SOCIAL ENGINEERING

WHAT IS SOCIAL ENGINEERING?

Social Engineering is a cyberattack that uses human interactions to gain access to systems and networks for financial gain. It uses manipulation of normal security precautions. This is usually an attackers first step, with their end goal of harming a system with malware.

TYPES OF SOCIAL ENGINEERING

PHISHING

Phishing is the most well-known and common social engineering attack. According to Verizon, in 2021, nearly 40% of breaches featured phishing. Phishing is the process of sending fraudulent emails or text message that look like legitimate emails from a trustworthy sender. The goal is to steal important information like credit card numbers or login information. The emails or text messages often have links that installs malware or trick the end-user into sending important information.

BAITING

When baiting, an attacker leaves a physical device, like a USB flash drive, in a place that is likely to be found. If the target is curious, the user inserts it into their computer and malware is then installed.

WHALING

Where a phishing victim is relatively random, whaling targets high-profile employees, like a CFO or CEO. The end-goal is for the high-profile employee to send sensitive information like approving large amounts of money to be wire transferred.

SCAREWARE

Scareware tricks a user into believing their device was infected with malware or that they have downloaded illegal content. The attacker gives the user a "solution" to fix the malware or downloaded attack. However, the "solution" is the real malware.

CLONE PHISHING

A legitimate email message is copied, then altered and sent from a trusted organization, and replaced with a link redirecting to a malicious website.

SPEAR PHISHING

Emails that directly target a specific organization or person using tailored information.

MASS CAMPAIGN

A wide net phishing scam is sent to the masses from a knock-off corporate entity asking them to enter their credentials or credit card details.

VISHING

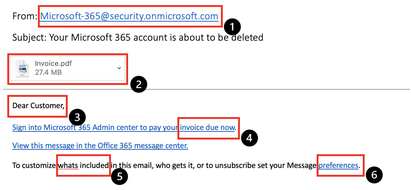
The end goal of Vishing ("Voice Phishing") is similar to the types of social engineering mentioned above but it uses the phone to steal financial and personal data. Most people have received these types of calls – often the messages will say suspicious activity has taken place in the victim's bank account, credit card account, or other financial services.

SECURITY CONCERNS

Humans are usually the weakest link in your security strategy and can expose vulnerabilities for these reasons:

- ❑ Poor decisions resulting from heavy workloads
- ❑ Distractions associated with working from home
- ❑ Insufficient knowledge of red flags to look for
- ❑ The forgetting curve, which is just as steep as the learning curve

HOW TO SPOT A SOCIAL ENGINEERING EMAIL



1. Check domain and email address: A part of the email may be legitimate, but the last part might have a variant like a letter, number, or look odd from the usual domain.
2. Don't click on attachments: if you aren't expecting an attachment or an attachment looks suspicious because it has a strange name, it might be malware or ransomware, which are frequently deployed through phishing.
3. Watch for overly generic greetings: cyber criminals will send a large batch of emails. Look for examples like, "dear valued customers."
4. Look for urgency: claiming a action is urgent, offering a special or insisting a company must make a payment before services are cut off. Examples like "You've won! Click here to redeem prize!" or "We have your browser history, pay now or we're telling your boss."
5. Look at grammar or formatting: beware of misspelling, bad grammar, odd phrasing, or weird color or font that don't match. This may be an attempt at bypassing spam filters.
6. Use caution with links: mouse over the link to see if the destination match where the email implies you will be taken or if it is the company's actual domain.

90% OF ALL INCIDENTS THAT END IN A DATA BREACH START WITH A PHISHING EMAIL

67% INCREASE IN THE FREQUENCY OF BUSINESS EMAIL COMPROMISED ATTACKS FROM 2019 TO 2020

WHY YOU SHOULD TRAIN YOUR EMPLOYEES

- ❑ Clear standards help employees provide good customer service
- ❑ The more knowledgeable your employees are, the better you can serve customers
- ❑ Investment in training strengthens the human firewall, aka your employees
- ❑ Spending on training yields a high return on investment. Preventing even a single social engineering attempt can save your company thousands
- ❑ Lower likelihood of falling for phishing scams
- ❑ Ability to address policy violations quickly

EMAIL SECURITY AWARENESS TRAINING

Social engineering is one of the most common attacks employees encounter. Luckily, regular security awareness training empowers employees to spot and stop fake emails and reduces your business's chance of experiencing a damaging cyberattack.

HawkPoint offers a training platform/learning management system that allows a member of your business to design training courses and then deploy them to other team members. Send fake emails to employees that are designed to see if they will click on bad links. If they fail, they're given training videos, courses and quizzes to learn more about email security and social engineering.

SECURITY AWARENESS TRAINING CAN REDUCE THE IMPACT OF A CYBERATTACK BY OVER **70%**

57% OF BUSINESSES SEE WEEKLY OR DAILY PHISHING ATTEMPTS

HAWKPOINT TECHNOLOGIES