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.

OUTPUT :

a) This is a **phishing scam** — a form of cybercrime where attackers impersonate legitimate organizations to trick individuals into giving up money or personal information.

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

1) **Request for money upfront** — Legitimate companies like Google never ask for a verification fee.

2) **Too-good-to-be-true offer** — ₹18 LPA for a fresher without an interview is suspicious.

3) **Urgency and pressure** — "Limited seats. Pay now to confirm" is a classic tactic used by scammers to rush victims.

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

- **Check the official company website or careers page** for job listings.
- **Contact the company directly** through verified channels to confirm the offer.
- **Look for professional email domains** (e.g., @google.com) instead of generic or social media messages.