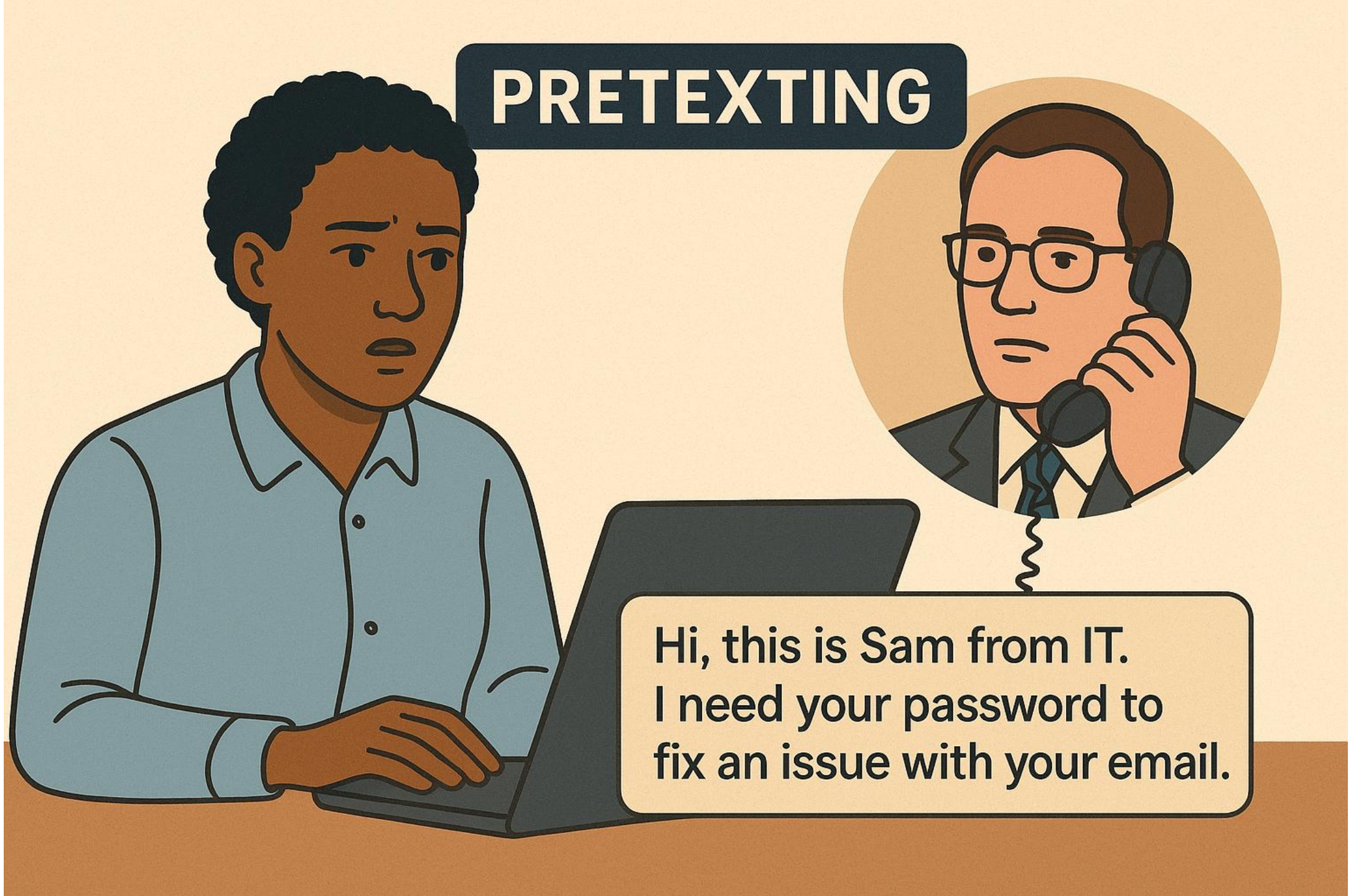
# 2. PRETEXTING / IN-PERSON SOCIAL ENGINEERING

Attackers create a convincing story or scenario to manipulate employees into revealing sensitive information or granting access. They may pose as IT staff, executives, vendors, or customers, and use phone calls, emails, or in-person interactions. The key is making the situation seem legitimate so the target willingly complies.


PRETEXTING
Hi, this is Sam from IT.
I need your password to
fix an issue with your email.

