TEXT MESSAGE SCAMS

One of the newer scams we are seeing become popular today is text messaging scamming, A.K.A. Smishing texts. These scams are very similar to email phishing scams, instead of email, the scammer attempts to trick the victim via a text message to their phone. When you get a smishing text, you will likely be asked to call a phone number or click a link to verify your bank account, email or some other form of personal information. Other messages will offer promises of cash prizes from well-known companies, but only if you click on the included link.

Here is an example of a smishing text:

"User #25384: Your Yahoo account has been compromised. Text back SENDNOW in order to reactivate your account."

What should you do if you get a smishing text? Never respond to the message, even if the text message says: "text 'stop' to stop receiving messages," never reply. Responding to the text message, even to ask the sender to stop, could possibly allow malware to install on your phone. It also lets the scammer know that your phone number is active and could lead to more smishing and spam messages.

The best way to avoid future smishing scams is to simply ignore and delete any text messages you get from numbers you don't recognize. Also be aware that some scammers can spoof their phone number to appear as though the text messages are coming from someone you might know. To be especially safe do not open any links that ask for login information, no matter who sent the message. Be skeptical if you're told to call a number, call the person back on the number you know.

Remember that no banks, legitimate businesses or government agencies – including the IRS- will ever request personal financial information via text messages (or email).

If you think you have a question or concern about smishing or have possibly fallen victim to a scam, please reach out to the SSND Help Desk at 1-800-373-7521 or email Helpdesk@ssndcp.org for assistance.