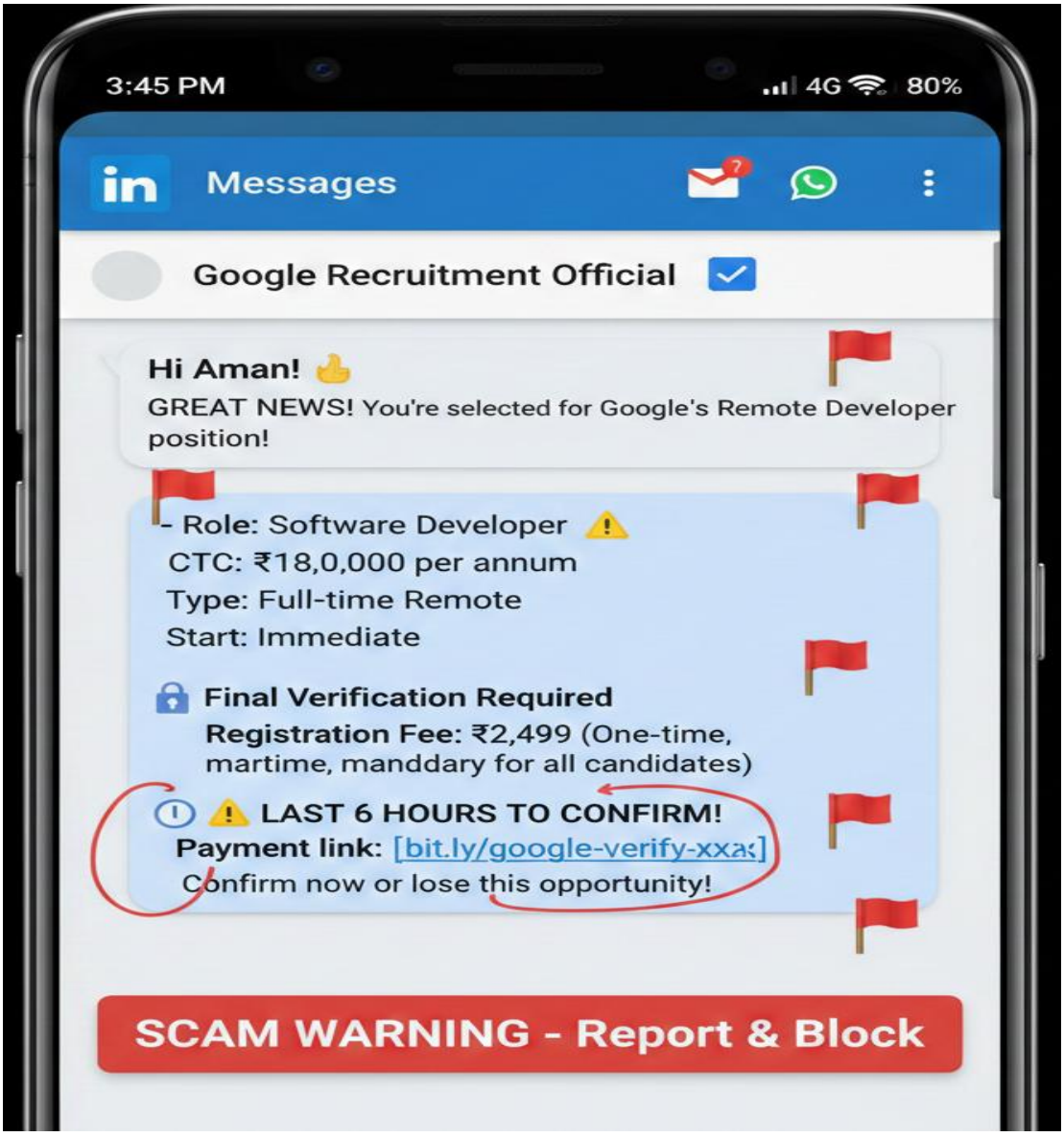
PRACTICAL – 8

OBJECTIVE: – Identify one real phishing email: A final-year student, Aman, receives a LinkedIn message saying:

"You are shortlisted for a Remote Software Developer role at Google.

Salary: ₹18 LPA. Pay ₹2,499 as verification fee. Limited seats. Pay now to confirm." ANSWER THE QUESTIONS: –

a. ***What type of cybercrime is happening here?***
b. ***List of 3 red flags that show it is a scam.***
c. ***What should he do to verify if a job offer is real?***



What type of cybercrime is happening here?

