OUCH! | September 2019

OUCH!

SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for You

Scamming You Through Social Media

Overview

Many of us have received phishing email, either at work or home. These emails look legitimate, such as from your bank, your boss, or your favorite online store, but are really an attack, attempting to pressure or trick you into taking an action you should not take, such as opening an infected email attachment, sharing your password, or transferring money. The challenge is, the more savvy we become at spotting and stopping these email attacks, the more cyber criminals try other ways of contacting and scamming us.

Attempts to scam or fool you can happen over almost any form of communication you use—from Skype, WhatsApp, and Slack to Twitter, Facebook, Snapchat, Instagram, and even gaming apps. Communication over these platforms or channels can feel more informal or trustworthy, which is precisely why attackers are using them to fool others. In addition, with today's technologies, it has become much easier for any attacker anywhere in the world to pretend to be anything or anyone they want. It is important to remember that any communications that come your way might not be what they seem and that people are not always who they appear to be.

Key Takeaways

Here are the most common clues that a message you just received or a post you just read may be an attack:

Urgency: The message has a sense of urgency that demands "immediate action" before something bad happens, like threatening to close your account or send you to jail. The attacker wants to rush you into making a mistake.

Pressure: The message pressures you to bypass or ignore policies or procedures at work.

Curiosity: The message invokes a strong sense of curiosity or promises something that is too good to be true. No, you did not just win the lottery.

Sensitive: The message includes a request for highly sensitive information, such as your credit card number or password, or any information that you're just not comfortable sharing.

Official: The message says it comes from an official organization, but has poor grammar or spelling. Most government organizations will not use social media for official communications directly with you. If you are not sure if the message is legitimate, call the organization back, but use a trusted phone number, such as one from their website.

Impersonation: You receive a message from a friend or co-worker, but the tone or wording just does not sound like them. If you are suspicious, call the sender on the phone to verify they sent the message. It is easy for a cyber attacker to create messages that appear to be from someone you know. In some cases, they can take over one of your friend's accounts and then pretend to be your friend and reach out to you. Be particularly aware of text messages, Twitter, and other short message formats, where it is more difficult to get a sense of the sender's personality.

You are the best defense against scams, cons, and attacks like these. If a post or message seems odd or suspicious, simply ignore or delete it. If it is from someone you personally know, call the person on the phone to confirm if they really sent it.

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

Dr. Jessica Barker *(@drjessicabarker) is a leader in the human side of cybersecurity. She is co-CEO of Cygenta, where she follows her passion of positively influencing cybersecurity awareness, behaviors, and culture around the world. She is also the Chair of ClubCISO and is a popular keynote speaker.*

Resources

Social Engineering:	https://www.sans.org/u/Uz6
Phone Call Scams:	https://www.sans.org/u/Uzb
Stop That Phish:	https://www.sans.org/u/Uzg
Personalized Scams:	https://www.sans.org/u/Uzl