OUCH! January 2022

SANS SECURITY AWARENESS

OUCH!

The Monthly Security Awareness Newsletter for You

Spot and Stop Messaging Attacks

What are messaging attacks?

Smishing (a portmanteau word combining SMS and phishing) are attacks that occur when cyber attackers use SMS, texting, or similar messaging technologies to trick you into taking an action you should not take. Perhaps they fool you into providing your credit card details, get you to call a phone number to get your banking information, or convince you to fill out an online survey to harvest your personal information. Just like in email phishing attacks, cyber criminals often play on your emotions to get you to act by creating a sense of urgency or curiosity, for example. However, what makes messaging attacks so dangerous is there is far less information and fewer clues in a text than there is in an email, making it much harder for you to detect that something is wrong.

A common scam is a message telling you that you won an iPhone, and you only need to click on a link and fill out a survey to claim it. In reality, there is no phone and the survey is designed to harvest your personal information. Another example would be a message stating that a package could not be delivered with a link to a website where you are asked to provide information needed to complete delivery, including your credit card details to cover "service charges." In some cases, these sites may even ask you to install an unauthorized mobile app that infects and takes over your device.

Sometimes cyber criminals will even combine phone and messaging attacks. For example, you may get an urgent text message from your bank asking if you authorized an odd payment. The message asks you to reply YES or NO to confirm the payment. If you respond, the cybercriminal now knows you are willing to engage and will call you pretending to be the bank's fraud department. They will then try to talk you out of your financial and credit card information, or even your bank account's login and password.

Spotting and Stopping Messaging Attacks

Here are some questions to ask yourself to spot the most common clues of a messaging attack:

- Does the message create a tremendous sense of urgency attempting to rush or pressure you into taking an action?
- Is the message taking you to websites that ask for your personal information, credit card, passwords, or other sensitive information they should not have access to?

- Does the message sound too good to be true? No, you did not really win a new iPhone for free.
- Does the linked website or service force you to pay using non-standard methods such as Bitcoin, gift cards or Western Union transfers?
- Does the message ask you for the multi-factor authentication code that was sent to your phone or generated by your banking app?
- Does the message look like the equivalent of a "wrong number?" If so, do not respond to it or attempt to contact the sender; just delete it.

If you get a message from an official organization that alarms you, call the organization back directly. Don't use the phone number included in the message, use a trusted phone number instead. For example, if you get a text message from your bank saying there is a problem with your account or credit card, get a trusted phone number on your bank's website, a billing statement, or from the back of your bank or credit card. Also remember that most government agencies, such as tax or law enforcement agencies, will never contact you via text message, they will only contact you by old fashioned mail.

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

Guest Editor

Jeff Lomas is a Detective for Las Vegas Metropolitan Police Department's Cyber Investigative Group and teaches SANS SEC487 Open-Source Intelligence Gathering and Analysis (OSINT) course. Jeff investigates high-tech financial crimes including Business Email Compromises, smishing, ransomware, and complex cryptocurrency theft and money laundering cases.

Resources

Stop That Phish: https://www.sans.org/newsletters/ouch/stop-that-phish/
Social Engineering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Vishing: Phone Call Attacks: https://www.sans.org/newsletters/ouch/vishing/