What is Social Engineering?

Cybercriminals don't just attack machines, they target people. Social engineering uses psychological manipulation to trick employees into giving away information, credentials, or access. By exploiting human trust, attackers often bypass even the strongest technical defences.

Common Tactics

Pretexting

Attackers invent a convincing story or role (such as IT support or a vendor) to make you hand over sensitive details.

Tip: *Always question unusual requests, especially those asking for personal or company data.*

Baiting

Free items, like USB sticks, software, or downloads, are offered to lure victims. Once used, they infect systems with malware.

Tip: *Don't use or install anything unless it comes from a trusted, verified source.*

Impersonation

Criminals pretend to be colleagues, managers, or business partners to build trust and get quick compliance.

Tip: *Verify identity through a separate channel before sharing information or taking action.*

Staying Alert

Social engineering preys on urgency, curiosity, or fear. If something feels unusual or suspicious, it usually is.

Tip: *Trust your instincts, follow any security awareness training you may have received, and report suspicious behaviour immediately.*