


























## 40+ Social Engineering Attack Types

#	Type	Description
<b>I. Digital / Online Attacks</b>		
1	Phishing	Fraudulent emails or messages to trick victims into revealing sensitive information or clicking malicious links
2	Spear Phishing	Highly targeted phishing attacks customized for specific individuals or organizations
3	SMS Phishing (Smishing)	Phishing via text messages to steal information or install malware
4	Mobile Phone Phishing	Phishing via mobile phone apps or messages
5	Vishing	Voice phishing via phone calls or voicemails to deceive victims
6	VoIP Phishing	Phishing via Voice over IP (VoIP) calls
7	Video Phishing	Sending fraudulent video messages to deceive victims
8	Browser Phishing	Creating fraudulent websites that mimic legitimate ones to steal information
9	Pop-Up Windows	Fake pop-ups claiming to be security alerts to trick users into taking harmful actions
10	Watering Hole Attack	Compromising websites frequently visited by targets to infect them with malware
11	Baiting	Offering something enticing to lure victims into a trap, often using malware-infected media
12	DNS Poisoning	Redirecting website traffic to malicious sites by manipulating DNS records
13	Spamming	Sending unsolicited bulk messages, often containing malicious content
14	Keystroke Logging	Using software or hardware to record keystrokes and steal sensitive information
15	Clipboard Data Theft	Exploiting clipboard vulnerabilities to steal copied data
16	Credential Harvesting	Collecting user credentials through deceptive means, often via phishing attacks or fake websites

17	 Business Email Compromise (BEC)	An email-based scam where a cybercriminal poses as a trusted partner to trick employees into transferring money or sensitive data
18	 Impersonation of Executives (Whaling)	A targeted phishing attack focused on high-profile individuals, where attackers pose as executives to gain sensitive information or funds
19	 Email Account Compromise (EAC)	A sophisticated attack where cybercriminals gain unauthorized access to legitimate email accounts using tactics like password spraying, phishing, or malware, allowing them to impersonate the victim and manipulate email communications
20	 Spim	Spam sent over instant messaging platforms
21	 Quishing	Phishing attacks that use QR codes to direct victims to malicious websites or download malware
<b>II. Social Media and Communication-based Attacks</b>		
22	 Reverse Social Engineering	Manipulating a situation so the victim initiates contact and offers information voluntarily
23	 Psychological Manipulation	Exploiting cognitive biases and emotions to influence victim behavior
24	 Pretexting	Creating a fabricated scenario to manipulate victims into divulging information or performing actions
25	 Quid Pro Quo	Offering a service or benefit in exchange for sensitive information or access
26	 Hoax Calls	Making false emergency or crisis calls to manipulate individuals or organizations
27	 TOAD (Telephone Oriented Attack Delivery)	A sophisticated vishing technique that uses automation to make a large number of calls, often employing social engineering tactics to manipulate victims over the phone
<b>III. Physical and In-Person Attacks</b>		
28	 Impersonation	Posing as a trusted entity to gain unauthorized access or information
29	 Impersonating Authorities	Posing as law enforcement or officials to manipulate victims
30	 Impersonating Support Staff	Posing as tech support or customer service to gain trust and access
31	 Tailgating	Following an authorized person into a restricted area without proper credentials

32	 Piggybacking	Gaining unauthorized entry by closely following an authorized person through a secure entrance
33	 Shoulder Surfing	Observing or recording sensitive information by looking over someone's shoulder
34	 Eavesdropping	Secretly listening to private conversations to gather sensitive information
35	 Dumpster Diving	Searching discarded materials for sensitive information
36	 Videotaping	Secretly recording people or sensitive areas for malicious purposes
37	 Lock Picking	Manipulating locks to gain unauthorized physical access
38	 Master Key Theft	Stealing master keys to gain widespread physical access
39	 Physical Access Attacks	Gaining unauthorized physical access to secure areas or systems
40	 Social Engineering in Person	Face-to-face manipulation and deception to obtain information or access
<b>IV. Financial and Identity Theft Attacks</b>		
41	 ATM Skimming	Installing devices on ATMs to steal card information
42	 Card Skimming	Using devices to steal card information at payment terminals
43	 Diversion Theft	Creating a distraction to steal physical items or information
<b>V. Tools and Techniques</b>		
44	 Social Engineering Toolkit (SET)	Software used to perform various social engineering attacks

<https://www.perplexity.ai/search/addquishing-and-spim-to-the-ta-MbuDF6h.RVmOrAC0TZnGOw#1>