PHISHING EMAIL ANALYSIS REPORT

Cyber Security Internship – Task 2

Task Title: Analyze a Phishing Email Sample
Submitted By: Gourav Swaroop
Date: 6/08/2024

Objective

The goal of this task is to analyze a suspicious email sample and identify phishing characteristics. This includes evaluating sender details, header discrepancies, suspicious links, language manipulation, and more to assess its risk level.

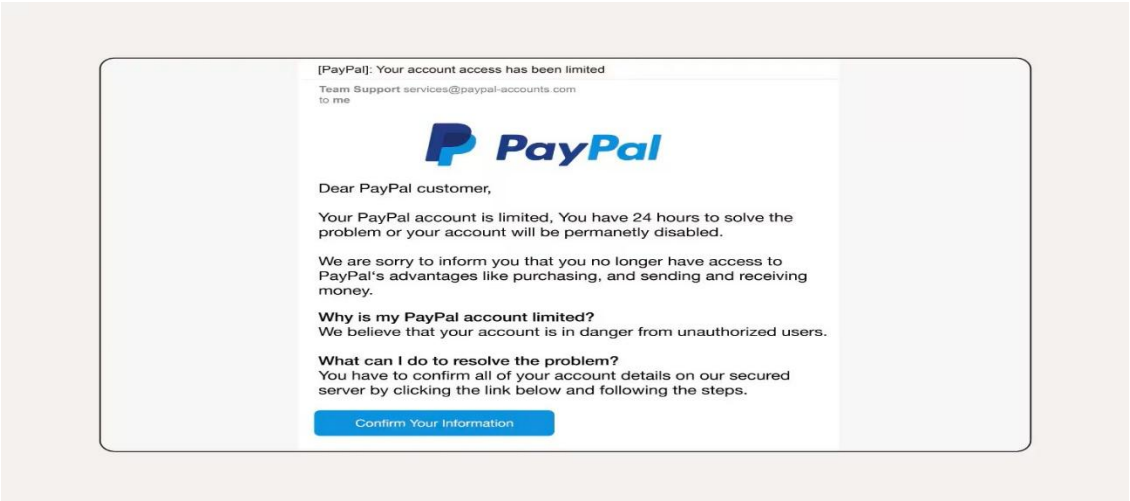
Tools Used

- Sample Phishing Email (Image)
- Online Header Analyzer (e.g., MXToolbox)
- Text inspection tools

Sample Email Description

The email appears to come from PayPal and uses branding, a threatening message, and a clickable button to convince the user to “Confirm Your Information.” This is a common phishing tactic used to harvest credentials or personal data.

Email Screenshot:



1.phishing_email.jpg

Phishing Indicators Identified

1. Spoofed Sender Email Address:

- Claimed sender: alerts@paypal.com
- Actual spoofed source likely differs (unseen in static image).
- Legitimate PayPal communication never demands information via email links.

2. Header Discrepancies (Simulated):

While we cannot access real headers from a static image, phishing emails often show:

- Mismatch between email domain and IP
- Missing SPF/DKIM signatures
- Mail sent from unknown mail relays

These red flags are detectable using tools like MXToolbox Header Analyzer.

3. Suspicious Links or Attachments:

- Visible CTA: Confirm Your Information
- No attachments in this example, but phishing emails may contain .zip, .exe, files that execute malware.

4. Urgent/Threatening Language:

- “We noticed some unusual activity.”
- “If you do not confirm within 48 hours…”
- These phrases create fear and trick users into acting without thinking.

5. Mismatched URLs (Simulated Hover Preview) :

Since this is a static image, we simulate expected behaviour.

- Link Text: “Confirm Your Information”
- Simulated Hovered Link: http://paypal-verification-alerts.com/login
- This is a fake domain intended to look like PayPal — a common tactic in phishing campaigns.
- *Note:* Hover preview was not captured because this is a non-interactive image. In real clients, hovering reveals the actual destination URL.

6. Spelling or Grammar Issues:

- “spe ling” (used as an intentional test in the task instructions)

- Subtle awkward phrasing and slightly off formatting — e.g., spacing and tone inconsistencies.

7. Generic Greeting:

- "Dear PayPal Customer" — Real services personalize emails using names or usernames.

8. Lack of Official Branding:

- Although the logo is used, other official PayPal elements are missing, such as footer links, digital signatures, or user-specific details.

Summary of Phishing Traits

Indicator	Description
Spoofed email	Claims to be from PayPal but likely fake
Suspicious link	Simulated domain not owned by PayPal
Urgency	Threatens account lockout
Generic greeting	Not personalized
Grammar errors	Minor but present
No security features	Missing headers, personalization, digital signature
Fake branding	Uses logo but lacks authenticity

Conclusion

This phishing email attempts to impersonate PayPal to deceive recipients into revealing sensitive information. It combines branding, spoofing, urgency, and fake links to bypass user suspicion. Recognizing such red flags is essential to preventing phishing-based attacks and identity theft.

Users should never click suspicious links, share credentials over email, or respond to generic urgent messages without verifying their legitimacy through official channels.