OUTPUT

1. **Suspicious sender address**

Check the email ID or domain carefully. Phishing messages often use fake or slightly altered addresses (e.g., extra letters or symbols).

2. **Urgent or threatening language**

Messages that pressure you to act immediately (such as account suspension or security alerts) are common phishing tactics.

3. **Unexpected links or attachments**

Avoid clicking links or downloading files from unknown or unexpected sources. Hover over links to verify the actual URL.

4.**Spelling and grammar mistakes**

Many phishing emails contain noticeable errors, poor formatting, or unprofessional language.

5.**Requests for sensitive information**

Legitimate organizations do not ask for passwords, OTPs, or bank details via email or messages.