OUCH! | July 2020

SANS SECURITY AWARENESS

Messaging / Smishing Attacks

Overview

One of the most common ways cyber attackers attempt to trick or fool people is by scamming you in email attacks (often called phishing) or try to trick you with phone calls. However, as technology continues to advance bad guys are always trying new methods, to include tricking you with messaging technologies such as text messaging, iMessage/Facetime, WhatsApp, Slack or Skype. Here are some simple steps to protect yourself and spot / stop these common attacks.

What Are Messaging Attacks?

Messaging attacks (sometimes called Smishing, a play on the word Phishing) are when cyber attackers use SMS, texting or messaging technologies to reach out to you and try to trick you into taking an action you should not take. Perhaps they want to fool you into clicking on a malicious link, or get you to call a phone number so they can get your banking information. Just like in traditional phishing email attacks, bad guys often play on your emotions to act. However, what makes messaging attacks so dangerous is that they often feel far more informal or personal than email, making it more likely you may fall victim. In addition, with messaging attacks there is less information and fewer clues for you to pick up on that something is wrong or suspicious. When you receive a message that seems odd or suspicious, start by asking yourself does this message make sense, why am I receiving it? Here are some of the most common clues of an attack.

- A tremendous sense of urgency, when someone is attempting to rush you into taking an action.
- Is this message asking for personal information, passwords or other sensitive information they should not have access to?
- Does the message sound too good to be true? No you did not win the lottery, especially one you never entered.

A message that appears to come from a co-worker or friend's account or phone number, but the wording does not sound like them. Their account may have been compromised and taken over by an attacker, or the attacker is attempting to pretend to be them, tricking you into taking an action.

If you get a message that makes you have a strong reaction, wait a moment and give yourself a chance to calm yourself and think it through before you respond.

Sometimes bad guys will even combine email and messaging attacks. For example, gift card scams can work this way. A cyber attacker will send you an urgent email pretending to be a friend or co-worker, then ask for your cell phone number. Then they can send repeated text messages, pressuring you to purchase gift cards. Once purchased, the attackers have you scratch off the code on the back of the cards and message a picture of the codes back to them. Another common attack urges you to "check out" a video or picture ("you won't believe this!"). It appeals to your sense of curiosity. If the message looks like it is from someone you know, perhaps call the person on the phone to verify before you act.

If you get a message from an official organization that alarms you, check with them directly. For example, if you get a text message from your bank saying there is a problem with your bank account or credit card, contact your bank or credit card company directly by visiting their website or calling them directly using the phone number from the back of your bank card or credit card. Bear in mind that most government agencies, such as tax or law enforcement agencies, won't contact you via text message.

When it comes to messaging attacks, you are your own best defense.

Subscribe to OUCH! and receive the latest security tips in your email every month - sans.org/ouch.

Do you think you've got what it takes to get into the cyber security industry? Or are you looking to improve your existing skillset? Training with SANS helps you achieve your goals. Level Up with SANS today! sans.org/Level-Up-Ouch

Guest Editor

Jen Fox *holds the DEF CON 23 black badge for Social Engineering and provides security awareness education as a Security Program Specialist at Domino's. You can follow her on Twitter as @j_fox.*

Resources

Social Engineering:	http://www.sans.org/u/XAQ
Stop That Phish:	http://www.sans.org/u/XAV
Phone Call Scams:	http://www.sans.org/u/XB0
Reporting fraudulent text messages:	https://www.consumer.ftc.gov/articles/0350-text-message-spam