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

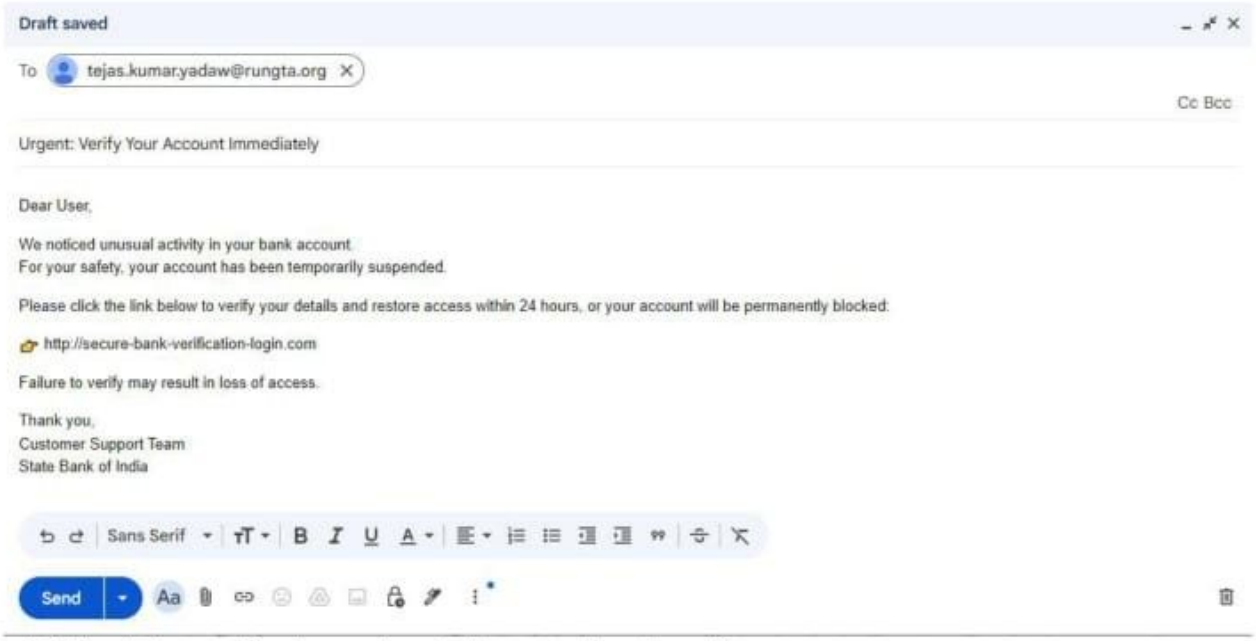
Based on the suspicious elements, categorize the message as phishing, fraud, malware attempt, etc.

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?

This is a **phishing scam** (specifically a **job recruitment scam**).
The scammer pretends to be a trusted company (Google) to trick the student into paying money.

---

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

1. **Demand for money** – Asking for a "verification fee" (₹2,499). Real companies do **not** charge candidates.
2. **Too good to be true offer** – High salary (₹18 LPA) with no interview or proper hiring process.
3. **Urgency pressure** – Phrases like "Limited seats" and "Pay now to confirm" are used to panic victims.

---

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

1. **Check the official Google careers website** for the job listing.
2. **Do not click links or pay any money** from messages on LinkedIn or email.
3. **Contact Google through official email IDs** or ask a college placement officer/career counselor.