# Phishing Email Analysis Report

Objective:

Analyze a suspicious email and identify phishing characteristics.

Sample Email:

Subject: Urgent! Your account will be suspended

from: support@paypa1-security.com

Body:

Dear user, your PayPal account has been compromised. Please verify your account immediately by

clicking http://paypal1security.com/verify

Failure to do so will result in suspension.

Analysis Steps:

1. Sender Email Address:

Fake domain detected: paypa1-security.com (uses '1' instead of 'l').

2. Email Headers:

SPF/DKIM failed; IP originates from unknown location.

3. Suspicious Links or Attachments:

Link: http://paypal-security.com/verify (not official PayPal domain).

4. Urgent or Threatening Language:

Phrases like 'urgent', 'your account will be suspended'.

5. Mismatched URLs:

Display text says 'PayPal Verification', actual link goes to malicious site.

6. Spelling or Grammar Errors:

Minor errors: 'your account will be suspend'.

Summary of Phishing Traits: - Fake sender domain. - Urgent tone. - Suspicious link redirecting to non-official site. - SPF/DKIM failure. - Grammar mistakes.

Conclusion:

This email is a classic phishing attempt aiming to steal credentials by creating urgency and using a fake

Domain.