Practical 8: **Identify Phishing Attack**

Aim

To identify phishing attempts through digital messages.

Objectives

- To detect cybercrime
- To recognize scam elements

Materials Required

- Provided phishing example

Procedure

Read message text

Carefully go through the entire message to understand its content and intent.

Make note of any unusual requests or unfamiliar senders.

Identify suspicious elements

Look for spelling errors, urgent demands, unknown links, or too-good-to-be-true offers.

These signs often indicate potential scams or malicious intent.

List cybercrime type

Based on the suspicious elements, categorize the message as phishing, fraud, malware attempt, etc.

This helps in understanding the nature and threat level of the cybercrime.

Write verification steps

Suggest ways to confirm authenticity, such as checking the sender's email, contacting the official source, or scanning links.

These steps help prevent falling victim to cyberattacks.

a) What type of cybercrime is happening here?

Phishing / Job Scam (Employment Fraud).

The attacker is pretending to be Google to steal money and possibly personal information.

---

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

1. Asking for money (₹2,499 verification fee) — Genuine companies never ask candidates to pay for interviews or verification.
2. “Limited seats / Pay now” pressure — Scammers create urgency so the victim does not think clearly.
3. Unrealistic offer without proper process — Google never sends job offers through random LinkedIn messages without interviews, HR contact, or email from official domain (@google.com)