

(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?

Ans:- This scenario describes a prime example of a job scam conveyed via a LinkedIn message.

a) The type of cybercrime happening here is **phishing**, specifically a targeted form of phishing known as **spear phishing** [1]. The perpetrator is impersonating Google to trick Aman into divulging money under false pretenses. The specific crime of using a fake job offer to steal money is also known as a **job scam** or **employment scam**.

b) Here are three major red flags in the message Aman received:

1. **Requirement for an upfront payment/fee:** No legitimate company, especially a major corporation like Google, will ask a job candidate to pay a "verification fee," "security deposit," or any other kind of money to secure a job offer or an interview [2]. This is the biggest red flag.
2. **Unprofessional Urgency and High Pressure:** The phrases "Limited seats" and "Pay now to confirm" are designed to create a sense of panic and prevent the victim from taking time to verify the offer's legitimacy. Legitimate recruitment processes move at a professional pace.
3. **Use of Personal Messaging for Formal Offers:** While initial contact might be made on LinkedIn, a formal job offer from a company like Google would be followed by official communication through an official company email domain (e.g., @google.com), not solely through a LinkedIn direct message from a potentially fake or compromised profile [1].

c) To verify the legitimacy of the offer, Aman should take the following steps:

1. **Do Not Engage with the Sender:** He should immediately stop all communication with the individual who sent the message and should not click any links provided in the message [1].
2. **Verify via Official Channels:** Aman should independently search for Google's official careers website and look for the job opening there [2]. Legitimate jobs are always listed on the official company careers portal. He can verify open roles on the official Google Careers website.
3. **Report the Incident:** He should report the message as a scam to LinkedIn directly through the platform's reporting mechanism to prevent others from being targeted. He can also report the scam to authorities if he wishes to do so.