Text messaging scamming has become very popular in today's world. Also known as "Smishing", these scams are much like email phishing scams. Instead of using email, the scammer uses text messaging to trick you into disclosing personal and/or financial information. There are many ways you can protect yourself against such scams.

1. Know how to recognize smishing:

Scammers will use text messaging to try and steal your passwords, account numbers, or Social Security numbers. If they can obtain this information, they could get access to your email, bank accounts, or other personal accounts or they could sell this information to other scammers. Thousands of these smishing attacks are launched every single day and they are often successful.

Smishing text messages often tell a story to trick you into clicking on a link or opening an attachment. For example, you may receive an unexpected text message that looks like it is from a company you know or trust (like Amazon, USPS, etc.). These messages might contain things like:

- We've noticed some suspicious activity or log-in attempts
- Claim there's a problem with your account or your payment information
- You need to confirm some personal or financial information
- Include an invoice you don't recognize
- Request for you to click on a link to make a payment
- Offer a coupon for free stuff

Real companies may communicate with you via text messaging; however, they will never request for you to update personal or financial information via a link.

2. Protect yourself:

You can protect yourself from falling victim to a smishing attack by doing several things. You can make sure the software on your cell phone stays up to date by checking for updates periodically and updating when prompted to.

Protect your personal accounts by using multi-factor authentication (MFA). Some accounts will offer extra security by requiring two or more credentials to log into your account. MFA makes it harder for scammers to log in to your accounts even if they can obtain your username and password.

Protect your data by backing it up. You can use cloud services such as OneDrive or iCloud to back up data on your phone.

3. What to do if you suspect a smishing attack:

If you responded to a smishing text message and you believe a scammer has your information such as you Social Security, credit card, or bank account number, then you can go to identitytheft.gov. At this website, there will be specific steps you can take based on the information that you lost.

Again, it is important to **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.