# Practical 8

## 1. What type of cybercrime is happening here?

The cybercrime happening here is **phishing**, specifically **job-offer phishing** or **employment scam**.

The scammer is pretending to be from Google and is trying to trick the student into paying a fake "verification fee," which makes it a clear case of **phishing to steal money and personal information**.

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

1. **Asking for Money (Verification Fee)**

Legitimate companies like Google **never** ask candidates to pay any fee for interviews, verification, or hiring.

2. **Unrealistic/Too-Good-to-Be-True Offer**

A high salary (₹18 LPA) for a student with no interview or process is **unrealistic**, which is a common trick used by scammers.

3. **Sense of Urgency ("Limited seats. Pay now")**

Scammers create urgency to pressure victims into paying quickly **without thinking or verifying**.

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

- **Check the official website and careers page**

Visit the company's official site (e.g., Google Careers) to see if the job position actually exists.

- **Verify the sender's email or profile**

Legitimate companies use official domains (like *@google.com*). Suspicious or generic emails indicate a scam.

- **Contact the company directly**

Reach out to the company's HR or support through official contact details, not the ones provided in the message.

- **Search online for similar scam reports**

Look up the message or offer wording—many fake job scams are reported online.

- **Check if they ask for money**

No real company asks for fees for interviews, verification, or registration. If they ask for payment, it's fake.