Final Report – Phishing Indicators Identified (PayPal Sample)

1. Introduction

This report summarizes the findings from the analysis of a phishing email impersonating PayPal. The investigation included sender verification, email header authentication checks, link inspection, urgency detection, formatting review, and social engineering analysis. The email was confirmed to be malicious and intended to steal PayPal login credentials.

2. Summary of Email Content

The email claims that unusual login activity was detected on the user's PayPal account and states that the account has been temporarily limited. It urges the user to verify their identity immediately using a provided link. A fake case ID is included to make the email appear legitimate.

3. Phishing Indicators Identified

A. Sender-Based Indicators

- Spoofed sender email: alert@paypalsecure-notice.com

- Fake "secure-notice" domain not owned by PayPal

- Reply-To mismatch (noreply@paypal.com)

- Not aligned with official PayPal sender addresses

B. Email Header Indicators

- SPF softfail (unauthorized server)

- DKIM missing (no digital signature)

- DMARC fail (domain rejects message)

- Sending IP 91.212.89.44 belongs to untrusted foreign VPS hosting

- No reverse DNS entry, marking untrustworthy mail routing

C. Malicious Link Indicators

Displayed text: "Verify Your Account Now"

Actual link: http://paypa1-verification-center.com/login

- Lookalike domain ("paypa1" instead of "paypal")

- HTTP instead of HTTPS

- Links to credential-harvesting phishing site

- Not owned by PayPal

D. Fake Case ID / Social Engineering

- “Case ID: PP-498124” used to fake legitimacy

- No official format followed

- No attachment provided, but psychological manipulation used

E. Urgency & Threat-Based Indicators

- Claims “unusual login activity”

- “Account temporarily limited”

- 12-hour deadline

- Threats of permanent restriction

- Subject includes “Urgent”

F. Grammar & Formatting Issues

- Generic greeting: “Dear Customer”

- Unprofessional formatting

- Missing PayPal branding elements

- Fake sign-off: “PayPal Security Team”

4. Conclusion

The analyzed email displays all major signs of phishing including sender spoofing, authentication failures, malicious links, urgency tactics, formatting errors, and URL deception. It is clearly a phishing attempt aimed at stealing PayPal credentials. The email must be treated as malicious and reported immediately.