Phishing Email Analysis Report

Name: Adil
Internship: Cyber Security Internship
Task: Task 11 – Phishing Email Analysis
Date: *(Add submission date)*
Operating System: Windows / Linux
Tools Used: Email Client, Web Browser, Manual Analysis

1. Objective

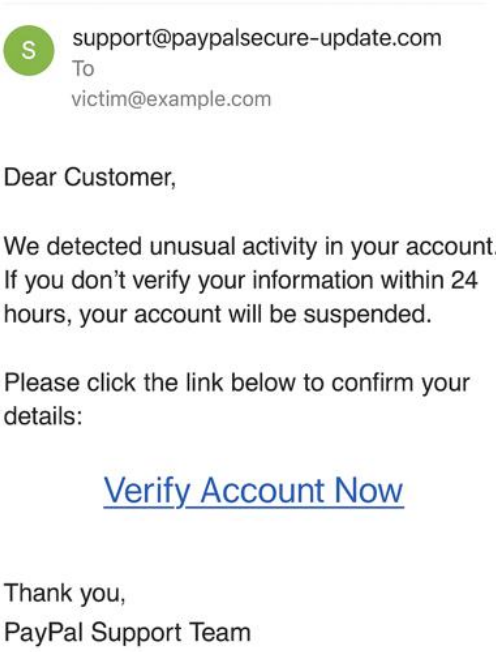
The objective of this task is to analyze a suspicious email and identify common phishing indicators. This task helps in understanding how attackers use social engineering techniques to trick users into revealing sensitive information such as login credentials and financial details.

2. Email Overview

The analyzed email claims to be sent from **PayPal Support Team** and warns the user about "unusual activity" in their account. The email pressures the user to verify their account within 24 hours, otherwise the account will be suspended.

This type of message is commonly used in phishing attacks to create fear and urgency.

Screenshot 1: Phishing email content



3. Suspicious Sender Analysis

- **Sender Email Address:** support@paypalsecure-update.com
- This email address does **not belong to PayPal's official domain** (paypal.com).
- Attackers often use domains that look similar to trusted brands to deceive users.

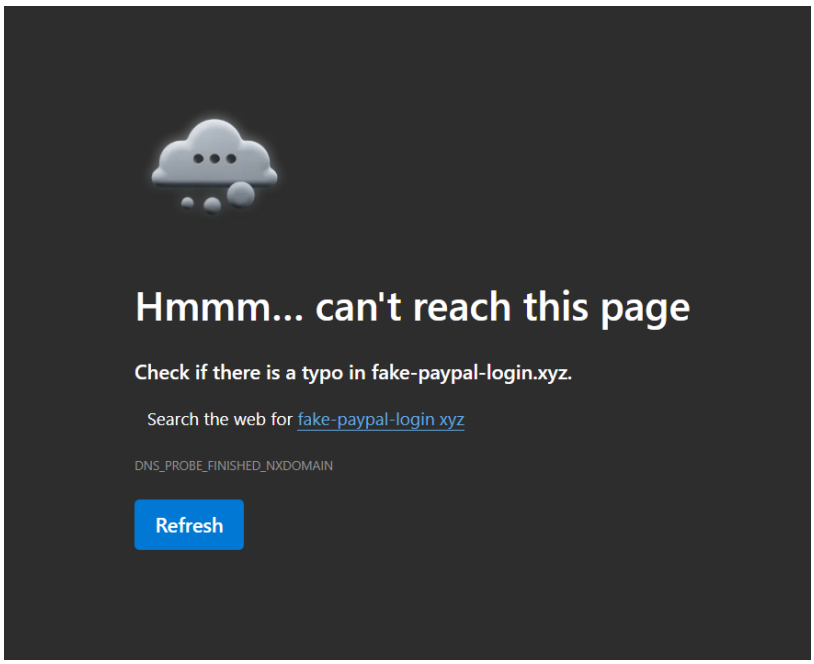
Red Flag: Legitimate PayPal emails are only sent from official PayPal domains.

4. Suspicious Link Analysis

- The email contains a clickable link labeled **"Verify Account Now"**.
- On interaction, the link redirects to: fake-paypal-login.xyz
- The domain fails to load and results in a **DNS error**, confirming it is **not a legitimate PayPal website**.

Red Flag: Legitimate companies never ask users to verify accounts through unknown domains.

Screenshot 3: Suspicious link leading to a fake domain



5. Social Engineering Techniques Used

The phishing email uses the following techniques:

- **Urgency:** “Verify within 24 hours”
- **Fear:** “Your account will be suspended”
- **Impersonation:** Pretending to be PayPal Support
- **Call to Action:** Encouraging the user to click a link

These techniques are designed to manipulate users into acting quickly without verifying authenticity.

6. Indicators of Phishing

Indicator	Observation
Fake sender domain	✔ Present
Urgent language	✔ Present
Suspicious link	✔ Present
Generic greeting	✔ “Dear Customer”
No personalization	✔ Present

7. Impact of Clicking the Link

If the user had entered credentials on the fake website:

- PayPal login details could be stolen
- Financial fraud could occur
- Account takeover could happen
- Identity theft risk increases

8. Prevention & Best Practices

- Always verify sender email addresses
- Do not click suspicious links in emails

- Hover over links before clicking
- Access accounts by typing the official website URL manually
- Enable Multi-Factor Authentication (MFA)
- Report phishing emails to the organization

9. Conclusion

This task successfully demonstrated how phishing emails attempt to impersonate trusted organizations and exploit human behavior. By analyzing the sender address, message content, and embedded links, it was confirmed that the email is a **phishing attempt**.

Understanding these indicators is essential for protecting personal and organizational data from cyber threats.

10. Learning Outcome

- Learned how to identify phishing emails
- Understood social engineering techniques
- Improved awareness of email-based cyber threats
- Gained hands-on experience in phishing analysis