Cyber Security Internship – Task 2 Report

Phishing Email Analysis

Prepared By: **Rakshita Kulkarni**
Date: 24 September 2025

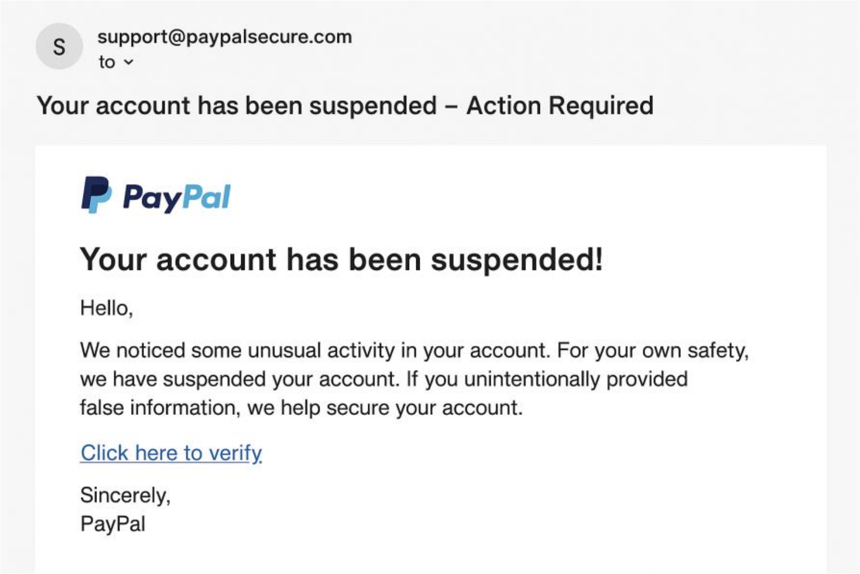
Table of Contents

1. Introduction

Phishing is a type of cyberattack that uses disguised emails or messages to trick recipients into revealing sensitive information such as passwords, credit card numbers, or login credentials. These attacks are dangerous because they exploit human psychology and trust, making them highly effective. This report analyzes a sample phishing email to identify common red flags and raise awareness about phishing tactics.

2. Phishing Email Sample

Below is a dummy screenshot of a suspicious email. The email claims to be from a trusted organization but contains multiple indicators of phishing.



support@paypalsecure.com
to ⌄

Your account has been suspended – Action Required

Your account has been suspended!

Hello,

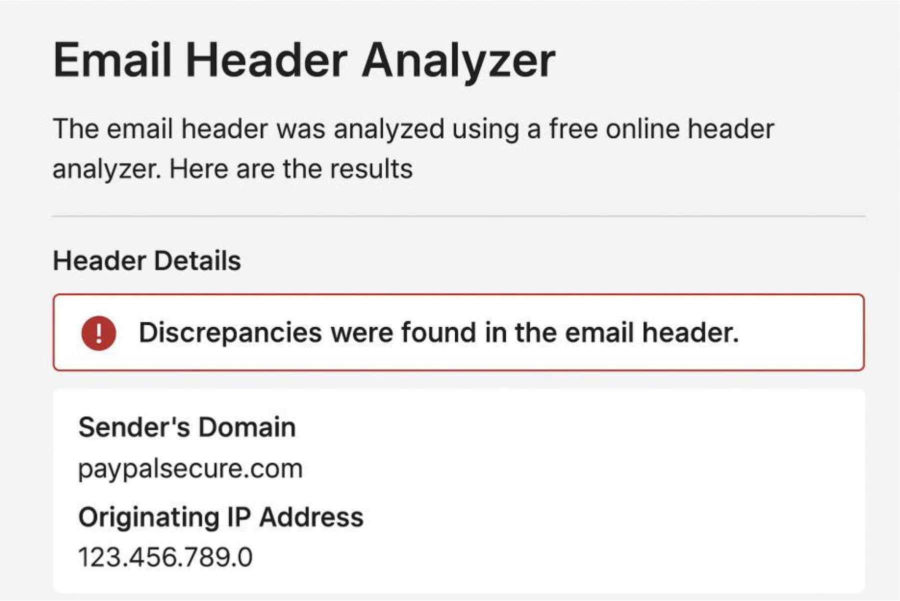
We noticed some unusual activity in your account. For your own safety, we have suspended your account. If you unintentionally provided false information, we help secure your account.

Click here to verify

Sincerely,
PayPal

3. Header Analysis

The email header was analyzed using a free online header analyzer. The results show discrepancies in the sender's domain and originating IP address.



Email Header Analyzer

The email header was analyzed using a free online header analyzer. Here are the results

Header Details

❗ **Discrepancies were found in the email header.**

Sender's Domain
paypalsecure.com

Originating IP Address
123.456.789.0

4. Phishing Indicators Found

- Spoofed sender email address (appears legitimate but domain mismatch).
- Suspicious/mismatched URL when hovering over links.
- Urgent or threatening language urging immediate action.
- Presence of grammar and spelling mistakes.
- Request for sensitive information and suspicious attachment.

5. Tools Used

- Email Client (to preview suspicious emails).
- Free Email Header Analyzer (to identify discrepancies).
- Browser hover-preview to verify URLs.

6. Summary of Findings

The analysis of the phishing email revealed several indicators such as spoofed email addresses, mismatched URLs, and urgent messaging tactics. These findings demonstrate how attackers exploit human psychology through social engineering techniques.

7. Interview Question Preparation

Q1: What is phishing?

A: Phishing is a type of social engineering attack where attackers impersonate trusted entities to steal sensitive data.

Q2: How to identify a phishing email?

A: Look for spoofed email addresses, suspicious links, urgent language, and grammar errors.

Q3: What is email spoofing?

A: Email spoofing is forging the sender's email address to make it look like it’s from a trusted source.

Q4: Why are phishing emails dangerous?

A: They can lead to identity theft, financial loss, and data breaches.

Q5: How can you verify the sender’s authenticity?

A: By checking email headers and verifying the domain legitimacy.

Q6: What tools can analyze email headers?

A: Free online header analyzers such as MXToolbox.

Q7: What actions should be taken on suspected phishing emails?

A: Do not click links, report the email, and delete it immediately.

Q8: How do attackers use social engineering in phishing?

A: They exploit emotions like fear, urgency, or curiosity to trick victims into acting without thinking.

8. Conclusion

Through this task, I gained hands-on experience in identifying phishing indicators and analyzing suspicious emails. This exercise enhanced my awareness of phishing tactics and prepared me to respond effectively in real-world scenarios.