Glossary of Social Engineering Attacks (A-Z)

This glossary provides definitions for various social engineering attacks, categorized alphabetically for ease of reference.

- **Baiting:** Leaving a tempting target (e.g., infected USB drive) to lure victims into taking a harmful action, like inserting it into their device.

- **Bird Dogging:** Following a target physically (e.g., tailgating) to gain unauthorized access to a secure location.

- **CEO Fraud:** Impersonating a high-level executive (CEO, CFO) via email or phone to trick employees into sending money or confidential information.

- **Deception Technologies:** Utilizing honeypots, decoy systems, and other virtual traps to lure and identify attackers.

- **Deepfake:** A manipulated video or audio recording that appears authentic, often used to impersonate someone for social engineering purposes.

- **DDoS Attack (Distributed Denial-of-Service):** Overwhelming a website or server with traffic to render it inaccessible to legitimate users. (Social engineering tactics may be used to initiate a DDoS attack).

- **Eavesdropping:** Spying on a conversation or electronic transmission to steal confidential information.

- **Gift Card Scam:** Pretending to be customer support or a legitimate company and tricking victims into purchasing gift cards for fraudulent purposes.

- **Impersonation:** Posing as a trusted entity (e.g., bank, tech support) to gain a victim's trust and steal personal information or money.

- **Phishing:** Sending emails or SMS messages (smishing) disguised as legitimate communications to trick victims into revealing sensitive information or clicking malicious links.

- **Pharming:** Deceptive websites designed to mimic legitimate ones to steal login credentials or financial information.

- **Pretexting:** Fabricating a scenario or story (pretext) to gain a victim's trust and obtain confidential information.

- **Quid Pro Quo Scam:** Offering something desirable (quid) in exchange for a victim's personal information or financial details (quo).

- **Romance Scam:** Building an online relationship with a victim to gain their trust and eventually exploit them emotionally or financially.

- **Shoulder Surfing:** Stealing sensitive information (e.g., passwords) by observing someone typing it on a keyboard.

- **Smishing:** Sending phishing text messages (SMS) to trick victims into revealing personal information or clicking malicious links.

- **Social Engineering:** The manipulation of human emotions, psychology, and trust to trick victims into taking actions or revealing confidential information that can be used for malicious purposes.

- **Spear Phishing:** A targeted phishing attack directed at a specific individual or organization.

- **Tailgating:** Following closely behind an authorized person to gain unauthorized access to a secure location.

- **Vishing:** Phishing attempts carried out over the phone, where attackers impersonate legitimate entities to trick victims into revealing sensitive information.

- **Watering Hole Attack:** Targeting websites frequented by a specific group (e.g., vendors) to infect devices that visit the compromised site.

- **Whaling:** Targeting high-profile individuals (CEOs, executives) with sophisticated social engineering attacks.

  Note: *This is not an exhaustive list, and new social engineering tactics are constantly emerging. Staying informed about these evolving threats is crucial for maintaining a strong defense.*