Task 2: Analyze a Phishing Email Sample.

Step 1: Obtain a phishing email sample

- Free sources for phishing emails (text or .eml format):
  - PhishTank (https://www.phishtank.com/)
  - APWG Email Threat Archive (https://apwg.org/)
  - Search for .eml phishing samples on GitHub (e.g., "email-samples" repos)
- Save as .eml or plain .txt for safe analysis.

Step 2: Examine sender address

- Check the from: field in the email.
- Look for:
  - Slightly altered domain names (e.g., support@micr0soft.com instead of microsoft.com)
  - Generic domains (e.g., gmail.com instead of official company email)
  - Mismatched display name vs email address

Step 3: Analyze headers

- Open email headers:
  - Gmail: More → Show original
  - Outlook: File → Properties → Internet headers
- Use **free online header analyzers**:
  - MXToolbox Email Header Analyzer
  - Google Message Header Analyzer
- Look for:
  - Received: chain mismatch (originating IP vs claimed source)
  - SPF/DKIM/DMARC authentication results
  - Suspicious Reply-To: addresses

Step 4: Identify suspicious links

- Hover over links (without clicking)
- Check for:
  - Mismatched URL and displayed text
    Example: https://www.paypal.com/login text links to http://malicious.com/login
  - Shortened links (bit.ly, tinyurl)
- Tools:

- VirusTotal URL scan
- curl -I <URL> to safely check headers

Step 5: Examine attachments

- Never open in main OS
- Look for:
  - .exe, .js, .vbs, .scr files → high risk
  - Macro-enabled Office docs (.docm, .xlsm) → often phishing
- Check file hash on VirusTotal

Step 6: Analyze email body

Look for phishing indicators:

1. Urgent or threatening language: “Your account will be closed!”
2. Poor grammar or spelling mistakes
3. Generic greetings (“Dear customer”)
4. Requests for sensitive info (passwords, OTPs, SSN)
5. Fake logos or images (check image URL if possible)

Step 7: Summarize phishing characteristics

Create a table like this:

Feature	Observation	Risk
Sender Email	support@micr0soft.com (typo in domain)	High
SPF/DKIM/DMARC	SPF fail, DKIM pass	Medium
Links	Displayed: paypal.com → Actual: bit.ly/malicious	High
Attachments	invoice.docm (macro-enabled)	High
Email Body	Urgent request, poor grammar	Medium