CYBER SECURITY INTERNSHIP REPORT

Task 2: Phishing Email Analysis

Name: Rakshitha Gurthuri
Organization: Elevate Labs
Date: 14-02-2026

GitHub Repository: https://github.com/Rakshithapatel/phishing-email-analysis

1. Objective

To identify phishing characteristics in a suspicious email sample using content analysis and email header examination techniques.

2. Tools Used

- Email client / Saved email text file
- Free online email header analyzer

3. Phishing Indicators Identified

- Typosquatting domain (e.g., paypa1-security.com)
- Urgent and threatening language to create panic
- Generic greeting (Dear Customer)
- Suspicious hyperlink redirecting to non-official website
- Request for sensitive information (account verification details)
- SPF, DKIM, and DMARC authentication failures
- Mismatch between sender domain and originating IP address

4. Risk Assessment

Threat	Impact	Risk Level
Credential Theft	Account takeover	High
Financial Fraud	Unauthorized transactions	High
Identity Theft	Personal data misuse	Medium

5. Outcome

This task enhanced awareness of phishing tactics and strengthened practical email threat analysis skills. It improved the ability to detect domain spoofing, analyze email authentication results, identify malicious links, and assess cybersecurity risks effectively.

6. Screenshots (Evidence)

Screenshot 1: Suspicious Email Sample (Insert Screenshot Here)

Screenshot 2: Email Header Analysis Result (Insert Screenshot Here)

Screenshot 3: SPF/DKIM/DMARC Authentication Result (Insert Screenshot Here)