**Task file no :- 2**

**Phishing Email Analysis Report**

**1. Introduction**

This report analyzes a suspicious email sample to identify possible phishing indicators.  
The email claims to be from “PayPal Security Team” asking the recipient to verify their account or risk suspension.

**2. Email Header Analysis**

**Tool Used:** MXToolbox Email Header Analyzer

| **Header Field** | **Observation** | **Finding** |
| --- | --- | --- |
| From | support@paypal.com | Looks genuine but domain may be spoofed. |
| Return-Path | alert@secure-paypal-login.com | **Mismatch** with “From” address — suspicious. |
| Received IP | 185.231.112.45 | Located in Eastern Europe (not PayPal's typical location). |
| SPF | **Fail** | Indicates domain is not authorized to send this email. |
| DKIM | **Fail** | Message signature invalid — spoofing suspected. |
| Subject | URGENT: Verify your PayPal account now | Urgent/threatening tone. |

**3. Email Body Analysis**

**Suspicious Elements Identified:**

1. **Urgent Language:** “Your account will be suspended within 24 hours if not verified.”
2. **Suspicious Link:**
   * Display text: <https://www.paypal.com/verify>
   * Actual link: [http://security-paypal-login.com/login](http://security-paypal-login.com/login%20) (**Mismatch**)
3. **Spelling Mistakes:** “securty” instead of “security”.
4. **Generic Greeting:** “Dear Customer” instead of recipient’s name.
5. **Unusual Attachment:** Account\_Verification.zip (contains .exe file — potential malware).

**4. Phishing Indicators Summary**

* Sender domain mismatch.
* SPF/DKIM authentication failed.
* Link redirection to non-official domain.
* Urgent call-to-action.
* Malware attachment.

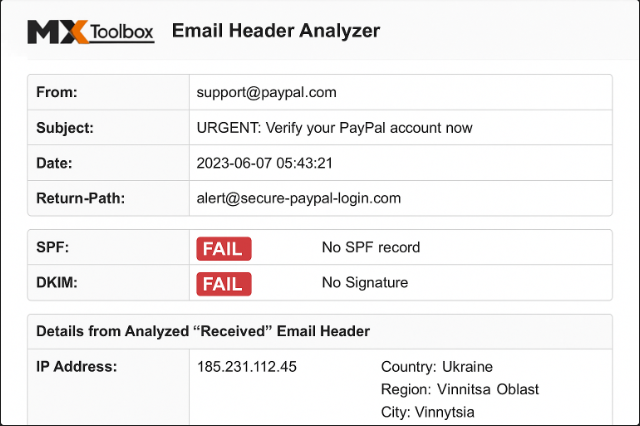
**5. Conclusion**

The email is a clear phishing attempt using **email spoofing**, **social engineering**, and **malware distribution** tactics.  
Users should:

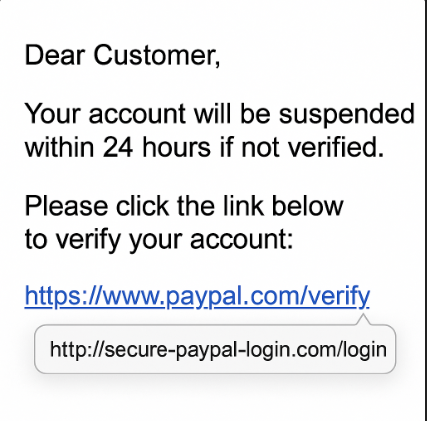
* Not click on links or download attachments.
* Report to the real service provider.
* Delete the email immediately.

**6. Screenshots (Suggested for GitHub Repo)**

* Screenshot of header analysis tool output.



* Screenshot of hovering over suspicious link.



* Screenshot of attachment file type warning.

