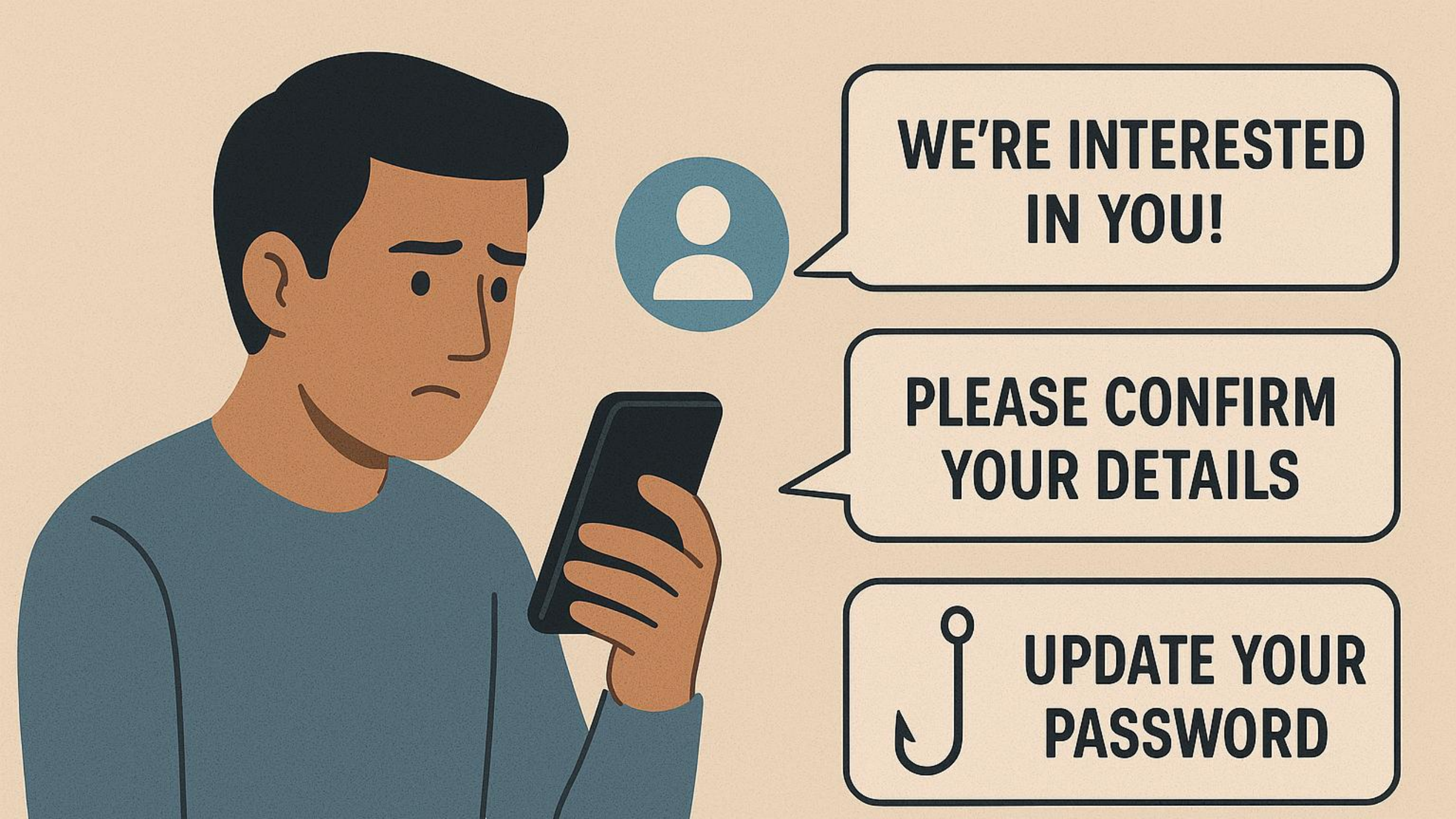
1. SOCIAL MEDIA PHISHING

Social media phishing occurs when attackers use platforms like LinkedIn, Facebook, Instagram, or X to pretend to be trusted individuals or organizations.

They may pose as employers, colleagues, recruiters, tech support, or even friends to gain trust.

Their goal is to trick users into clicking malicious links, sharing personal details, or handing over account credentials by appearing credible and familiar.


WE'RE INTERESTED IN YOU!
PLEASE CONFIRM YOUR DETAILS
UPDATE YOUR PASSWORD

Scenario: Maryam Gets a Fake LinkedIn Job Offer

Maryam receives a LinkedIn message from someone posing as a recruiter:

“Hi Maryam, we reviewed your profile for a remote job. Download the job description.”

The profile looks professional, with a company logo and several connections, so she trusts it.

But the file she’s asked to download contains malware designed to infect her system and steal data.

Lesson: Always verify recruiters and job offers before downloading any files. Legitimate recruiters will never ask you to open unknown documents without proper verification.


Acme Recruiters
Hi Maryam, we reveiwed your profile for remote job remote job. Downioad the job description.
Download Job Descripti
MALWARE
Suspricus File Detected

Tactics on Social Media

- Fake profiles
- Free giveaways
- Investment schemes
- Fake support agents
- Fake HR recruiters

How to Identify Fake Profiles

- Very few connections
- Generic photos
- No work history
- Asking to download files or click links
- Profile created recently

Prevention Tips

- Don’t download files from unknown profiles
- Verify LinkedIn recruiters
- Don’t share work info publicly
- Keep social media privacy tight