Q. 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?

Ans:- **Phishing / Job Offer Scam (Employment Fraud).**
The attacker is pretending to be a legitimate company (Google) to trick the victim into paying money.

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

Ans:- 1. **Asking for money (₹2,499 verification fee)** — No genuine company, especially Google, charges money for hiring.

2. **Unrealistic offer / Too good to be true** — High salary (₹18 LPA) for a remote role via LinkedIn message without any interview.
3. **Urgency (“Limited seats. Pay now”)** — Scammers create false urgency to make victims act quickly.

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

Ans:- 1. **Check the sender's profile** – Genuine recruiters have verified company emails, proper LinkedIn profiles, and official domains (@google.com).

2. **Visit the official company careers website** – Google posts all real jobs only on *careers.google.com*.
3. **Contact the company directly** – Email Google HR or support to verify the offer.

4. **Never pay any money** – Legitimate companies never ask for fees for interviews, verification, or onboarding.