Phishing Email Analysis - Cybersecurity Task

From: PayPal Support

To: you@example.com

Subject: Urgent: Unusual Activity Detected On Your Account

Date: Wed, 03 Jul 2025 14:23:18 +0530

Reply-To: noreply@secure-paypall.com

Message-ID: <A1B2C3D4E5F6G7@secure-paypall.com>

MIME-Version: 1.0

Content-Type: text/html; charset="UTF-8"

Link: Verify Now

Html page for example:

```
<html>
  <body>
    <h2 style="color: red;">Important Security Alert</h2>
    <p>We noticed unusual login attempts on your PayPal account.</p>
    <p>To ensure your account security, we have temporarily limited your access.</p>
    <p>Please verify your information immediately by clicking the link below:</p>
    <a href="http://secure-paypall-verification.com/login">Verify Now</a>
    <p>Failure to verify within 24 hours will result in permanent suspension of your account.</p>
    <p>Thank you,<br>PayPal Security Team</p>
  </body>
</html>
```

phishing-email-analysis/

|

├— suspicious_email_sample.txt   # The suspicious email (text format)

├— header_analysis_result.txt   # Result from the header analyzer tool

├— phishing_indicators_report.md   # Your analysis report

├— README.md   # Overview and instructions

Identify phishing characteristics in a suspicious email sample using:

- An email client or saved email file (in `.txt` format)

- A free online email header analyzer

🛠️ Tools Used

- Email header analyzer: [MXToolbox](https://mxtoolbox.com/EmailHeaders.aspx) / [Google Admin Toolbox](https://toolbox.googleapps.com/apps/messageheader/)

- Text Editor (VS Code, Notepad++)

- GitHub for documentation

📄 Files Included

- `suspicious_email_sample.txt` – Raw suspicious email content

- `header_analysis_result.txt` – Output from the header analyzer tool

- `phishing_indicators_report.md` – Report listing phishing indicators

- `README.md` – Project documentation and instructions

🔍 Analysis Steps

1. **Save the suspicious email** in `.txt` format from your email client.

2. **Upload the email headers** to an online analyzer like MXToolbox.

3. **Examine the results** for anomalies (e.g., SPF/DKIM/DMARC failures, sender mismatch).

4. **Review email content** for:

  - Urgent or threatening language

- Unusual sender address
- Suspicious links or attachments
- Grammar or formatting issues

5. **Document phishing indicators** in `phishing_indicators_report.md`.

📌 Phishing Indicators (Summary)

Some of the key phishing indicators found:

- Mismatch between “From” and “Return-Path” domains
- Spoofed sender using a lookalike domain
- Unverified links with shortened URLs
- Threatening language urging immediate action
- SPF or DKIM check failures