5/12/2023: Smishing (Text Message Phishing)

In today's world, digital scams are becoming increasingly sophisticated and more difficult to detect. Smishing (short for SMS phishing) is a type of attack that uses text messages to trick you into divulging personal or account information. While there are several variations of this scam, the most common smishing attacks impersonate legitimate companies, like popular retailers, shipping companies, and financial institutions. Ultimately these scams have three goals: getting you to click a link that downloads malware, directing you to a phishing site that will steal your information, or prompting you to call bad guys so that they can social engineer you into sending them money. Here's a breakdown of a few of those popular smishing attempts and some tips on how you can identify them:

"Did you attempt this charge?" – Scammers may send you a fake alert appearing to be from your financial institution or a popular retailer about a suspicious purchase. Usually, they'll ask you to call a number they provide to confirm. Sometimes, they'll ask you to respond "yes" or "no" to confirm the transaction before they call you directly. Once you're on the phone, they'll try to trick you into divulging your personal or financial information. Similarly, instead of asking you to verify a charge or to call a number, they might ask you to click a link they provide to verify your account details so the lock can be removed. If you click the link, you'll be taken to a phishing website that asks you to enter personal or financial information. Scammers have been known to build near replicas of legitimate websites in hopes that you'll enter your login credentials, which could grant them access to your accounts, financial information, or personal information.

"You Won!" – Scammers often use the fear of missing out (FOMO) as a popular tactic to social engineer unsuspecting consumers. You might receive a text saying that you've won a prize, but need to act quickly by clicking a link or calling a number that is provided in the message. Just like those situations listed above, messages like these almost always lead to personal or account information being compromised.

"You owe us money" – Scammers understand that most people are anxious when dealing with the IRS or other government entities and will use that to their advantage. They'll impersonate agents and text or call telling you that there's a warrant out for your arrest, or that you're eligible for government funds. In all cases, they want to social engineer you into sending them money and providing your information.

If any message creates a sense of urgency <u>and</u> includes a phone number to call, or a link to click, there's a good chance it's a scam. Do not click links or call phone numbers listed in correspondence you might receive. Doing this could lead you straight to a fraudster who is just waiting to take advantage of you. Reach out to the organization directly, using only contact information you can confirm on their official website. For larger retailers, you may be required to sign into your account and submit a support message, as they don't always list a customer support number you can call. The IRS (and other government agencies) will NEVER send you an unsolicited text asking for your personal or financial information, nor will they ask you to pay a "fee" to accept a tax refund or access other benefits.