****

**ELEVATE LABS  
Cyber Security Internship**

**Task 2  
Documetation Report  
Submitted by Suhaila P.S**

**Phishing Email Analysis Report**

**1. Overview**

**Task:** Analyze a phishing email sample to identify common phishing traits and security risks.

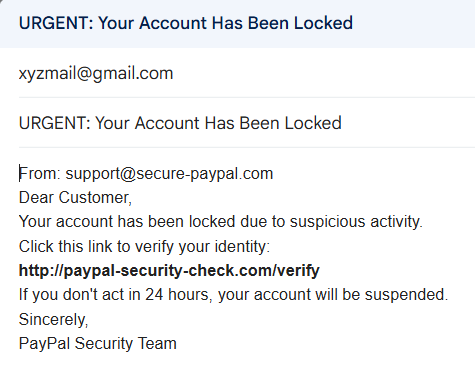
**Date:** 27-05-2025

**Analyst:** Suhaila  
  
  
**2. Email Sample Details**

| **Field** | **Value** |
| --- | --- |
| Subject | URGENT: Your Account Has Been Locked |
| Sender | [support@secure-paypal.com](mailto:support@secure-paypal.com) |
| Received On | [27-05-2025/3:00 PM] |

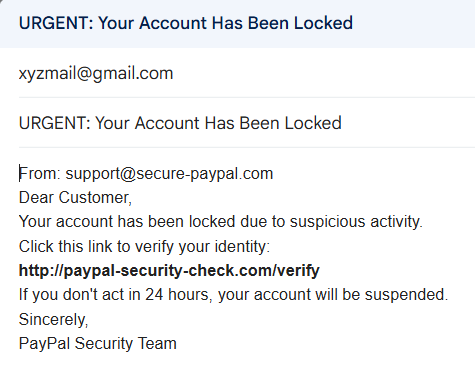
**3. Step-by-Step Analysis**

**Step 1: Email Content**

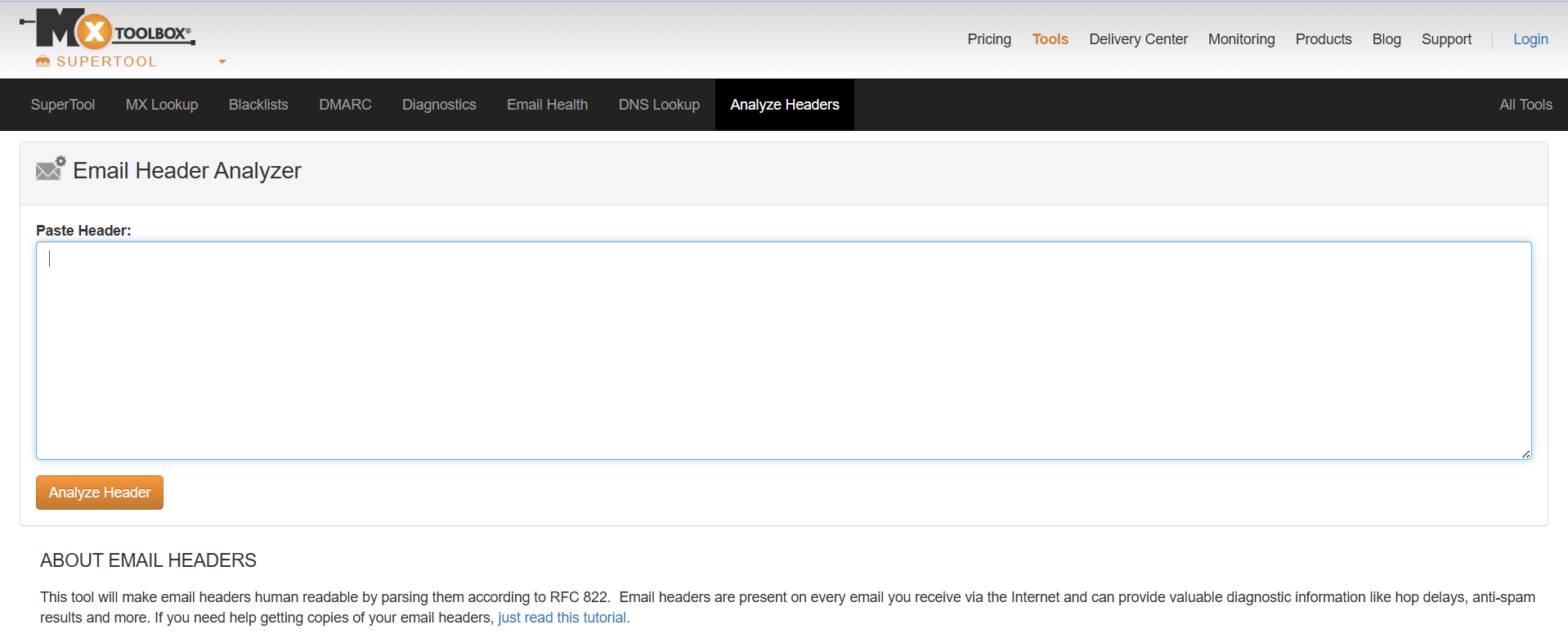
* The email warns about suspicious activity and urges the user to verify their identity by clicking a link.
* The language creates a sense of urgency by threatening permanent account suspension within 24 hours  
  

