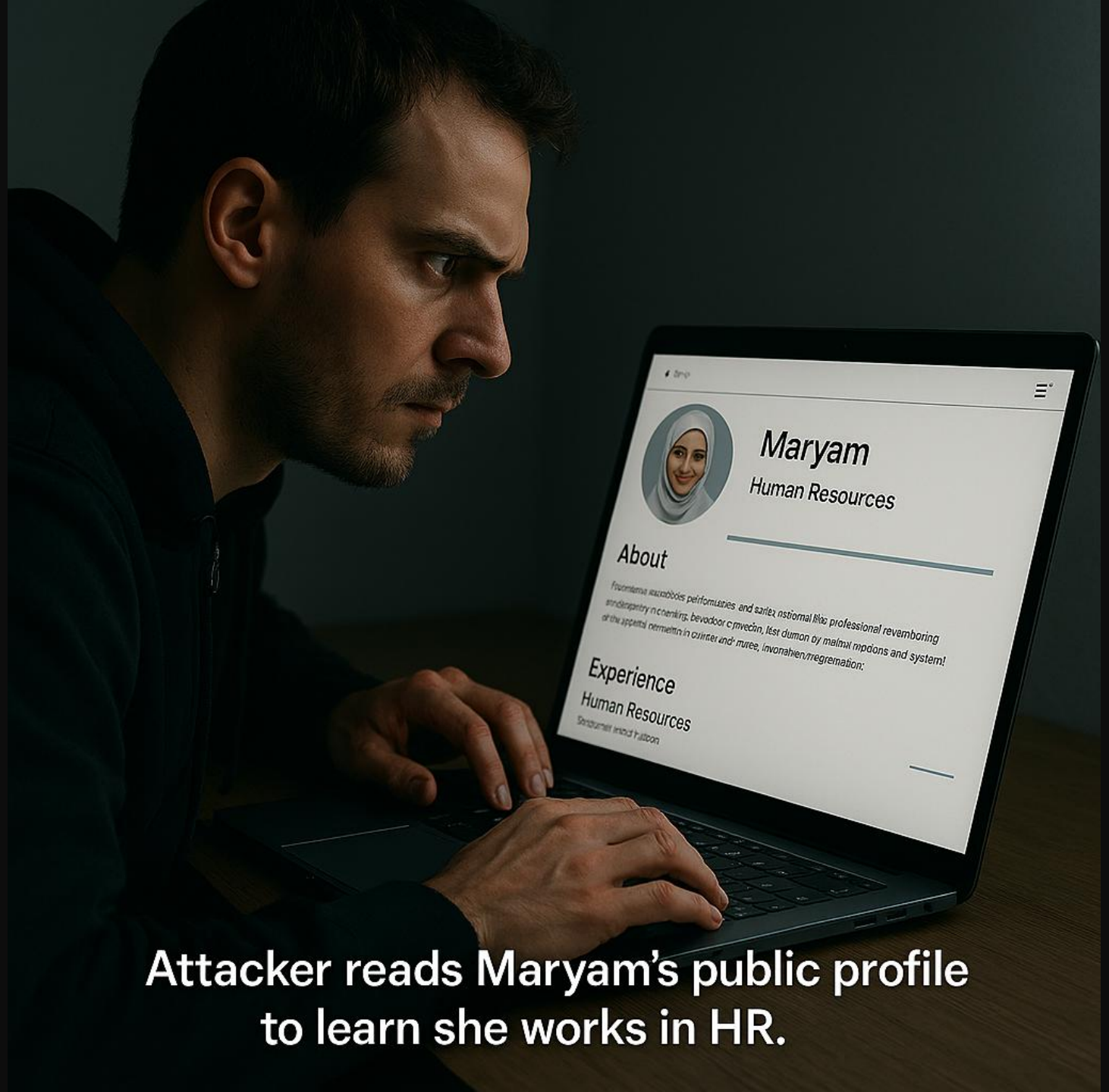
How Phishing Works (Anatomy of an Attack)

Overview of Phishing Workflow

- Phishing is a **step-by-step trick** used by attackers.
- The attacker pretends to be someone trusted.
- They want you to **click, share, or download** something harmful.
- Goal: steal information or access your accounts.

