bank
prov.

Security Tips: Social Engineering

Social Engineers are hackers who exploit the one weakness that is found in every organization: the human. Using a variety of tools, including phone calls, social media, email and devices, these engineers trick people into offering them access to sensitive information.

three common attack types.

Phishing: Phishing scams are the most common type of social engineering attacks used today. Phishing attempts are performed to obtain personal information, such as, name, address, social security number, or account number. Often, shorter or embedded links that appear legitimate are used to redirect a user to a malicious website. At times, threats or a sense of urgency may be used to manipulate the user into action on the request.

Some phishing emails are poorly written, oftentimes exhibiting spelling and grammar errors, but are still capable of directing victims to a fake website or forms where they can steal user login credentials and other personal information.

Pretexting: With pretexting, attackers focus on creating a good angle, fabricating a realistic scenario, that they can use to steal personal information. These types of attacks commonly take the form of a scammer who pretends that they need certain bits of information from their target in order to confirm their identity. Advanced attacks will also try to manipulate their targets into performing an action that enables them to exploit the structural weaknesses of an organization. Unlike phishing emails, pretexting relies on building a false sense of trust with the victim, requiring the attacker to build a believable situation that leaves little room for doubt.

Baiting: Baiting is very similar to a phishing attack. What differentiates it from other types of social engineering is the promise of an item or information – fictitious things the hackers use to entice the victim. Baiting attacks are not restricted to online schemes, either. Attacks can also include the exploitation of human curiosity by utilizing physical media such as USB's.

best practices.

Stopping attacks like those listed above is simpler than you think – common sense is your best defense. If something seems suspicious or does not feel right, it may be an attack. The most common red flags of a social engineering attack include the following:

- Someone creates a sense of urgency, trying to get you to respond quick and make a mistake.
- Someone asks for information they should not have access to or should already know.
- Someone asks for your password – no legitimate company will ever ask you for that.
- Someone pressures you to bypass or ignore security procedures or protocols.
- Someone promises something that is too good to be true (money or valuable goods).
- A friend or co-worker send you an email, but it appears suspicious or odd, not typical of that person. Reach out to that person through another means to confirm whether the email was in fact valid or malicious before replying or interacting with it at all.