and steal data about U.S. calls.

U.S. officials have also said that the hackers stole telephone audio intercepts, along with a large tranche of call record data. Officials have said those records mainly concerned people in the Washington area.

“The PRC-affiliated cyber activity poses a serious threat to critical infrastructure, government agencies, and businesses,” Greene said in a statement, using an acronym for the People’s Republic of China. “We urge software manufacturers to incorporate Secure by Design principles into their development lifecycle to strengthen the security posture of their customers.”

An FBI official, Bryan Vorndran, warned that “threat actors” affiliated with the Chinese communist regime “have targeted commercial telecommunications providers to compromise sensitive data and engage in cyber espionage” against U.S. companies.

Reuters contributed to this report.

Jack Phillips
Breaking News Reporter

Jack Phillips is a breaking news reporter who covers a range of topics, including politics, U.S., and health news. A father of two, Jack grew up in California's Central Valley. Follow him on X: https://twitter.com/jackphillips5

Author’s Selected Articles

UnitedHealthcare CEO Killed in Targeted Attack: 5 Things We Know

Dec 04, 2024

NATO Secretary-General Warns Trump of New Threats If Ukraine Gets Bad Deal

Dec 04, 2024

Trump Defense Nominee Pete Hegseth Says He Will Not ‘Back Down’ Amid New Allegations

Dec 04, 2024

UnitedHealthcare CEO Killed in ‘Targeted Attack’ in Manhattan, NYPD Chief Says

Dec 04, 2024

Cookies Settings