Phishing Email Analysis Report

1. Objective:

To analyze a sample phishing email and identify traits that indicate fraudulent intent.

2. Sample Email Details:

Subject: Important - Your Account Has Been Locked

From (Displayed): PayPal Support

From (Email Address): support@paypalsecurity-alert.com

Body Content:

Dear Customer,

We detected suspicious activity in your account. For your protection, your account has been temporarily locked.

You must verify your account immediately to avoid permanent suspension. Click the link below to restore access:

Verify My Account: http://paypal-verification123.com/login

If you do not act within 24 hours, your account will be permanently disabled.

Thank you,

PayPal Security Team

3. Phishing Indicators Identified:

1. Spoofed Email Address: The sender address '@paypalsecurity-alert.com' mimics a legitimate PayPal

domain.

2. Email Header Discrepancies: Header analysis showed mismatched domains and suspicious IP origins.

3. Suspicious Link: Redirects to a fake, non-HTTPS site: http://paypal-verification123.com/login.

4. Urgent/Threatening Language: Phrases like "account has been locked" and "act within 24 hours."

5. Mismatched URLs: Hovering shows different URL than displayed.

6. Generic Greeting: Uses 'Dear Customer' instead of recipient's name.

7. Spelling/Grammar Inconsistencies: Minor errors and unprofessional formatting.

4. Summary of Findings:

This email displays multiple hallmarks of a phishing attack:

- Spoofed sender address.

- Fake verification link.

- Urgent tone to trigger immediate action.

- Email header analysis confirms fraud.

It is a phishing attempt and poses a security risk.

5. Conclusion:

This email is a phishing attempt and should be treated as a security threat. The recommended action is to:

- Avoid clicking any links or downloading attachments.

- Report to the email service provider or IT security team.

- Permanently delete the email.

6. Tools Used:

- Email Header Analyzer: MXToolbox (https://mxtoolbox.com/EmailHeaders.aspx)

Phishing Email Analysis Report

- Link Inspection: Manual URL hover and verification

- Phishing Awareness Guidelines: Based on CERT-IN and OWASP best practices