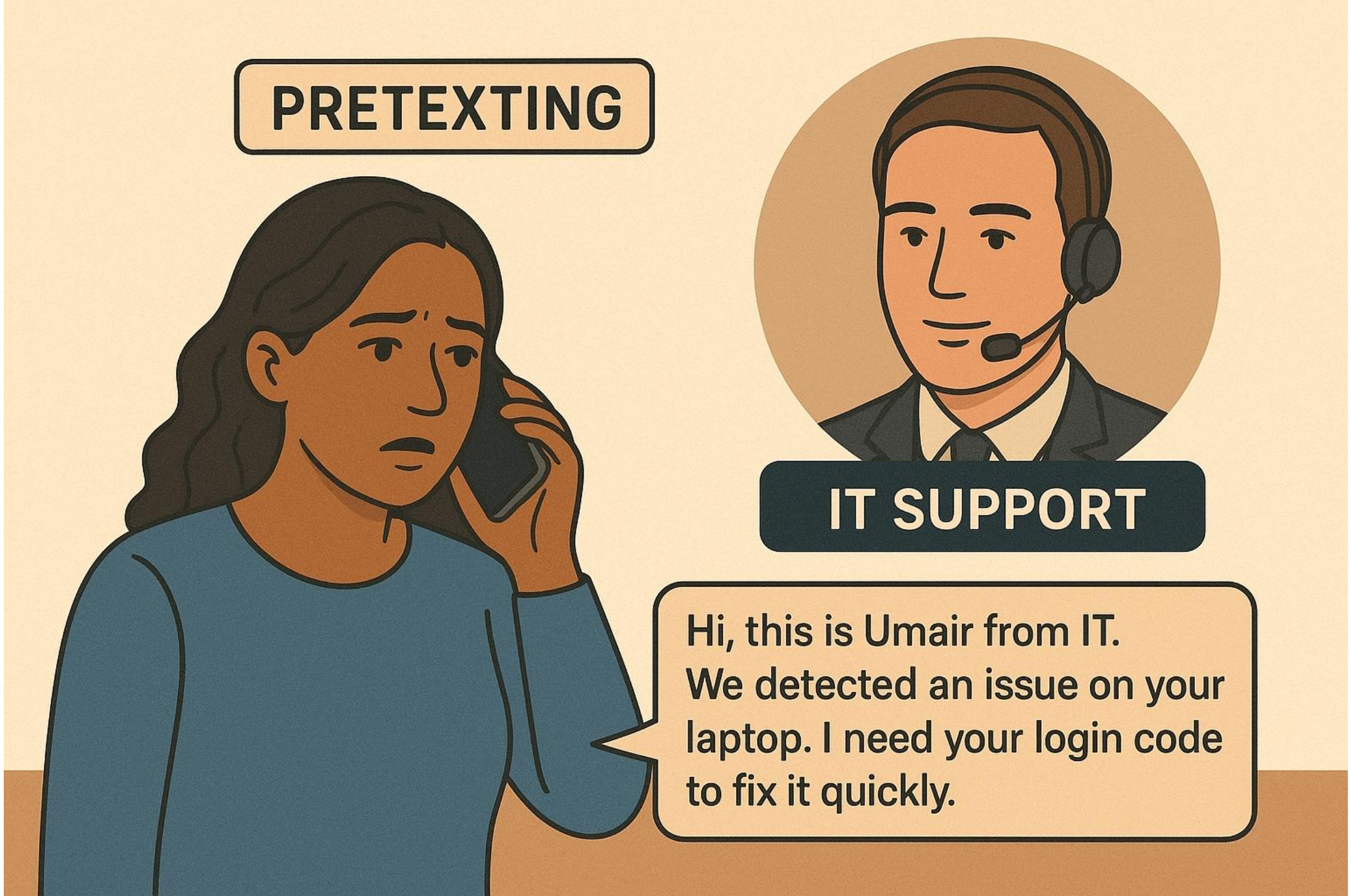
# Scenario: Maryam Receives a Call From “IT Support”

Maryam gets a call:
“Hi, this is Umair from IT. We detected an issue on your laptop. I need your login code to fix it quickly.”

The caller sounds calm and professional, but it’s an attacker using a carefully scripted pretext.

The attacker creates urgency and authority to pressure Maryam into sharing sensitive credentials.

Lesson: Always verify IT requests through official channels. Never share passwords, OTPs, or access codes over unsolicited calls, even if the caller seems legitimate.


PRETEXTING
IT SUPPORT
Hi, this is Umair from IT.
We detected an issue on your laptop. I need your login code to fix it quickly.

# How Pretexting Tricks Employees?

- Polite, confident tone
- Use of internal terminology
- Pretends to be “helping” with a problem
- Creates urgency to skip verification

# Red Flags Maryam Should Notice

- Unknown internal extension
- Unexpected request for login codes
- No support ticket raised
- Asks for private/sensitive info on the call

# Prevention Tips

- Always verify caller identity
- Never share passwords or 2FA codes
- Follow official IT support channels
- Report suspicious calls immediately