Step 1 – Attacker Plans the Target

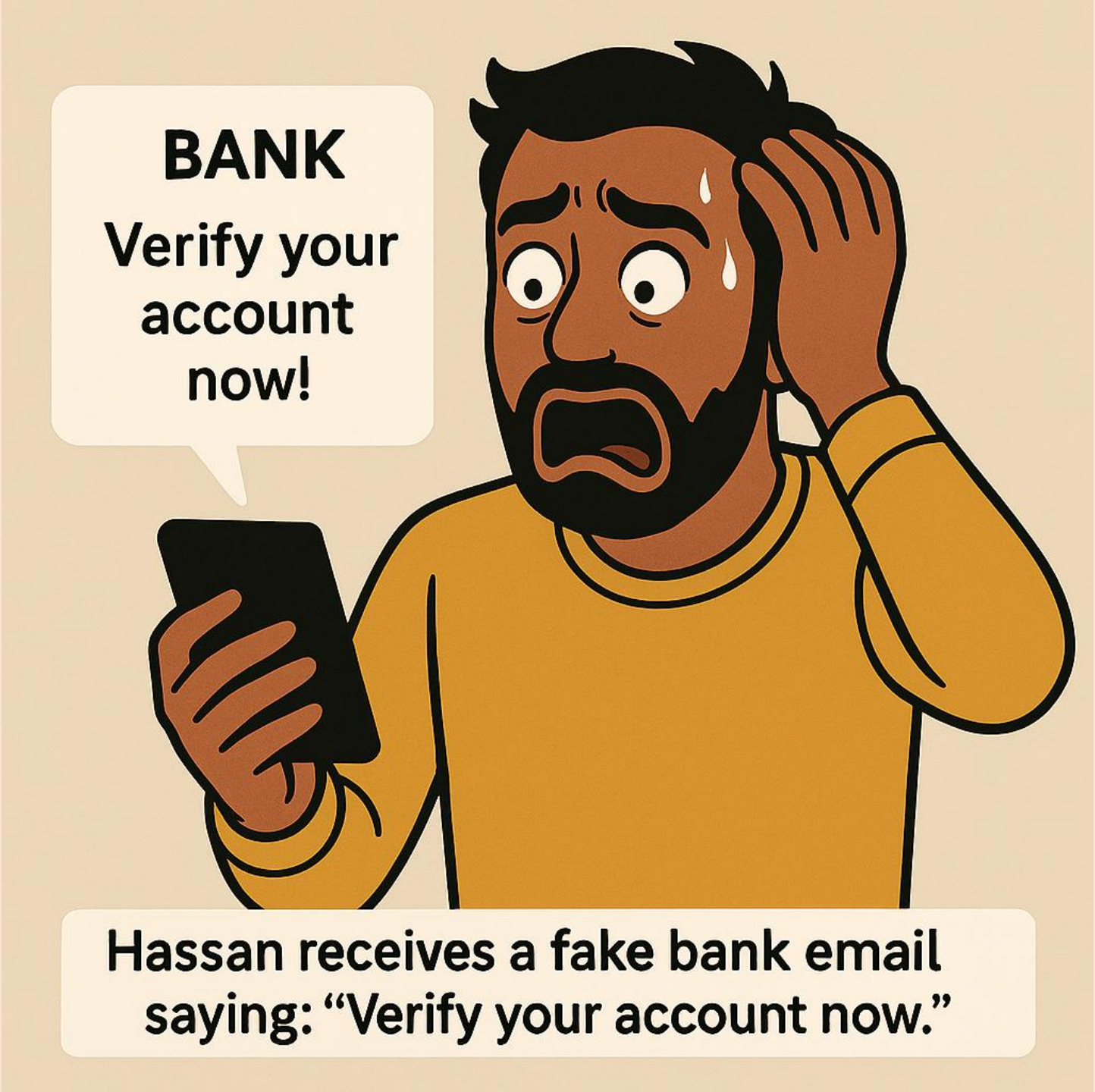
- They choose who to attack (individual or company).
- They gather basic info: email, job role, interests.
- They decide what type of message will work best.
- This step is called ***reconnaissance***.



Attacker reads Maryam's public profile to learn she works in HR.