This is a case of Job/Employment Phishing Scam (also called Recruitment Fraud or Advance Fee Fraud).
Specific cybercrime categories involved:

1. Phishing - Fraudulent attempt to obtain money by impersonating a legitimate company (Google)
2. Advance Fee Fraud - Requesting upfront payment for a fake opportunity
3. Identity Theft Risk - If personal/financial details are shared during "verification"
4. Brand Impersonation - Unauthorized use of Google's name and reputation

List of 3 Red Flags that Show It's a Scam

🚩 Red Flag #1: Upfront Payment Request

- Legitimate companies NEVER ask candidates to pay verification fees, processing fees, or any charges for job offers
- Real recruiters, especially from reputed companies like Google, bear all recruitment costs
- Any request for money (₹2,499 or any amount) is an immediate scam indicator

🚩 Red Flag #2: Unrealistic Urgency & Pressure Tactics

- "Limited seats. Pay now to confirm" creates artificial urgency
- Scammers use time pressure to prevent victims from thinking critically
- Real recruitment processes have proper timelines and don't pressure candidates to make instant financial decisions

🚩 Red Flag #3: Unprofessional Communication Channel & No Proper Selection Process

- Direct job offer on LinkedIn message without any interview, assessment, or formal application
- No mention of interview rounds, technical tests, or HR screening
- Legitimate Google recruitment involves multiple interview stages, coding tests, and official communication through @google.com email addresses
- ₹18 LPA salary offered without any evaluation of skills or qualifications

Additional Red Flags (Bonus Indicators):

- Too Good to Be True: High salary (₹18 LPA) for fresher/final-year student without interview
- Grammar/Spelling Issues: Often phishing messages contain poor language (though not mentioned in this example)
- Sender Verification: Message likely from fake/unverified LinkedIn profile, not official Google recruiter
- No Official Domain: No communication from @google.com email

What Should He Do to Verify if a Job Offer is Real?

Immediate Actions:

1. DO NOT Pay Any Money

- **Never send money for job verification, registration, or processing fees**
- **Block and report the sender immediately**

2. Verify the Sender's Authenticity

- **Check the LinkedIn profile thoroughly:**
  - **Is it verified with a blue checkmark?**
  - **Does it show employment at Google with verifiable details?**
  - **How many connections? New profiles are suspicious**
  - **Check profile history and recommendations**
- **Real Google recruiters will have:**
  - **Verified LinkedIn profiles**
  - **Clear employment history at Google**
  - **Professional profile with recommendations**
  - **Google email address (@google.com)**

3. Contact the Company Directly

- **Visit Google Careers official website (careers.google.com)**
- **Call Google's official HR helpline or support**
- **Email Google's recruitment team through official channels**
- **Check if there's a job posting matching the offer**

Verification Checklist:

✅ **Check Official Channels:**

- **Visit the company's official career portal**
- **Look for the specific job posting**
- **Verify if the position actually exists**

✅ **Validate Communication:**

- **Official emails should come from company domain (@google.com, not @gmail.com)**
- **Check email headers for authenticity**
- **Verify phone numbers against official company website**

✅ **Research the Recruitment Process:**

- **Google's hiring process is well-documented online**
- **Includes multiple rounds: phone screening, technical interviews, behavioral interviews**
- **No legitimate stage involves payment**

✅ **Cross-Check Information:**

- **Search online: "[Company name] + recruitment scam"**
- **Check on forums like Glassdoor, Reddit, or company review sites**
- **Ask current employees on LinkedIn or professional networks**

✅ **Report the Scam:**

- **Report on LinkedIn: Flag the message as spam/scam**
- **Cybercrime Portal: Report to https://cybercrime.gov.in**
- **Company: Inform Google about brand impersonation**
- **Warn Others: Share experience to prevent others from falling victim**

What Legitimate Job Offers Look Like:
Real recruitment process includes:

- **Official communication from company email domain**
- **Formal interview rounds (technical, HR, managerial)**
- **Skills assessment and verification**
- **Offer letter on official letterhead with company details**
- **Zero upfront costs or fees**
- **Reasonable timeline without artificial pressure**
- **Clear job description, responsibilities, and benefits**
- **Direct communication with verified HR representatives**

Summary: Golden Rules to Avoid Job Scams

1. **Never pay money for job opportunities**
2. **Verify through official company channels**
3. **Be skeptical of unsolicited job offers**
4. **Trust your instincts - if it seems too good to be true, it probably is**
5. **Do thorough background research before sharing personal information**
6. **Report suspicious activities immediately**

What Aman Should Do:

1. ❌ **Do NOT click any links or pay the fee**
2. 🚫 **Block and report the sender on LinkedIn**
3. 📧 **Report to cybercrime.gov.in**
4. ⚠️ **Warn friends and classmates about the scam**
5. ✅ **Apply through official Google Careers portal if genuinely interested**
6. 📚 **Educate himself about common recruitment scams**