**Step 2: Sender’s Email Address Analysis**

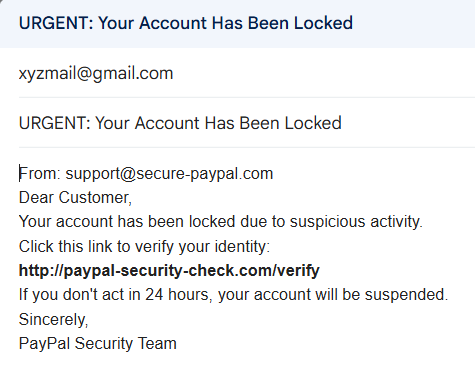
* The sender domain secure-paypal.com is **not** the official PayPal domain (paypal.com).
* This is a common phishing tactic to mimic trusted domains.





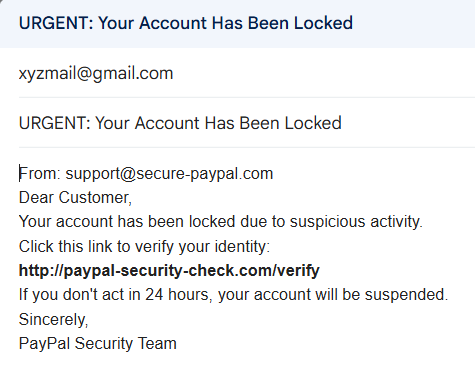
**Step 3: Email Header Analysis :**  
Unable to check real headers since this is a manually created sample.  
In a real scenario, I would use Gmail’s “Show original” and analyze it using MxToolbox Email Header Analyzer to detect spoofing or mismatches.  
  
  
  
The MxToolbox website homepage: For header analysis in real cases.  
  
  
**Step 4: Link and Attachment Analysis**

* The link http://paypal-security-check.com/verify is suspicious and not an official PayPal domain.
* Hovering over the link shows a mismatch between link text and URL.

  
  
**Step 5: Language and Tone**



* Urgent and threatening language is used to create panic.
* Generic greeting "Dear Customer" instead of personalized name.

  
  
**Step 6: Grammar and Spelling Check**



* No major spelling mistakes found.
* Slightly unnatural phrasing to create urgency.

**4. Summary of Findings**

|  |  |
| --- | --- |
| **Indicator** | **Observation** |
| Spoofed Domain | secure-paypal.com instead of paypal.com |
| Suspicious Link | paypal-security-check.com – unofficial URL |
| Urgent/Threatening Tone | “Failure to do so in 24 hours will result in suspension” |
| Generic Greeting | “Dear Customer” |
| Grammar & Spelling | Mostly correct but unnatural phrasing |

**5. Conclusion**

The email is a **phishing attempt** designed to trick recipients into clicking malicious links by mimicking PayPal and using urgent language. Users should avoid interacting with the email and report it to their email provider or security team.

**6. Recommendations**

* Never click on suspicious links or download attachments from unknown sources.
* Verify sender addresses carefully.
* Use email security tools that check SPF, DKIM, and DMARC.
* Educate users to recognize phishing emails.
* Report phishing attempts to IT/security teams immediately.