Cybercrime Prevention Flyer

Report a crime to U.S. Army Criminal Investigation Division

Cyber Field Office

27130 Telegraph Road
Quantico, Virginia 22134

Email

CFO Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

"DO WHAT HAS TO BE DONE"

CPF 0002-2022-CID361-9H **5 January 2022**

Smishing: Short Message Service Phishing

With roughly 290 million smartphone users in the United States, cybercriminals have a target-rich environment. Anyone with a smartphone, or possibly still with a landline, has likely received or is familiar with robocalls and vishing attacks, which are voice phishing to obtain personal information such as financial or credit card information. The recommended course of action has been to ignore the call or hang up and register the receiving phone number with the National Do Not Call Registry through the Federal Trade Commission or block the robocall or vishing number via the receiving smartphone.

Not a new tactic, but one increasing in popularity among cybercriminals, is smishing.

Smishing is very similar to phishing via email except the message is received on a smartphone as a Short Message Service (SMS) message, also known as a text. The message may include a link or request a reply with the cybercriminal goal to compromise the recipient's personal or financial accounts or obtain personal information to commit fraud in the recipient's name.

The smishing messages and scam topics cybercriminals can come up with are endless, similar to the number of phone numbers the cybercriminals can use and send to. Cybercriminals and scammers are relentless, but remain vigilant and take the necessary steps to avoid becoming a victim.

Common Smishing Attacks

- **Fraudulent Account Activity or Account Locked** – The recipient receives a message indicating their credit card or financial account was fraudulently used or is locked. The message, which includes a link to a site that may look like the web address to their financial institution, leads to a mimicked website requesting the recipient's personal or financial information.
- **Prize Winner** – Everyone likes to win a prize. Text messages indicating the recipient has won a prize, even when the recipient has not signed up for a contest, can be convincing. The cybercriminal's text includes a link to a legitimate looking prize website or asks the recipient to reply with personal information to collect their prize.
- **Purchase or Package Delivery Update** – A smartphone user, whether a frequent online shopper or not, receives a text with a purchase or package delivery update. The message includes a somewhat suspicious link containing the legitimate name of an online retailer or shipping company. Clicking on the link downloads malware to the smartphone, possibly compromising the device, or leads to a mimicked website requesting specific information from the message recipient.
- **IRS Scam Messages** – The new year, 2022, just began and from now until April, everyone will be filing their 2021 taxes. Cybercriminals know this and will send out IRS themed messages about

recalculating tax refunds, needing financial and other personal information to process a refund, requesting information to avoiding prosecution by the IRS, requesting information to avoid having the message recipient's social security number canceled, and a multitude of other tax themed messages to get people to respond.

Smishing Protection Tips

- If you receive a text from your financial institution, play it safe and call the financial institution on the phone number indicated on the financial institution's website. It is not uncommon for financial institutions and credit card companies to send legitimate text messages to inform their customers about fraudulent activity or to verify purchase requests.
- Do not send your credit card or financial information in a text or input in a website from a link provided in an SMS message to someone you do not know.
- Do not send your full name, date of birth, social security number, other personal information, or the information of your family members to someone you do not know or trust.
- Keep your smartphone operating system and the applications on the phone up to date.
- Do not be so quick to click on links received in text messages or to reply to a text message if the sender is unknown or the message looks questionable.
- Avoid responding to phone numbers you do not recognize.
- Avoid text messages offering quick and easy money, random coupon text messages, and text messages stating you are the next winner of the big prize.
- Most smartphones offer a way to block phone numbers. If you receive a scam message, block the number and delete the message.
- Report the scam number to you cell phone service provider.
- The IRS does not text taxpayers. The IRS contacts taxpayers through the U.S. Postal Service unless under special circumstances, which would result in a phone call.

Additional Resources

How To Recognize and Report Spam Text Messages

Mobile Phone Texts: Spam and Scams

Phishing Scams and Email Spoofing

Tips on Spotting and Reporting Spam Text Messages

5 Ways to Outsmart a Social Engineer

SMS About Bank Fraud as a Pretext for Voice Phishing

National Do Not Call Registry

To receive future CFO Cybercrime Prevention Flyers, send an email to: Subscribe CPF