# 3. ON-SITE SOCIAL ENGINEERING ATTACK

Attackers try to gain physical access to offices or restricted areas by pretending to be legitimate staff, delivery personnel, maintenance workers, or IT support. They rely on confidence, urgency, and social pressure to slip past security checks, often aiming to plant devices, steal data, or access workstations left unattended.

MALWARE
IT Support

# Scenario: Arham Holds Door for a “Delivery Guy”

A man carrying boxes walks toward the office door:
“Bro can you hold it? I just need to drop this inside.”

Arham opens the door politely, assuming it’s a normal delivery.

The attacker slips inside and walks straight toward employee areas, bypassing all security checks.

The boxes and casual tone are used to lower suspicion and exploit basic politeness.

Lesson: Never allow unknown individuals into secure areas without proper verification. Direct visitors to reception or security, even if they seem harmless or in a hurry.

SERVER
EQUIPHENT

# How On-Site Social Engineering Works?

- Relies on politeness
- Tailgating behind employees
- Fake uniforms or badges
- Pretending to be in a hurry

# Red Flags Arham Should Notice

- Delivery person entering without verification
- No visitor pass
- Avoids eye contact
- Knows too much/or too little about office layout

# Prevention Tips

- Never let unknown individuals inside
- Direct visitors to reception
- Challenge unknown persons politely
- Report tailgating attempts immediately