Cell Phone Dangers this Holiday Season!

Reporting and Identifying Spam Text Messages and Phishing (SMSishing)

As the holiday season approaches, scammers will find new and creative ways to steal your personal information and wreak havoc. They have one key goal and that is to trick you into providing extremely valuable Personally Identifiable information (PII) such as passwords, birthdates, Social Security numbers, and even your pet's name.

Recently, the Federal Trade Commission (FTC) has warned on their website about how threat actors use SMSishing (Short Message Service (SMS) + phishing) to trick people into divulging information that can harm them.

Do not Fall for the Bait!

Hackers will bait and entice you. They will send text messages directly to your cell phone as their delivery mechanism. They may use the "carrot method" to dangle something desirable and reel you in just like a fish on the line. The FTC has noted ways they do this:

- Promise gift cards and free prizes
- Offer low or no interest credit cards
- Promise to help pay off your student loans

Remember this is a trap and the bad actor will not deliver on the promise.

Fear Tactics and Preying on Emotions. Do not be a Victim!

Hackers also use fear tactics because they know they are effective. They may:

- Say they are calling from your bank and notice suspicious activity. If you have a Debit card, they may try to tell you that someone is trying to fraudulently purchase something with a high dollar amount. The text message may give you a number to call. NEVER call a number you do not recognize. Once you do this, the hacker will impersonate the bank officer and attempt to steal your credentials. They may even say that you need to pay a certain amount of money to stop this transaction. Do not fall for these tactics.
- Say that they are calling from Microsoft and that they notice malware on your computer. Remember that Microsoft will NEVER call you about this. This is a bad actor impersonating a technical representative.
- Claim that there is a problem with your payment information. .
- Send you a fake invoice and ask you to contact them.
- Send you a package delivery notification.
- Fraudsters may also pretend to be government officials working for the IRS or the Social Security office. They may claim that there is fraudulent activity or that you owe money and could be arrested. If there is a real problem with your Social Security account or with the IRS, you will always receive a letter in the mail. Do not call or click on any text message link saying it is from them.

How to Protect Yourself, Friends, and Family Members

1. **NEVER** click on any link that you have not verified first or that you are not expecting.

2. **NEVER** call any number that you do not recognize. This could be falling directly into the hands of the bad actor. Once you call the number on the screen, the bad actor may try to get you to wire funds or provide valuable personal information.

3. If you make the mistake of calling, **NEVER** provide any personal information or wire funds. Also, do not download any software. Hackers impersonating Microsoft technicians often ask for their victims to download a RAT (Remote Administration Tool). This tool allows the scammer to have complete control over your computer and upload all its valuable data.

4. **ALWAYS** verify any message from your bank or financial institution by calling these numbers directly. Look up the actual phone number of your bank on the internet.

5. **AWAYS** warn friends and family members. Scammers have been known to target the elderly. It is important to warn older friends and relatives.

How to Report and Filter Out Spam Text Messages

The Federal Trade Commission (FTC) has offered some important steps you can take to filter out and report these spam text messages.

Three Ways to Report Spam Text Messages:

- Copy the message and forward it to 7726 (SPAM). This helps your wireless provider block similar messages in the future.
- Report it to the FTC at ReportFraud.ftc.gov.
- Report it on the messaging app that you currently use. Look for the option to report junk or spam.

Filter Unwanted Text Messages:

The FTC recommends filtering out unwanted text messages even before they can reach you.

- Your cell phone may have an option to filter and block spam or messages from unknown senders.
- Contact your wireless provider and find out if they have a tool that allows you to block calls and text messages.
- Call-blocking apps allow you to also block unwanted text messages. Go to ctia.org, a website for the wireless industry to learn about more options.

Remember to stay cyber safe and be especially vigilant this holiday season!