Phishing Email Analysis Report

Internship Task: Cybersecurity – Phishing Email Analysis

Date: 24 September 2025

Submitted by: Lokesh M

# 1. Objective

The purpose of this task is to analyze a suspicious email to identify phishing characteristics, email spoofing, malicious links, and social engineering tactics. The goal is to improve awareness of email-based threats and develop threat detection skills.

# 2. Sample Email

From: support@paypall.com  
To: user@example.com  
Subject: Urgent: Your Account Will Be Suspended  
Date: Mon, 23 Sep 2025 10:45:00 +0000  
  
Dear Customer,  
  
We have detected unusual activity on your PayPal account.   
To avoid permanent suspension, please verify your account immediately by clicking the link below:  
  
http://www.paypa1-login-secure.com/verify  
  
Failure to do so within 24 hours will result in account termination.  
  
Thank you for your prompt attention.  
  
Sincerely,  
PayPal Security Team

# 3. Analysis of Phishing Indicators

|  |  |  |
| --- | --- | --- |
| Indicator | Observation | Explanation |
| Suspicious Sender | support@paypall.com | Extra “l” in the domain; attacker is spoofing a legitimate sender. |
| Header Discrepancy | Return-Path: scammer@evil.com | The email was not sent from the official domain; spoofing is evident. |
| Fake URL | http://www.paypa1-login-secure.com/verify | The URL contains a number instead of the letter “l” and is not official. |
| Urgency / Threat | “Failure to do so within 24 hours” | Creates fear and pressure to act quickly – social engineering tactic. |
| Social Engineering | Fear of account suspension | Exploits trust and anxiety to trick the user into revealing credentials. |
| Grammar / Spelling Errors | Typo in domain (“paypall.com”) | Phishing emails often contain spelling or formatting errors. |

# 4. Tools Used

- Email client (for inspecting email content)  
- Manual link inspection (hover over links to verify URL)  
- Optional: Free online email header analyzer (MXToolbox, Google Message Header Analyzer)

# 5. Recommended Actions

1. Do not click on any links or download attachments.  
2. Report the email to the IT/security team.  
3. Delete or quarantine the email.  
4. If any credentials were entered, immediately change the password on the real service.

# 6. Outcome / Learning

- Learned to identify phishing emails and suspicious senders.  
- Understood the importance of checking email headers for spoofing.  
- Gained awareness of malicious links, urgency tactics, and social engineering techniques.  
- Developed skills to safely analyze and report phishing threats.