SOCIAL ENGINEERING & PRETEXTING

What Is Social Engineering?

- It is when an attacker tricks people instead of hacking machines.
- They use emotions like fear, trust, or urgency.
- Goal: make you reveal information or perform an action.

What Is Pretexting?

- A fake story created by the attacker to look believable.
- They pretend to be someone important (IT admin, HR, bank officer).
- They use small details to gain your trust.
- Purpose: get info like passwords, OTPs, documents.

Maryam receives a phishing call

Caller: ‘Hello, I’m from ‘IT Support,’

“We saw suspiccious login attempts on your email.”

Please tell me your OTP so I can secure your account.

→ This is pretexting –

Components of a Successful Pretext

Identity: Fake role such as auditor, manager, or vendor.

Story: Believable narrative aligned with the victim’s environment.

Trigger: Urgency, compliance, or authority pressure.

Objective: Extract credentials, financial info, or system access.

What You Should Do

- Never share OTPs, passwords, or admin codes.
- Hang up and call the real department yourself.
- Report the suspicious attempt to the security team.
- Stay calm — attackers want you to panic.