Phishing Email Analysis Report

1. Check Email Headers for Discrepancies

- **Action Taken:**
  I examined the email headers using an online header analyzer to detect any discrepancies. The detailed results of this analysis have been saved in a file named **"Header analyze data.txt"** and are attached to this report.
- **Finding:**
  The header analysis revealed some discrepancies, including mismatched SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) records. These inconsistencies suggest that the email may not have originated from the claimed sender and could be a spoofed message.
- **Conclusion:** The email headers show signs of being manipulated, indicating potential phishing.

2. Identify Suspicious Links or Attachments

- **Action Taken:**
  Upon reviewing the email, I identified that an attachment was included. The document attached to the email could potentially be harmful.
- **Conclusion:** The attachment should not be opened unless thoroughly scanned using antivirus or a sandbox environment.

3. Look for Urgent or Threatening Language in the Email Body

- **Action Taken:**
  I carefully reviewed the body of the email for any language designed to invoke urgency or fear.
- **Finding:**
  While the email does not contain threatening language, it does mention "Immediate action required" and "Your account is in jeopardy," even though I do not have an account with the supposed sender. This creates a false sense of urgency and confusion.
- **Conclusion:** The email is using urgency to pressure the recipient into acting quickly, even though it is irrelevant to the recipient, indicating it is likely a phishing attempt.

Summary of Phishing Indicators:

Based on the examination of the email, the following phishing indicators were identified:

- Discrepancies in email headers, showing that the email may have been spoofed.
- Suspicious attachment that could contain malware or malicious code.
- False urgency in the email body, claiming account issues despite the recipient not having an account with the sender.