Innovation Growth Partners Specialty®

CONTACT US

Dave Perkins, RPLU
(508) 848-4263
dave.perkins@igpspecialty.com

Types of Social Engineering Attacks

Social engineering attacks manipulate people into divulging information or taking actions that compromise security, and common types include Phishing (email-based), Vishing (voice-based), and Smishing (text-based), which are often escalated into Spear Phishing and Whaling when targeting specific individuals. Other tactics include Pretexting (creating a believable story), Baiting (offering incentives), Scareware (using fake warnings), Quid Pro Quo (trading favors for information), and physical intrusions like Tailgating.

Here are some common types of social engineering attacks.

Remote/Digital Attacks

Phishing
Attackers use fraudulent emails, messages, or websites to trick victims into revealing sensitive information, like passwords or credit card numbers.

Spear Phishing
A more targeted form of phishing that uses personalized information to make the attack seem legitimate and highly relevant to the specific victim.

Whaling
A highly targeted form of phishing that specifically targets high-level executives, such as CEOs, for high-value information or financial gain.

Vishing (Voice Phishing)
Involves using phone calls to manipulate victims, often by impersonating banks or other authorities.

Smishing (SMS Phishing)
Uses text messages (SMS) to send malicious links or prompts, often appearing as urgent notifications or prize claims.

Baiting
Entices victims with a promise of something desirable, like a free download or prize, to trick them into a malicious act.

Pretexting
Involves creating a believable false scenario or backstory to gain the victim's trust and elicit sensitive information.

Quid Pro Quo
Offers something in return for a requested action or piece of information, such as pretending to be tech support to get a user to download malware.

Scareware
Uses pop-up warnings or other alarming messages to trick users into visiting malicious websites or purchasing useless software.

Physical/In-Person Attacks

Tailgating/Piggybacking
An attacker follows a legitimate employee to gain unauthorized access to a restricted area, often by pretending to have forgotten their access card.

Baiting (Physical)
Involves leaving infected devices, such as USB drives, in public places, enticing a curious victim to plug it into a computer.

©2026 Innovation Growth Partners Specialty, LLC | igpspecialty.com