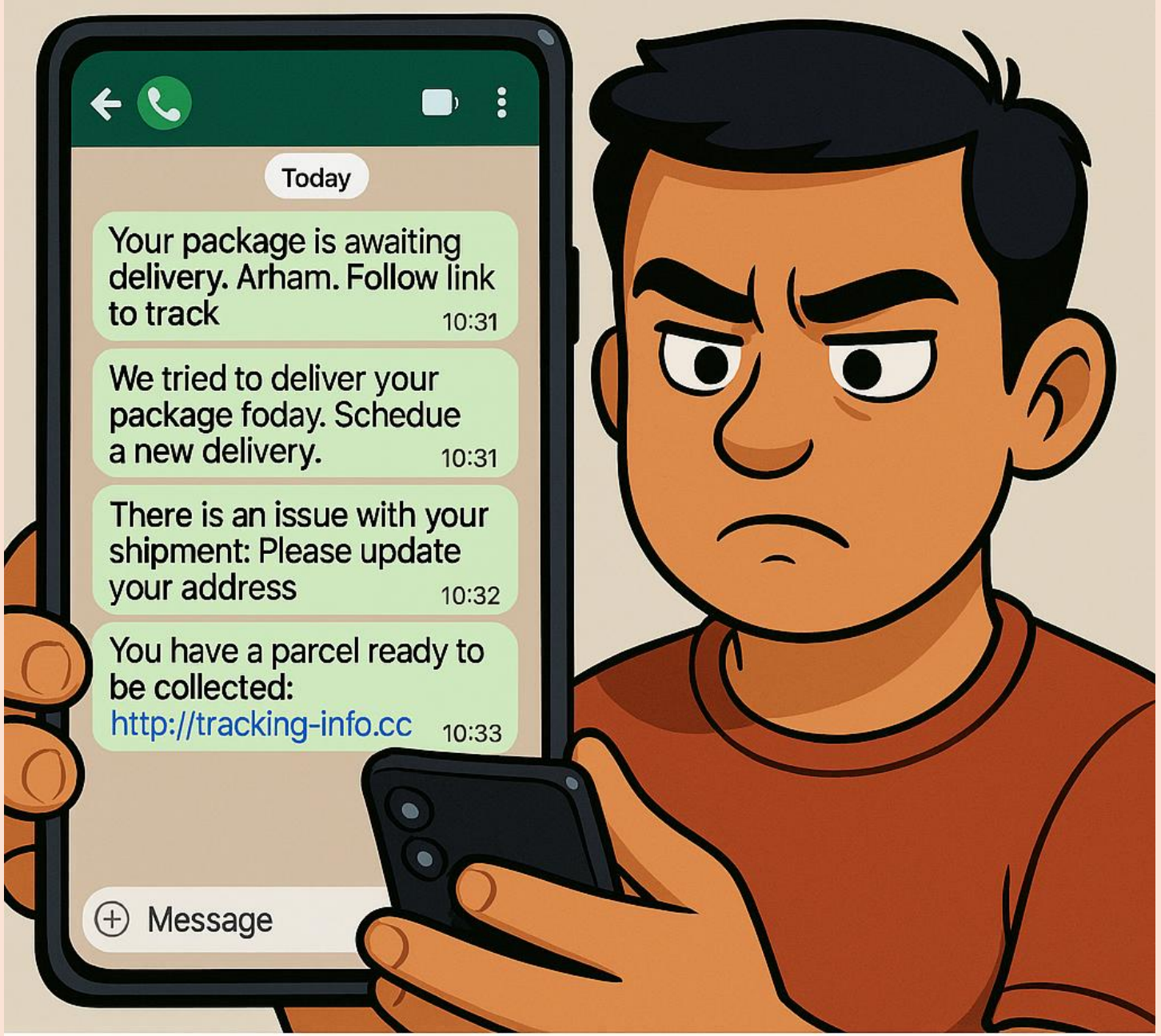
Step 2 – Crafting the Lure

- They design an email, SMS, or social media message.
- It looks like it’s from a trusted company.
- It may contain a ***fake link or harmful attachment***.
- Message creates **urgency.**


BANK
Verify your account now!
Hassan receives a fake bank email saying: “Verify your account now.”

Step 3 – Delivery of the Attack

- Message reaches the target through email, SMS, WhatsApp, etc.
- Attackers send thousands of messages at once.
- Their goal: someone will eventually click.
- This is called ***phishing delivery***.



Arham gets a WhatsApp message pretending to be from a parcel delivery service

Step 4: The Hook (Victim Action)

- The victim clicks a link or downloads a file.
- Fake website collects passwords.
- Attachment installs malware.
- The moment you interact — the attack succeeds.

Step 5 – Attacker Gains Access

- Attacker logs into your real account.
- They may steal money, contacts, data, or files.
- Sometimes they spread the attack to others.
- This final step is where damage happens.

Attack Lifecycle Summary