KnowBe4



KnowBe4 Scam of the Week: Deepfake, Deep Trouble

In this week's scam, cybercriminals are using artificial intelligence (AI) to try to trick you into clicking malicious links. You receive a text message or voice call from someone claiming to be a senior United States government official. They will try to establish a friendly relationship with you by sounding genuine, making the official seem trustworthy.

But these messages are fake and were actually created by AI. No matter the message you receive, the "official" will eventually ask you to use a different messaging app to continue the conversation. They will then send you a link that will supposedly take you to the new app. However, the link is actually malicious. If you click it, cybercriminals will be able to access your data and personal information!

Follow these tips to avoid falling victim to a phishing scam:

- Be suspicious when strangers try to become friends quickly through texts or calls. Scammers will often try to become friendly with you so that you will be more likely to fall for their tricks.

- Never click on links sent to you by an unknown person. These links could install malware, steal your data, or take you to fake websites designed to capture your personal information.
- This scam is based in the United States but be careful about messages from anyone claiming to be a government official, even if they act friendly. Scammers could use similar tactics anywhere in the world to try to steal your data!

The KnowBe4 Security Team