Phishing Email Analysis Report

Prepared By: Vignesh

Role: Cybersecurity Analyst (Entry-Level)

Certification: Google Cybersecurity Professional Certificate

Date: 07-Dec-2025

1. Executive Summary:

- This report analyzes a phishing email that impersonates PayPal in an attempt to deceive users into disclosing their login credentials. Indicators of compromise, attack techniques, impact, and mitigation steps are documented below.

2. Phishing Email Content:

From: support@paypa1.com

Subject: Urgent: Verify Your Account

Dear user,

Your PayPal account has been temporarily limited due to suspicious activity.

Please verify your account immediately to avoid closure.

Click below to verify:

http://paypa1-security-check.com/login

Regards,

PayPal Support

3. Indicators of Compromise (IOC):

- Sender domain uses typo: paypa1.com instead of paypal.com
- Urgent language designed to create panic
- Suspicious link (HTTP instead of HTTPS)
- Link domain unrelated to PayPal
- Fake threat of account closure

4. Attack Techniques:

- Technique: Social engineering via phishing
- Goal: Credential harvesting
- Methods:
    - Brand impersonation
    - Fear-based messaging
    - Malicious URL

5. Impact:

- Victims may disclose PayPal login credentials, leading to financial loss, identity theft, and unauthorized transactions.

6. Recommendations:

1. Verify sender address before taking action
2. Avoid clicking unknown links
3. Check for HTTPS and valid certificates
4. Enable multi-factor authentication
5. Report phishing emails to provider
6. Educate users about phishing techniques

7. Conclusion:

- The analyzed email is a phishing attempt designed to steal user credentials through social engineering. Security awareness and technical controls are essential to mitigate the risk of such attacks.