EXPERIMENT:- 08

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 ₹2,4GG as verification fee.

Limited seats. Pay now to confirm.”

ANSWER THE QUESTIONS: -

a) What type of cybercrime is happening here? ans => The type of cybercrime is happening here:

The above message is an example of phishing and job fraud (advance-

fee scam), where the scammer pretends to be a recruiter from Google and asks for money in the name of a verification fee.

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

ans => a) Type of cybercrime

The above message is an example of phishing and job fraud (advance-fee scam), where the scammer pretends to be a recruiter from Google and asks for money in the name of a verification fee.

b) Three red flags showing it is a scam

1. Asking for money for a job:

A genuine company like Google will never ask a candidate to pay any verification fee, registration fee, or interview fee to get a job. Any demand for payment to secure a position is a strong sign of a scam.

2. Too good an offer with pressure:

The message promises a high salary (₹18 LPA) and uses urgent language like “Limited seats. Pay now to confirm”, which is a common tactic used by scammers to create panic and stop the victim from thinking carefully.

3. Unprofessional and unofficial approach:

A real job offer from Google normally comes through official email IDs or the Google careers portal, after proper application and interviews, not through a random LinkedIn message asking for immediate payment. The message does not share any proper interview process, official contact details, or offer letter

on the company letterhead.

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

1. Check the official source:

- Visit the official Google Careers website (careers.google.com) and see if such a job (Remote Software Developer, similar salary, etc.) is listed.
- He should also check if he has applied for such a role.

2. Verify the sender’s identity:

- Open the sender’s LinkedIn profile and check whether they have

a proper company tag (Google), enough connections, work history, and a professional profile.

- Search the person’s name and email ID on Google to see if they are a genuine recruiter.

3. Cross-check through official communication:

- He should contact Google only through official channels (official email addresses or contact forms from the Google website), not reply to the suspicious message.
- He must never pay any money. If still doubtful, he should show the message to a teacher, placement cell, or cybercrime helpline and can report the message on LinkedIn as a scam.