Experiment 8

Que.8- 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.

a) Salary: ₹18 LPA. b) Pay ₹2,499 as verification fee. c) Limited seats. Pay now to confirm.”

QUESTIONS :

a. **What type of cybercrime is happening here ?**

Ans. This is a phishing scam (specifically a job offer scam) where attackers impersonate a trusted company (Google) to trick victims into paying money or sharing sensitive information.

b. **List 3 red flags that show it is a scam ?**

Ans. 3 Red Flags :-

1. **Upfront Payment Request – Legitimate companies never ask candidates to pay a “verification fee” or any money during recruitment.**
2. **Too Good to Be True Offer – A high salary (₹18 LPA) for a fresh graduate without interviews or proper process is suspicious.**
3. **Urgency & Pressure Tactics – “Limited seats. Pay now to confirm” is a classic scam technique to push victims into acting quickly without verifying.**

c. **What should he do to verify if a job offer is real ?**

Ans. How to Verify if a Job Offer is Real :-

1. **Check Official Sources – Visit Google’s official careers page (careers.google.com) or LinkedIn’s verified company profile to confirm if the role exists.**
2. **Verify Sender Identity – Ensure the recruiter’s LinkedIn profile is genuine (look for verified badge, work history, connections).**
3. **Cross-Check via Direct Contact – Reach out to Google HR through official email or LinkedIn channels, not through the suspicious message.**