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.

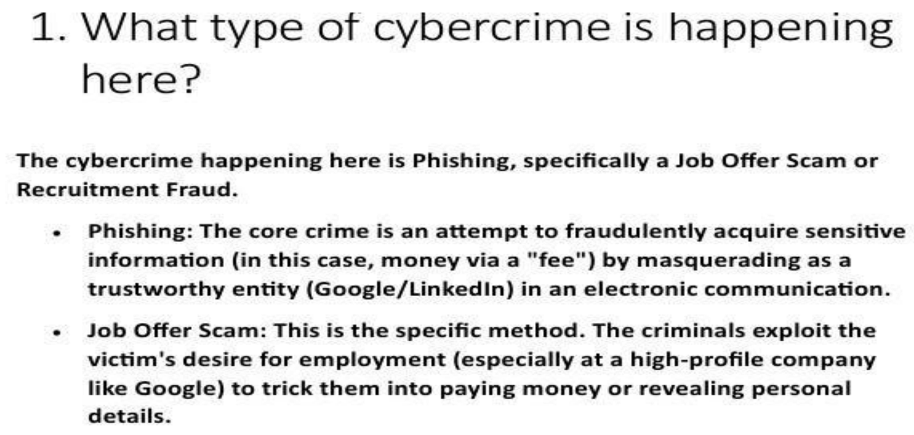
Limited seats. Pay now to confirm."

ANSWER THE QUESTIONS :-

a. What type of cybercrime is happening here?

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

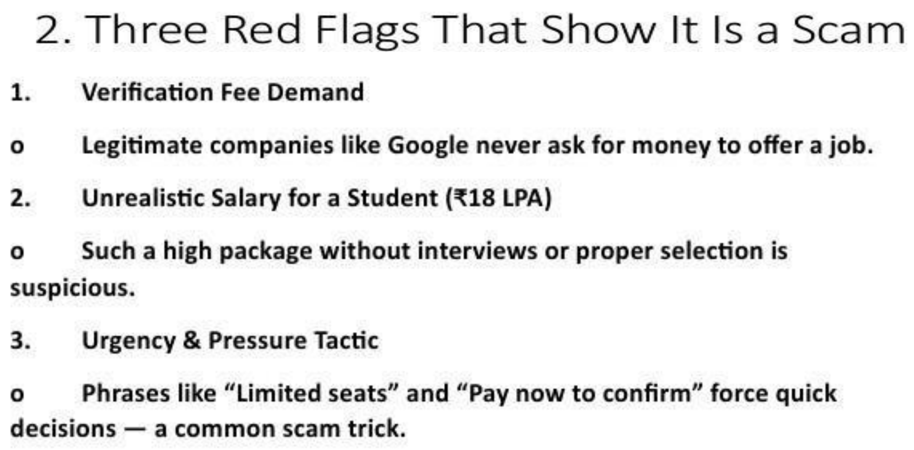
c. What should he do to verify if a job offer is real?



1. What type of cybercrime is happening here?

The cybercrime happening here is Phishing, specifically a Job Offer Scam or Recruitment Fraud.

- **Phishing: The core crime is an attempt to fraudulently acquire sensitive information (in this case, money via a "fee") by masquerading as a trustworthy entity (Google/LinkedIn) in an electronic communication.**
- **Job Offer Scam: This is the specific method. The criminals exploit the victim's desire for employment (especially at a high-profile company like Google) to trick them into paying money or revealing personal details.**



2. Three Red Flags That Show It Is a Scam

1. Verification Fee Demand

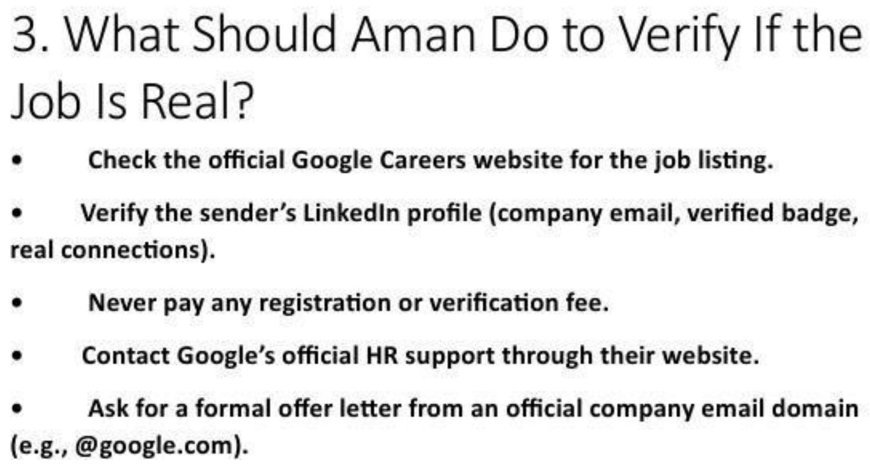
o Legitimate companies like Google never ask for money to offer a job.

2. Unrealistic Salary for a Student (₹18 LPA)

o Such a high package without interviews or proper selection is suspicious.

3. Urgency & Pressure Tactic

o Phrases like "Limited seats" and "Pay now to confirm" force quick decisions — a common scam trick.



3. What Should Aman Do to Verify If the Job Is Real?

- **Check the official Google Careers website for the job listing.**
- **Verify the sender's LinkedIn profile (company email, verified badge, real connections).**
- **Never pay any registration or verification fee.**
- **Contact Google's official HR support through their website.**
- **Ask for a formal offer letter from an official company email domain (e.g., @google.com).**