Phishing Email Analysis Report

1. Introduction

Name: Suman Paul

Task: Phishing Email Analysis

Date: 25-06-2025

This report analyzes a sample phishing email and identifies common phishing traits used to deceive users and compromise security.

2. Sample Phishing Email

Sample Email (Simulated):

From: security@paypa1.com

To: sumanpaul210040@gmail.com

Subject: Urgent: Suspicious Activity Detected in Your Account

Dear Customer,

We noticed suspicious activity in your account. For your safety, please login using the link below to verify your identity: https://paypal-security-login.com/verify

Failure to act within 24 hours will result in account suspension.

Thank you,

PayPal Security Team

Phishing Email Analysis Report

3. Identified Phishing Indicators

Phishing Indicators Identified:

1.Sender's email uses spoofed domain: "paypa1.com" (not official).

2.Urgent and threatening language: "act within 24 hours or account will be suspended".

3.Suspicious URL: Hover reveals non-PayPal link.

4.Generic greeting: "Dear Customer" instead of name.

5.Slight grammar inconsistencies.

6.Domain mismatch between visible and actual link.

7.Fake sense of urgency to trigger impulsive action.

4. Email Header Analysis

Header Analysis (Simulated):

- Received path shows irregular mail servers.
- SPF and DKIM fail (indicates spoofing).
- Return-path domain mismatch.

Used Tool: Google Admin Toolbox Messageheader tool.

5. Conclusion

Conclusion:

The email displays clear signs of phishing through email spoofing, urgency, link obfuscation, and social engineering.

Phishing Email Analysis Report

Users should avoid clicking unknown links, always verify sender details, and report suspicious messages.