OUCH! July 2024

OUCH!

The Monthly Security Awareness Newsletter for You

SANS SECURITY AWARENESS

Text Messaging Attacks: A Smishing Saga

Mark was perplexed by the text message, a package delivery notification from Amazon - "Delivery attempt missed! Click the link now to reschedule or your package will be returned." Mark could not remember ordering anything online recently, but to be honest, he ordered so many things online it was easy to forget. Not wanting to miss any packages, he clicked the link, and a page loaded asking for his contact information "to ensure proper rescheduling." The message seemed a bit odd, but Mark figured better safe than sorry. He entered his home address details and was then asked for additional information, including his credit card information. Trusting the company, he entered everything it asked to ensure delivery. The page then said his package should be delivered soon. Then, within fifteen minutes Mark received a phone call from his credit card company notifying him that his card was being used to make numerous online charges from all over the world. Mark froze as he realized that there was no package and that the text message had been a scam to trick him out of all his information, including his credit card.

What Are Messaging Attacks (Smishing)

Messaging attacks, also called Smishing (a combination of the words SMS and Phishing), occur when cyber attackers use SMS, texting, or similar messaging technologies to trick you into taking an action you should not take, such as giving up your credit card or bank account password or installing a fake mobile app. Just like in email phishing attacks, cyber criminals often play on your emotions, such as creating a sense of urgency or curiosity. However, what makes messaging attacks so dangerous is that 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.

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

Spotting and Stopping Smishing Attacks

Here are some of the most common clues of a messaging attack:

- **Urgency**: Any message that creates a tremendous sense of urgency, when someone is attempting to rush or pressure you into taking an action, such as claiming your accounts will be closed or you will go to jail.
- **Greed**: Does the message sound too good to be true? No, you did not really win a new iPhone for free.
- **Curiosity**: If you get a message that looks like the equivalent of a “wrong number,” or someone you do not know just saying “hi”, do not respond to it or attempt to contact the sender; just delete it. These are attempts by cyber criminals to start a conversation with you, such as romance scams.
- **Personal Info**: Is the message taking you to websites asking for your personal information, credit card, passwords, or other sensitive information they should not have access to?
- **Payments**: Be very suspicious of unusual payment requests, like sending money through Western Union or Bitcoin.

If you get a text message from an official organization that you believe may be legitimate, call the organization back directly. However, don’t use the phone number included in the message, instead use a trusted phone number. 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 by visiting your bank’s website, find the phone number on a billing statement or from the back of your bank or credit card, then call using that number. 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 message-based Smishing attacks, you are your own best defense.

Guest Editor

Destiney Plaza is a Cybersecurity Engineer at Carnegie Mellon University’s Software Engineering Institute. She loves to inspire by giving talks to a diversity of audiences ranging from beginners to cybersecurity professionals. She holds a CISSP, BS in computer science, and MS in management information systems.

Resources

Messaging Do’s and Dont’s: https://www.sans.org/newsletters/ouch/messaging-dos-and-donts/
Stop Phone Calls Scams: https://www.sans.org/newsletters/ouch/stop-phone-call-scams/
Emotional Triggers – How Cyber Attacks Trick You: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/