FORTRA

Terranova Security®

What are Smishing and Vishing?

Smishing and vishing are cyber crimes that use manipulative text or voice messages to steal confidential information from people. Typically, these messages are persuasive and urge victims to respond or take further action immediately.

Examples of Common Smishing and Vishing Tactics

01 FAKE LINKS

In this smishing scenario, the sender pretends to represent a real-life organization and includes a believable link in a text message. Cyber criminals will then ask users to click on the link and act, such as updating login information.

02 MALWARE ATTACK

Smishing text messages can also include a link to an executable file that installs malware on a victim's device. Trojan Horse software is often used in this type of attack to record a user's keystrokes, making it easy to steal passwords and other sensitive data.

03 PHONE PHISHING

The most common vishing attacks include fake calls from your bank to report suspicious activity, government or tax agencies, computer support teams claiming to call to fix your computer, and organizations offering you a prize or major discount.

04 WARDIALING

This vishing technique uses software to call specific area codes, using a recorded message that seemingly comes from a bank, business, or local law enforcement office. When a victim answers the call, the automated message asks them to divulge sensitive data.

05 VoIP

VoIP technology makes it very easy for cyber criminals to create fake numbers that appear to be local or ones that use a 1-800 prefix. Some numbers even spoof local organizations, like government departments or hospitals.

Who are Smishing and Vishing Targets?

Any type of business, government, organization, or individual is a social engineering target. Cyber criminals look to victimize anyone quick to believe the validity of urgent-sounding smishing and vishing messages. Cyber criminals may even use intimidating language to push users to take immediate action.