FORTRA

Terranova Security®

Co-sponsored by Microsoft

What Is Social Engineering?

Social engineering is a manipulation technique used to trick victims into following malicious instructions. Social engineering relies on the basic human instinct of trust and, because of this, can be hard to defend against. Cyber criminals hope to catch victims off-guard and gain access to systems or sensitive organizational data, such as login credentials and personal information.

Examples of Common Social Engineering Tactics

01 PHISHING

Encompassing deceitful email, websites, text messages, and more, cyber criminals use phishing campaigns to steal confidential personal and organizational information. Often, hackers will hide behind email senders or websites that are familiar to the intended victim.

02 BAITING

Baiting is both an online and in-person social engineering tactic that relies on the human desire for reward. The attacker will promise the victim something tantalizing, like a prize, in exchange for their immediate action.

03 WATER-HOLING

Water-holing targets a group of users and websites they normally visit. Security vulnerabilities are exploited to infect those websites with malware, which in turn will affect one or several members of the targeted group.

04 PRETEXTING

Pretexting leverages a false identity to trick the victim into giving up confidential information. A common example is when cyber criminals impersonate a customer service representative for a known company where a user recently made a purchase.

05 QUID PRO QUO

Quid pro quo social engineering scams hinge on an exchange of a reward or information that convinces a victim to act. A common technique is for a criminal to contact an employee, claiming to be an IT support employee and urging them to confirm login credentials.

Who Could Be a Social Engineering Target?

Any type of business, government, organization, or individual could be a social engineering target. Cyber criminals look to victimize anyone who isn't alert to the presence of a cyber threat. It's not uncommon for people to become repeat victims of social engineering attacks due to busy schedules, complacency, or forgetfulness.