Defending Against Social Engineering Attacks

Insights
4.13.17

The term "social engineering" used to conjure up images of social scientists with Ph.D's brainstorming ways to improve race relations or provide lower income groups with greater access to education and employment opportunities. Today, however, the term is more frequently associated with the use of technology and basic principles of human nature to trick individuals into divulging confidential or personal information that may be used for fraudulent purposes. The social engineering techniques employed by these modern day con artists may be the biggest threat to your Company's confidential and proprietary information.

Phishing, Vishing and Smishing

Three of the most common types of social engineering scams involve the use of "spoof" communications via email, telephone, or text messaging. In a typical phishing scam, the victim receives an email which appears to be a legitimate email from a known and trusted sender and which tries to get the victim to reply and provide information they should not be distributing. One phishing scam involved an email which looked like it was coming from the Company CEO and directed the employee to wire transfer funds to a particular account. The employee, thinking he was just doing his job at the CEO's request, complied, only to find out later that the email had been a fake.

Another variation on phishing is the use of ransomware. In this scam, the perpetrator sends an attachment with an intriguing yet innocuous title such as "urgent account info" with a file extension of ".PDF.zip" or ".PDF.rar." The malware launches a covert attack which often encrypts the entire hard disk or the documents and demands a bitcoin payment to unlock.

When this type of scam is perpetrated by telephone, it is called "vishing." In one vishing scam directed at consumers, the victim receives a robocall from someone who says: "Oh, I'm sorry, *I'm adjusting my headset* right now. Can you hear me now?" The normal human response would be to say "yes" - -which is exactly what the scammer wants. The audible "yes" is recorded and the scammer then tries to use the recorded response to authorize unwanted charges on the victim's utility or credit card account. This particular scam has been used so much that on March 27, 2017, the Federal Communications Commission (FCC) issued an alert warning consumers to be on the lookout for it and to just hang up when the call is received.

When this type of attack is perpetrated by the use of text messaging, it is called smishing. A smishing attack often occurs because your phone number was entrusted to the wrong person on the

internet. The attacker often sends a text message with a link hoping you click it, and when you do, the link installs spyware and or malware on your device. Smishing is growing more popular as it has proven to be an effective way of gaining access to an individual's data.

Social Engineering Attacks Are Just The Beginning

Social engineering attacks are usually not isolated events, but part of a larger scheme to develop pathways to even more information. Cybercriminals are adept at extracting bits and pieces of information and combining them to worm their way even deeper into a Company or to steal a person's financial identity.

Defending Against Social Media Threats

According to a 2015 study by Intel Security, internal actors were responsible for 43% of data loss -- half of which was intentional and half accidental. In addition to technological defenses, Companies must train their employees on how to spot and avoid social engineering attacks. At a minimum, Companies should conduct a bi-annual training geared towards each user group (end-users, IT staff, managers, etc.) so that everyone is aware of the latest attacks. It is also helpful to engage a third party to conduct a social engineering test of your employees to see if they are steering clear or taking the bait.

The following are a few clues to help spot phishing emails:

- Poor spelling and grammar
- Unexpected or out of place message
- Attempting to elicit some sort of emotion, positive or negative
- Unfamiliar sender
- Unfamiliar URL

The following are good general rules that employees should follow to help avoid falling victim to social media attacks:

- Employees should not open attachments in emails of unknown origin
- Employees should not respond to unsolicited communications (email/phone) without verifying the identity of the person on the other side
- Be wary of emails that request confirmation of personal or financial information with high urgency
- Change password access at least every few months and at unpredictable times

Companies spend a lot of time and money on the installation of sophisticated technological barriers against unauthorized users gaining access to their data -- and well they should. However, it is just

against unauthorized users gaining access to their data - -and well they should. However, it is just as important to address the human risk factor when designing your risk management plan. Strengthening your computer systems against technical intrusion has little value if the employees who have access to them are vulnerable to social engineering attacks. By training employees to identify and avoid these types of scams, you can establish a "human firewall" sufficient to retard the efforts of would be thieves.