NIGC Tech Alert

BOLO: MALICIOUS MESSAGING CAMPAIGN

Malicious actors employing the latest technologies to attack organizations is not a new phenomenon. Tribal cybersecurity strategies have progressed to thwart these kinds of attacks along with organizational vigilance at every level and communication across tribal nations and the United States (US). Effective application of practical cybersecurity techniques significantly reduces the number of vulnerable points of intrusion. Unfortunately, malicious actors have had significant success directing social engineering attacks like smishing, vishing and spear phishing to transition victims to an alternate messaging platform with the goal of obtaining personally identifiable information (PII) and organization data.

Be on the lookout (BOLO)! The FBI has recently issued a **Public Service Announcement warning (May 2025)**, along with recommended mitigation tips concerning malicious text (smishing) and voice messaging (vishing) campaigns. Since April 2025, attackers have successfully impersonated senior US government officials to target individuals, many of which are current or former senior US federal or state government officials and their contacts. The announcement also identifies the smishing and vishing attacks as being AI-generated techniques. 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 (ic3.gov). The FBI also offers some recommendations beneficial to every organization:

- 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.
- Carefully examine the email address; messaging contact information, including phone numbers; URLs; and spelling used in any correspondence or communications.
- 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.

Remember, no legitimate company will call or send a pop-up message to your computer requesting access. Malicious threats to Indian Country reinforce the need for extra vigilance in assuring network infrastructures is being properly maintained and monitored.

You may read the FBI Public Service Announcement, Alert Number: I-051525-PSA (May 15, 2025) at:
https://www.ic3.gov/PSA/2025/PSA250515

If you suspect you have fallen victim to a vishing, smishing or AI-generated attack, please inform the Division of Technology (DoT) using the iso@nigc.gov email address. If you have questions concerning any social engineering compromise or any other technical matter, please email ocio@nigc.gov.

July 2025