Volume #4 - Issue #167
July 6th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Text Message Phishing

It seems like every time you turn around these days some hacker has come up with a new way to try and part you from your money or steal your identity. Scammers are constantly posting rogue apps on Facebook, putting malware links in Tweets, and sending you phishing e-mails, and now they've moved on to text-based phishing on your cell phone.

This new type of hack is know as Smishing. Smishing is basically phishing scams that are sent over Short Message Service (SMS) text messages.
So, you think to yourself that you surely wouldn't fall for that. But, apparently someone is falling for it, as they wouldn't be doing it if it didn't work some of the time.
Most Phishing Scams Play on Your Fear of Things Such as:
– Fear of someone stealing your money
– Fear of being accused of a crime that you did not commit
– Fear of someone doing harm to you or your family
– Fear of something embarrassing being revealed about you (whether it is true or not)
We are all human. When we are confronted by fear, we may throw logic and reason out the window and might end up falling for a scam even though we thought we were "too smart" to be fooled by such a thing. A lot of phishing attacks which end up being successful likely go unreported because the victims don't want people to think they were gullible enough to get conned. Phishers refine their scams over time learning which ones work, and which don't.
If you get a text that fits into one of the fear categories above, be extra skeptical. If it is threatening in any way to your or your family members, report it to the local authorities and also to the Internet Crime Complaint Center.
Given the short nature of SMS messages, phishers have a very limited canvas on which to work so they have to be extra creative in a smishing attack.
One of the most prevalent current texting scams involves fake bank texts. Many banks don't send text messages because they don't want people to fall for smishing attacks. If they do have an option to send send text alerts find out what number they use to generate them so you will know if they are legitimate. However, the scammers may use spoofed alias numbers that

look like they are from your bank, so you should still be skeptical and not reply directly. Contact your bank at their regular customer service number to see if the text was legit or not instead of responding directly to the text message.

Here are some general tips to prevent falling victim to a smishing scam.

1) Avoid clicking links within text messages, especially if they are sent from someone you don't know. But, be aware that attack messages can appear to come from someone you do know, so think before you click.

2) Don't respond to text messages that request private or financial information from you.

3) As stated above, If you get a message that appears to be from your bank, financial institution, or other entity that you do business with, contact that business directly to determine if they sent you a legitimate request.

4) Beware of messages that have a number that says it is from "5000" or some other number that is not a cell number. Scammers often mask their identity by using email-to-text services to avoid revealing their actual phone number.

5) If a text message is urging you to act or respond quickly, stop and think about it. Remember that criminals use this as a tactic to get you to do what they want.

6) Never reply to a suspicious text message without doing your research and verifying the source. If your bank is really going to cancel your credit card, you should be able to call the number on the back of your card to discuss this matter with them.

7) Never call a phone number from an unknown texter.

8) Use Your Cell Providers Text Alias Feature. Almost all major cell providers allow you to setup an Text Alias that you can use to receive texts. The texts still come to your phone and you can send texts, but anyone you text sees your alias instead of your actual number. You can then block

incoming texts from your real number and give all your friends and family the alias you are using.

9) Enable the "block texts from the internet" feature if available from your cell provider. Most spammers and smishers send texts via an internet text relay service which helps hide their identity and also doesn't count against their text allowance (scammers are notoriously frugal). Many cell providers will let you turn on a feature that will block texts that come in from the internet.

Expect SMiShing to become more prominent in the coming year. The statistics are in the criminals' favor, and it's up to cellphone users to be smart about their behavior.

Thank you for subscribing to our email!