

FBI warns of ongoing scam that uses deepfake audio to impersonate government officials

The FBI is warning people to be vigilant of an ongoing malicious messaging campaign that uses AI-generated voice audio to impersonate government officials in an attempt to trick recipients into clicking on links that can infect their computers.

“Since April 2025, malicious actors have impersonated senior US officials to target individuals, many of whom are current or former senior US federal or state government officials and their contacts,” Thursday’s advisory from the bureau’s Internet Crime Complaint Center said. “If you receive a message claiming to be from a senior US official, do not assume it is authentic.”

Think you can’t be fooled? Think again.

The campaign’s creators are sending AI-generated voice messages—better known as deepfakes—along with text messages “in an effort to establish rapport before gaining access to personal accounts,” FBI officials said. Deepfakes use AI to mimic the voice and speaking characteristics of a specific individual. The differences between the authentic and simulated speakers are often indistinguishable without trained analysis. Deepfake videos work similarly.

One way to gain access to targets' devices is for the attacker to ask if the conversation can be continued on a separate messaging platform and then successfully convince the target to click on a malicious link under the guise that it will enable the alternate platform. The advisory provided no additional details about the campaign.

The advisory comes amid a rise in reports of deepfaked audio and sometimes video used in fraud and espionage campaigns. Last year, password manager LastPass warned that it had been targeted in a sophisticated phishing campaign that used a combination of email, text messages, and voice calls to trick targets into divulging their master passwords. One part of the campaign included targeting a LastPass employee with a deepfake audio call that impersonated company CEO Karim Toubba.

In a separate incident last year, a robocall campaign that encouraged New Hampshire Democrats to sit out the coming election used a deepfake of then-President Joe Biden's voice. A Democratic consultant was later indicted in connection with the calls. The telco that transmitted the spoofed robocalls also agreed to pay a \$1 million civil penalty for not authenticating the caller as required by FCC rules.

<https://arstechnica.com/security/2025/05/fbi-warns-of-ongoing-scam-that-uses-deepfake-audio-to-impersonate-government-officials/>