PRACTICAL 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. 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?

This is a phishing scam (specifically, a job offer scam). The attacker tries to trick Aman into sending money by pretending to offer a high-paying job.

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

1. Upfront payment request: Legitimate companies like Google never ask candidates to pay a “verification fee” to confirm a job.

2. Too good to be true: The offer of ₹18 LPA for a remote role with minimal process is unusually high for a final-year student.

3. Pressure tactics & urgency: Phrases like “Limited seats. Pay now” create false urgency, a common trick in scams.

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

1. Check the official website: Look for the job posting on Google’s official careers page.

2. Verify the sender: Check the LinkedIn profile carefully – official recruiters usually have a verified account with detailed professional info.

3. Never pay upfront: Legitimate companies never charge candidates any fees.

4. Contact the company directly: Use official contact information from the company website to confirm the offer.