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.

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?

ANSWERS:-

a) What type of cybercrime is happening here?
This is a **phishing scam** related to a **fake job offer**.

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

1. Asking for money as a verification or registration fee.
2. Offering a very high salary without a proper interview process.
3. Creating urgency by saying “limited seats” and “pay now”.

c) What should he do to verify if a job offer is real?
He should check the official company website, verify the sender’s details, and contact the company through official communication channels. He should never pay any fee for a job offer.