This Week's Tip: Social Engineering - Staying Alert for Subtle Scams

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick people into making security mistakes or giving away sensitive information.

Say you receive an email, and the urgent tone makes you feel that you should ignore a security warning and open an attachment. This is one example of how an attacker might use social engineering to manipulate you into installing malicious software (malware).

Another common approach is to build familiarity and trust. An attacker may research an organization's routines, processes, and cultural norms to establish credibility. Then, they may be able to persuade an employee to transfer money to the scammer's account instead of a legitimate account.

An Attacker's Arsenal

A successful social engineering attack often involves a combination of tactics. Here are some common examples:

- Phishing emails and texts – Fraudulent emails and text messages can entice, trick, or scare a person into clicking malicious links or providing confidential information.

- Researching targets online – Scammers use social networks to gather personal details and may try to impersonate a legitimate connection online.

- Voice phishing (vishing) – Phone calls provide direct access for scammers to ask for confidential information.

- In-person deception – Scammers may visit their target locations, often using a false identity. They might pretend to be a vendor or contractor, a job applicant, or an employee.

- Tailgating – A scammer may try to follow another person through a secure entrance. They may pretend to have lost their badge and ask you to hold the door for them.

- Shoulder surfing – Scammers can steal passwords, access codes, PINs, and other important information just by observing you. A scammer typically tries to watch a user log into a system to learn their credentials, using a camera, software, or their own eyes.

Developing Your Own Skills

Social engineering comes in many different forms and can be performed anywhere human interaction is involved. The following tips can help you identify these types of attacks:

- Verify that people are who they claim to be, in person, via email, and over the phone.

- Trust your instincts—if something seems odd, check with your IT support staff.

- Protect passwords and other sensitive data.

- Never hold open secure doors for people you do not know.

If you have any questions, please contact Information Security via Mark.Nagiel@SupremeLending.com. Thanks for participating in the Information Security effort!