OUCH! November 2020

The Monthly Security Awareness Newsletter for You

Social Engineering Attacks

Overview

A common misconception about cyber attackers is that they use only highly advanced tools and techniques to hack into peoples' computers or accounts. Cyber attackers have learned that the easiest ways to steal your information, hack your accounts, or infect your systems is by simply tricking you into doing it for them using a technique called social engineering. Let's learn how these attacks work and what you can do to protect yourself.

What is Social Engineering

Social engineering is a psychological attack where an attacker tricks you into doing something you should not do through various manipulation techniques. Think of scammers or con artists; it is the same idea. However, today's technology makes it much easier for any attacker from anywhere in the world, to pretend to be anything or anyone they want, and target anyone around the world, including you. Let's take a look at two real-world examples:

You receive a phone call from someone claiming to be from the government informing you that your taxes are overdue and that if you do not pay them right away you will be fined or arrested. They then pressure you to pay over the phone with a credit card, gift card, or wire transfer warning you that if you don't pay you could go to jail. The caller is not really from the government, but an attacker attempting to trick you into giving them money.

Another example is an email attack called phishing. This is when attackers create an email that attempts to trick you into taking an action, such as opening an infected email attachment, clicking on a malicious link, or giving up sensitive information. Sometimes phishing emails are generic and easy to spot, such as pretending to come from a bank. Other times phishing emails can be highly customized and targeted as attackers research their targets first, such as a phishing email pretending to come from your boss or colleague.

Keep in mind, social engineering attacks like these are not limited to phone calls or email; they can happen in any form including text message, over social media, or even in person. The key is to know what clues to look out for.

Common Clues of a Social Engineering Attack

Fortunately, common sense is your best defense. If something seems suspicious or does not feel right, it may be an attack. The most common clues include:

- A tremendous sense of urgency or crisis. The attackers are attempting to rush you into making a mistake. The greater the sense of urgency, the more likely it is an attack.
- Pressure to bypass or ignore security policies or procedures you are expected to follow at work.
- Requests for sensitive information they should not have access to or should already know, such as your account numbers.
- An email or message from a friend or coworker that you know, but the message does not sound like them - perhaps the wording is odd or the signature is not right.
- An email that appears to be from a coworker or legitimate company, but the email is sent using a personal email address such as @gmail.com.
- Playing on your curiosity or something too good to be true. For example, you are notified your package was delayed, even though you never ordered a package or that you've won a prize in a contest that you never entered.

If you suspect someone is trying to trick or fool you, do not communicate with the person anymore. Remember, common sense is your best defense.

Guest Editor

Christian Nicholson (@GuardianCosmos) is a SANS instructor for SANS SEC560 and SANS SEC504, as well as Partner/Cyber Lead at Indelible (https://indelible.global). Christian specializes in Application Security, Purple Teaming, and Automation for secure integration, programming and engineering.

Resources

Phone Call Attacks: https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams
Stop That Phish: https://www.sans.org/security-awareness-training/resources/stop-phish
CEO Fraud / BEC: https://www.sans.org/security-awareness-training/resources/ceo-fraudbec
Personalized Scams: https://www.sans.org/security-awareness-training/resources/personalized-scams