**TASK\_2**

**Phishing email analysis report**

1. Email Sample Information

Subject: Urgent: Your Account Will Be Locked in 24 Hours

Sender Name: PayPal Support

Sender Email: support@paypall.com

Date Received: May 25, 2025

Attachment(s): Invoice\_Receipt.pdf

Header Analyzer Used: MXToolbox Email Header Analyzer

2. Phishing Indicators Identified

A. Spoofed Sender Email Address

Observed: support@paypall.com

Issue: This email closely mimics the official PayPal domain. The extra "l" in paypall.com is a common typo-squatting trick.

Phishing Indicator: Domain spoofing to deceive users into thinking it's legitimate.

B. Email Header Discrepancies

Findings from Header Analyzer:

SPF check: Fail

DKIM: Missing

Return-Path: noreply@unknownhost.ru

Phishing Indicator: Authentication failures and suspicious return-path indicate the email may be forged or sent from a malicious server.

C. Suspicious Links

Displayed URL: https://www.paypal.com/verify

Actual URL (hovered): http://secure-paypall.loginverify.ru

Phishing Indicator: Mismatched and misleading links redirect to an unrelated and suspicious domain.

D. Urgent or Threatening Language

Email Body Excerpt:

> “Your account will be permanently suspended in the next 24 hours unless you verify your identity. Click below immediately to avoid loss of access.”

Phishing Indicator: Creates a sense of urgency to provoke quick action without scrutiny.

E. Spelling and Grammar Errors

Examples Found:

“permanently suspensed” (should be suspended)

“Click hear to verify” (should be here)

Phishing Indicator: Legitimate companies usually avoid basic errors, which are common in phishing messages.

F. Suspicious Attachment

Filename: Invoice\_Receipt.pdf

Observation: Unsolicited invoice without prior transaction history; potential to contain malicious macros or links.

Phishing Indicator: Attachments disguised as invoices or receipts are common phishing vectors.

3. Summary of Phishing Traits

Indicator Status

Spoofed Sender Address ✅ Present

Header Authentication Failure ✅ Present

Mismatched or Malicious URLs ✅ Present

Urgent/Threatening Language ✅ Present

Spelling/Grammar Errors ✅ Present

Suspicious Attachment ✅ Present

4. Conclusion

This email exhibits multiple phishing indicators, including a spoofed sender domain, failed authentication headers, mismatched URLs, threatening language, and suspicious attachments. It should be classified as a phishing attempt and reported to the appropriate security team or email provider.

Example:

Subject: Urgent: Your PayPal Account Has Been Limited

From: PayPal Support <support@secure-paypal-alert.com>

Body:

Dear Customer,

We noticed unusual activity in your PayPal account and have temporarily limited your access for your protection.

To restore your account, please verify your identity by clicking the secure link below:

**Verify Now**

If you do not respond within 24 hours, your account will be permanently suspended.

Thank you for your prompt attention to this matter.

Sincerely,

PayPal Security Team

🔍 Key Red Flags:

Generic greeting ("Dear Customer" instead of your name).

Urgent language designed to create panic ("account will be suspended").

Suspicious sender domain (secure-paypal-alert.com instead of paypal.com).

Fake link (disguised as "Verify Now" but points to a non-PayPal domain).

Threats of consequences to pressure immediate action.