June 1, 2024

KaiPerm Education

What Is Smishing?

A method of identity theft that uses texts to impersonate a trusted sender to steal information. It's crucial to know what smishing looks like to avoid being deceived. Fraudsters use text messaging to impersonate a trusted organization to steal your personal information, such as your Social Security number, account usernames and passwords, bank account information or credit card numbers. Smishing texts often include malicious links the victim is encouraged to open. When the victim clicks the link, malware may be downloaded to their device or they may be directed to a login or billing screen. The scammer can then capture the victim's login credentials, financial information or personal data, which can ultimately be used for identity theft. These scams rely on creating excitement, urgency, or fear to get victims to act quickly. They may promise prizes, warn of financial or legal trouble to coerce you to act, or attempt to confuse you by sending fake invoices for products you never ordered.

How to Protect Yourself from Smishing Attacks:

- **Pause before you act -** Scammers turn up the emotional heat to pressure you to act quickly. They create urgency by insisting that time is running out, or by threatening you with consequences if you don't act now.
- **Don't respond to communication from unfamiliar senders-** If you receive a message from a sender you don't know, such as a company you don't do business with or a strange phone number, don't respond. Responding at all, even just to say "stop," tips the scammer off that your number is live, which can lead to more spam. Instead, block unwanted messages without replying.
- **Don't click any links-**Smishing texts may include links that could infect your device with malware or to lead you to enter your information into fake website that's masquerading as a trusted site.
- **Contact trusted parties directly-** If you receive a suspicious text claiming to be from a sender you believe has a legitimate reason to contact you, communicate with the organization through a known, trusted channel, such as by navigating to their website or calling them directly.
- **Keep your devices secure-** Keep your cellphone safe from hackers by keeping your software up to date. Phone operating systems such as Android and iOS regularly receive patches designed to close security holes, so neglecting to install updates can leave you vulnerable to cyberattacks. Make sure all your apps are kept up to date as well.