UBI
A COMMUNITY
FEDERAL CREDIT UNION

Social engineering is a method of manipulating individuals into divulging confidential or sensitive information, performing certain actions, or making decisions that they wouldn't typically do. It's a non-technical approach to hacking that exploits human psychology and behavior rather than relying on computer code or vulnerabilities. Social engineering attacks typically aim to exploit trust, authority, fear, or other emotions to deceive individuals.

Here are some common techniques and examples of social engineering:

1. **Phishing:** This involves sending fraudulent emails or messages that appear to come from a legitimate source, such as a credit union/bank or a trusted organization. The goal is to trick recipients into clicking on malicious links, downloading malware, or providing personal information like login credentials or credit card details.
2. **Pretexting:** In pretexting, attackers create a fabricated scenario or pretext to obtain information. For instance, someone might impersonate a co-worker or a utility company representative over the phone to extract sensitive data.
3. **Baiting:** This tactic involves enticing victims with something appealing, like a free software download or a tempting link. When the victim takes the bait, they unwittingly compromise their security.
4. **Quid Pro Quo:** Attackers offer something of value in exchange for information or access. For example, someone may claim to be an IT support agent offering to fix a computer issue remotely while gaining access to the victim's system.
5. **Tailgating:** In a physical setting, a social engineer might follow an authorized person into a secure area, relying on their presence and trustworthiness to gain unauthorized access.
6. **Impersonation:** Attackers may impersonate legitimate personnel, like a delivery person, technician, or a company executive to gain physical or digital access to a target.
7. **Reverse Social Engineering:** This technique involves convincing the target that they need the social engineer's help. The attacker may pretend to be a security expert who needs the target's assistance to thwart a security threat.

Social engineering attacks can be highly effective because they exploit human tendencies like trust, helpfulness, or curiosity. To defend against social engineering, it's essential to be cautious and verify the legitimacy of requests for sensitive information, especially when they come unexpectedly. Education and awareness training are also crucial in recognizing and thwarting social engineering attempts.

Remember, UBI Federal Credit Union is local and here for you! Please let us know what we can do to help with your banking and financial needs! 860-747-4152 or find us at www.UBIFCU.com