Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-051525-PSA
May 15, 2025

Senior US Officials Impersonated in Malicious Messaging Campaign

FBI is issuing this announcement to warn and provide mitigation tips to the public about an ongoing malicious text and voice messaging campaign. 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. If you receive a message claiming to be from a senior US official, do not assume it is authentic.

SPECIFIC CAMPAIGN DETAILS

The malicious actors have sent text messages and AI-generated voice messages — techniques known as smishing and vishing, respectively — that claim to come from a senior US official in an effort to establish rapport before gaining access to personal accounts. One way the actors gain such access is by sending targeted individuals a malicious link under the guise of transitioning to a separate messaging platform. Access to personal or official accounts operated by US officials could be used to target other government officials, or their associates and contacts, by using trusted contact information they obtain. Contact information acquired through social engineering schemes could also be used to impersonate contacts to elicit information or funds.

"Smishing" is the malicious targeting of individuals using Short Message Service (SMS) or Multimedia Message Service (MMS) text messaging. "Vishing", which may incorporate AI-generated voices, is the malicious targeting of individuals using voice memos. Both smishing and vishing use tactics similar to spear phishing, which uses email to target specific individuals or groups.

SMISHING, VISHING, AND SPEAR PHISHING ARE COMMON CRIMINAL TACTICS

Traditionally, malicious actors have leveraged smishing, vishing, and spear phishing to transition to a secondary messaging platform where the actor may present

malware or introduce hyperlinks that direct intended targets to an actor-controlled site that steals log-in information, like user names and passwords. For smishing, malicious actors typically use software to generate phone numbers that are not attributed to a specific mobile phone or subscriber to engage with a target by masquerading as an associate or family member. For vishing, malicious actors are more frequently exploiting AI-generated audio to impersonate well-known, public figures or personal relations to increase the believability of their schemes.

RECOMMENDATIONS

The following guidance can be used to identify a suspicious message and help protect yourself from this campaign.

Spotting a Fake Message

- Verify the identity of the person calling you or sending text or voice messages. Before responding, research the originating number, organization, and/or person purporting to contact you. Then independently identify a phone number for the person and call to verify their authenticity.
- Carefully examine the email address; messaging contact information, including phone numbers; URLs; and spelling used in any correspondence or communications. Scammers often use slight differences to deceive you and gain your trust. For instance, actors can incorporate publicly available photographs in text messages, use minor alterations in names and contact information, or use AI-generated voices to masquerade as a known contact.
- Look for subtle imperfections in images and videos, such as distorted hands or feet, unrealistic facial features, indistinct or irregular faces, unrealistic accessories such as glasses or jewelry, inaccurate shadows, watermarks, voice call lag time, voice matching, and unnatural movements.
- Listen closely to the tone and word choice to distinguish between a legitimate phone call or voice message from a known contact and AI-generated voice cloning, as they can sound nearly identical.
- AI-generated content has advanced to the point that it is often difficult to identify. When in doubt about the authenticity of someone wishing to communicate with you, contact your relevant security officials or the FBI for help.

How to Protect Yourself from Potential Fraud or Loss of Sensitive Information

- Never share sensitive information or an associate’s contact information with people you have met only online or over the phone. If contacted by someone you know well via a new platform or phone number, verify the new contact information through a previously confirmed platform or trusted source.
- Do not send money, gift cards, cryptocurrency, or other assets to people you do not know or have met only online or over the phone. If someone you know (or an associate of someone you know) requests that you send money or cryptocurrency, independently confirm contact information prior to taking action. Also, critically evaluate the context and plausibility of the request.

- Do not click on any links in an email or text message until you independently confirm the sender's identity.
- Be careful what you download. Never open an email attachment, click on links in messages, or download applications at the request of or from someone you have not verified.
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it. Actors may use social engineering techniques to convince you to disclose a two-factor authentication code, which allows the actor to compromise and take over accounts. Never provide a two-factor code to anyone over email, SMS/MMS text message or encrypted messaging application.
- Create a secret word or phrase with your family members to verify their identities

Victim Reporting and Additional Information

- For additional information, see FBI's guidance on Spoofing and Phishing as well as a previous Public Service Announcement about how "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud." Cybersecurity and Infrastructure Security Agency (CISA) has published the following resources "Phishing Guidance: Stopping the Attack Cycle at Phase One | CISA" and "Teach Employees to Avoid Phishing | CISA."

If you believe you have been the victim of the campaign described above, contact your relevant security officials and the FBI. The FBI requests victims report any incident to your local FBI Field Office or the Internet Crime Complaint Center (IC3) at www.ic3.gov. Be sure to include as much detailed information as possible.