FORTRA

Terranova Security®

How to Protect Your Data from Smishing and Vishing

Smishing and vishing attacks can dupe even the most vigilant users with persuasive, convincing text and voice messages. By using impersonation and authoritative language, it can be hard to distinguish fraudulent activity from legitimate inquiries. Here's how to avoid these types of cyber threats:

1

CAREFULLY READ AND LISTEN TO ALL MESSAGES

Before responding to any suspicious text or voice message, pay attention to the language being used and think about what is being said. Be wary of senders or callers that use intimidation, threats, and an aggressive or urgent tone. Hang up and use official contact information to call back.

BEWARE OF MESSAGES FROM UNKNOWN NUMBERS

If a smishing or vishing messages originates from an unfamiliar or blocked number, be on your guard. In the case of vishing attempts, let the call go to voicemail and listen to the resulting message carefully before taking any action. Do not trust a call back number provided in the message.

2

3

LOOK OUT FOR THE USE OF MANIPULATIVE LANGUAGE

Cyber criminals who launch smishing and vishing campaigns often design messages to prey on basic human emotions like fear, greed, and trust. It's important to use good judgement and scan each message thoroughly for suspicious elements.

ASK THE SENDER QUESTIONS ABOUT THEIR REQUEST

If a sender is trying to obtain your information in exchange for a prize or commodity, ask them for verifiable proof of their identity and professional role. If the caller refuses to provide this or any other relevant information, stop replying to them.

4

5

DON'T CLICK ON UNEXPECTED LINKS OR ATTACHMENTS

As with other types of cyber threats, don't click on any unexpected links or open any attachments that come with a suspicious message. Remember, an organization will never ask you to transfer funds or divulge confidential information over the phone or an SMS conversation.

NEVER RESPOND TO REQUESTS WITH CONFIDENTIAL INFORMATION

Even if a smishing or vishing message appears to come from a bank, hospital, police department, or government office, never give up your personal information without verifying the sender's legitimacy first. Also, avoid giving out your phone number to unfamiliar email sources.

6