Phishing Email Analysis Report

Task 2 – Cyber Security Internship

1. Introduction

This report analyzes a fabricated PayPal-style phishing email (full headers included in sample- email.txt). The objective is to identify phishing indicators using header analysis, body inspection, and provide remediation recommendations.

2. Email Details

Sample used: PayPal look-alike credential-phishing email (fabricated for training). Subject: Important: Account Verification Required
From (display): PayPal <alerts@paypal-security.com> To: Palaksh <victim@example.com>
Date: Mon, 22 Sep 2025 10:14:58 +0000
Originating host (from headers): mailout.hosting-provider.info (IP 198.51.100.45)

3. Header Analysis (using MXToolbox - simulated output)

I pasted the raw headers (from sample-email.txt) into MXToolbox Email Header Analyzer. The results below reflect the analyzer output for those headers.
=== MXToolbox - Email Header Analyzer (simulated) ===
Received path: mail.example.com <- mailout.hosting-provider.info [198.51.100.45]
SPF Check: FAIL - domain 'paypal-security.com' is not authorized to send from IP 198.51.100.45. DKIM Check: NONE - No DKIM signature found in the message headers (dkim=none).
DMARC Check: FAIL - DMARC policy not met; alignment fails. (dmarc=fail)
Message-ID / Return-Path: Message-ID domain: mailout.hosting-provider.info; Return-Path domain: paypal-security.com (not paypal.com).
Originating IP: 198.51.100.45 - belongs to a generic hosting provider, not PayPal.
Conclusion: Multiple authentication failures (SPF=fail, DKIM=none, DMARC=fail), inconsistent message-id/return-path, and originating IP belonging to a generic hosting provider strongly indicate a forged/suspicious email (phishing).

4. Body Analysis

Key findings from examining the email body:

- Urgent language: 'verify within 24 hours or your account will be suspended' — creates pressure to act immediately.
- Deceptive link: Anchor text 'Click here to verify your account' points to a look-alike domain 'secure-paypal.verify-account.com' instead of paypal.com.
- Branding: Uses visual PayPal logo to appear legitimate, but technical signals contradict authenticity.
- Social engineering elements: Fear and urgency combined with a one-click call-to-action for credential entry.

5. Phishing Indicators Summary

- Spoofed sender domain: alerts@paypal-security.com (not paypal.com)
- SPF/DKIM/DMARC authentication: SPF=FAIL, DKIM=NONE, DMARC=FAIL
- Originating IP does not belong to vendor: 198.51.100.45 (generic hosting provider)
- Look-alike / mismatched URL: secure-paypal.verify-account.com instead of paypal.com
- Urgency / fear tactics: 24-hour suspension threat
- Message-ID / headers inconsistent: Message-ID from mailout.hosting-provider.info

6. Recommendations

Steps to mitigate and respond to such phishing attempts:

- Do NOT click links or call phone numbers included in suspicious emails.
- Verify account issues by typing the vendor's official URL (e.g., paypal.com)

or using official apps.

- Report the phishing email to the vendor's abuse team (e.g., phishing@paypal.com) and to your

email provider.

- Block the sender domain and add spam filtering rules for the originating IP if recurring.
- Provide user training: teach hover-to-check URLs and basic header checks.

7. Repository Contents

phishing-email-analysis/ contains:

- README.md (project overview and instructions)
- Phishing-Analysis.pdf (this document)
- sample-email.txt (raw headers and HTML body of fabricated sample)

-screenshot