KEY STATISTICS

98%
of cyberattacks rely on social engineering.

3.4 billion
phishing emails are sent every day globally.

$4.5 million
is the average cost of a social engineering breach.

8 COMMON ATTACK TYPES

1 Phishing

Fraudulent emails that mimic trusted sources to steal credentials or install malware.

How to spot it:

- Sender domain is slightly misspelled.
- Urgent call-to-action or threat.
- Links don't match the display text.

Channel: Email, SMS, Voice

2 Spear Phishing

Highly targeted attacks that use personal details to appear legitimate to a specific person or organisation.

How to spot it:

- References your name, role, or specific projects.
- Requests unusual wire transfers or sensitive data.
- Claims to be a senior executive or trusted contact.

Channel: Targeted email, Targeted messaging

3 Pretexting

The attacker fabricates a scenario, posing as IT support, an auditor, or a vendor, to extract sensitive information.

How to spot it:

- Caller demands credentials 'to fix an issue'.
- Story feels rehearsed or unusually detailed.
- Request cannot be verified through official channels.

Channel: Phone, In-person

4 Baiting

Entices victims with something appealing such as a free download, a USB drive, or a prize, to deploy malware or steal data.

How to spot it:

- Unexpected free offer or prize notification.
- Unknown USB drive or physical media left in a common area.
- Download requires you to disable security software.

Channel: Physical, Digital

5 Tailgating

Physically following an authorised person through a secure access point without proper credentials.

How to spot it:

- Stranger waits closely behind you at a secured door.
- Claims their access badge is broken or forgotten.
- Carries large items to justify a request for help.

Channel: Physical access

6 Vishing

Voice phishing calls that impersonate banks, government agencies, or IT helpdesks to steal personal information.

How to spot it:

- Creates fear: threat of arrest, fraud, or account suspension.
- Pressures you to act immediately without time to think.
- Asks for OTPs, PINs, or card details over the phone.

Channel: Voice, VoIP

7 Smishing

SMS-based attacks that deliver malicious links or fake alerts to steal data or money from mobile users.

How to spot it:

- Text arrives from an unknown short code or number.
- Fake package delivery or bank alert contains a link.
- Link leads to a lookalike login or payment page.

Channel: SMS, Mobile

8 Quid Pro Quo

The attacker offers a service such as free tech support in exchange for login credentials or system access.

How to spot it:

- Unsolicited offer to fix your computer or account.
- Requests remote access to 'resolve the issue'.
- The help offered always comes with strings attached.

Channel: Phone, Service exchange

YOUR DEFENSE CHECKLIST

1. Verify identities through official channels before sharing any information.
2. Slow down, urgency and pressure are red flags, not reasons to comply.
3. Never share OTPs, passwords, or PINs, no legitimate organisation will ask.
4. Hover over links to check the real URL before clicking.
5. Enable multi-factor authentication on all critical accounts.
6. Report suspicious contacts to your IT or security team immediately.