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 Job Phishing/Employment Scam. It is a form of Social Engineering where the attacker impersonates a reputable company (Google) to steal money or sensitive personal information.

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

- **Payment Request**: No legitimate company, especially a global leader like Google, will ever ask a candidate to pay a "verification fee" or "onboarding fee" to secure a job.
- **Artificial Urgency**: The use of phrases like "Limited seats" and "Pay now to confirm" is a tactic designed to make you act quickly without thinking or verifying the details.
- **Suspicious Salary/Offer Ratio**: Receiving a high-paying offer (₹18 LPA) via a random LinkedIn message without a formal interview or application process is highly unrealistic.

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

- **Check the Email Domain:** Ensure the sender's email address ends exactly in the official company domain (like @google.com) rather than a public or misspelled one.
- **Search Official Portals:** Visit the company's official careers website and search for the specific Job ID or role mentioned in the message.
- **Follow the No-Fee Rule:** Remember that legitimate employers will never ask for money—for "verification," "training," or "security"—at any stage of the hiring process.