Social Engineering Attacks

Social engineering is the art of one human attempting to coerce or deceive another human into doing something or divulging information. We do this all the time in our day-to-day lives. Children social engineer their parents into giving permission or providing something they want. As a spouse, you may social engineer your partner into doing a chore you're responsible for. Criminals and hustlers are no different: They use social engineering tactics to get humans to divulge information about themselves or someone else. This is key in order to obtain private data to perfect identity theft. Hackers also attempt to social engineer targeted employees into divulging information about IT systems or applications so that the hackers can gain access.

Hackers and perpetrators use many different tactics to attempt to social engineer their victims. Here is a summary of social engineering attacks that may be used on you or your organization:

Authority—Using a position of authority to coerce or persuade an individual to divulge information.

Consensus/social proof—Using a position that "everyone else has been doing it" as proof that it is okay or acceptable to do.

Dumpster diving—Finding unshredded pieces of paper that may contain sensitive data or private data for identity theft.

Familiarity/liking—Interacting with the victim in a frequent way that creates a comfort and familiarity and liking for an individual (e.g., a delivery person may become familiar to office workers over time) that might encourage the victim to want to help the familiar person.

Hoaxes—Creating a con or a false perception in order to get an individual to do something or divulge information.

Impersonation—Pretending to be someone else (e.g., an IT help desk support person, a delivery person, a bank representative).

Intimidation—Using force to extort or pressure an individual into doing something or divulging information.

Scarcity—Pressuring another individual into doing something or divulging information for fear of not having something or losing access to something.

Shoulder surfing—Looking over the shoulder of a person typing into a computer screen.

Tailgating—Following an individual closely enough to sneak past a secure door or access area.

Trust—Building a human trust bond over time and then using that trust to get the individual to do something or divulge information.

Urgency—Using urgency or an emergency stress situation to get someone to do something or divulge information (e.g., claiming that there's a fire in the hallway might get the front desk security guard to leave her desk).

Vishing—Performing a phishing attack by telephone in order to elicit personal information; using verbal coercion and persuasion ("sweet talking") the individual under attack.

Whaling—Targeting the executive user or most valuable employees, otherwise considered the "whale" or "big fish" (often called *spear phishing*).