Konfydence
Outsmart Scams - Together

Social Engineering & Scam Terminology

Term	Category	Definition
Social Engineering	Psychology / Umbrella term	The psychological manipulation of people to make them disclose confidential information or perform risky actions (e.g. transferring money, clicking links). It is the basis of most scams.
Phishing	Email fraud	Attempts to obtain passwords or sensitive data via email by impersonating a trusted entity (bank, manager, authority).
Smishing	SMS / text fraud	Phishing carried out via SMS or messaging apps (e.g. WhatsApp, Telegram), often using urgent messages about parcels, taxes, or refunds.
Vishing	Voice fraud	Phishing conducted via phone calls, where scammers pose as bank staff, IT support, or police to manipulate victims.
Impersonation	Psychology / Tactic	Pretending to be someone else (e.g. a bank employee, professor, family member) to gain trust or authority.
CEO Fraud / Business Email Compromise (BEC)	Impersonation	A scam where attackers impersonate a senior executive and pressure employees to make urgent, confidential payments.
Spear Phishing	Phishing variant	Highly targeted phishing attacks tailored to a specific person or organization, often using personal information.
Pretexting	Psychology / Tactic	Creating a believable story or excuse to obtain sensitive information (e.g. “account verification”).
Tailgating	Physical security	Gaining unauthorized access to secure areas by closely following an authorized person.
Shoulder Surfing	Physical security	Stealing PINs or passwords by watching

		someone over their shoulder in public places.
Baiting	Malware distribution	Luring victims with an attractive "bait" (e.g. a USB stick labeled "Salary List") to infect their device.
Malware	Software risk	A general term for malicious software, including viruses, trojans, spyware, and ransomware.
Ransomware	Malware	Malware that encrypts files and demands payment to restore access.
Account Takeover (ATO)	Account abuse	When attackers gain control of an online account using stolen or reused credentials.
Credential Stuffing	Account abuse	Using leaked username/password combinations from other breaches to access accounts.
Password Reuse	Human behavior risk	Using the same password across multiple services, increasing the impact of breaches.
Money Mule	Financial fraud	A person who transfers stolen money on behalf of criminals, knowingly or unknowingly.
Payment Redirection Scam	Financial fraud	Scammers manipulate victims into sending payments to fraudulent accounts instead of legitimate ones.
Refund Scam	Financial fraud	Fake refund messages that trick victims into sharing banking or card details.
Marketplace Scam	Consumer fraud	Fraud involving fake buyers or sellers on online marketplaces.
Romance Scam	Emotional manipulation	Long-term scams where attackers build emotional relationships to extract money or information.
Tech Support Scam	Impersonation / Vishing	Scammers pose as technical support to gain access, install malware, or demand payment.
QR Code Phishing (Quishing)	Modern phishing	Malicious QR codes that redirect victims to fake login or payment pages.

Limbic Hijack	Psychology	A stress response where emotional reactions override logical thinking, leading to impulsive decisions.
Authority Bias	Psychology	The tendency to comply with requests from perceived authority figures without questioning them.
Urgency Bias	Psychology	The tendency to act quickly under time pressure, bypassing careful decision-making.
Cognitive Load	Psychology	Mental overload that reduces the ability to detect scams, especially under stress or multitasking.