PHISHING EMAIL ANALYSIS REPORT

# Objective:

Identify phishing characteristics in a suspicious email sample.

# Tools Used:

1. Email client or saved email file (text)

2. Free online email header analyzer (e.g., MXToolbox, Google Admin Toolbox)

# Step-by-Step Procedure:

1. Obtain a phishing email sample.

2. Examine the sender's email address. Check for spelling inconsistencies or suspicious domains.

3. Extract the email header.

4. Paste the header into an online analyzer.

5. Inspect the email content for suspicious links or attachments. Hover over hyperlinks to see their true destination.

6. Look for urgent or threatening language .

7. Identify grammar or spelling errors, which are often signs of phishing.

8. Compile a list of phishing indicators found in the email.

# Sample Phishing Email :

Subject: Immediate Action Required: Suspicious Activity Detected on Your Account

From: security-update@paypai-alerts.com

To: samson@gmail.com

Date: June 25, 2025

Reply-To: support@paypai-helpdesk.com

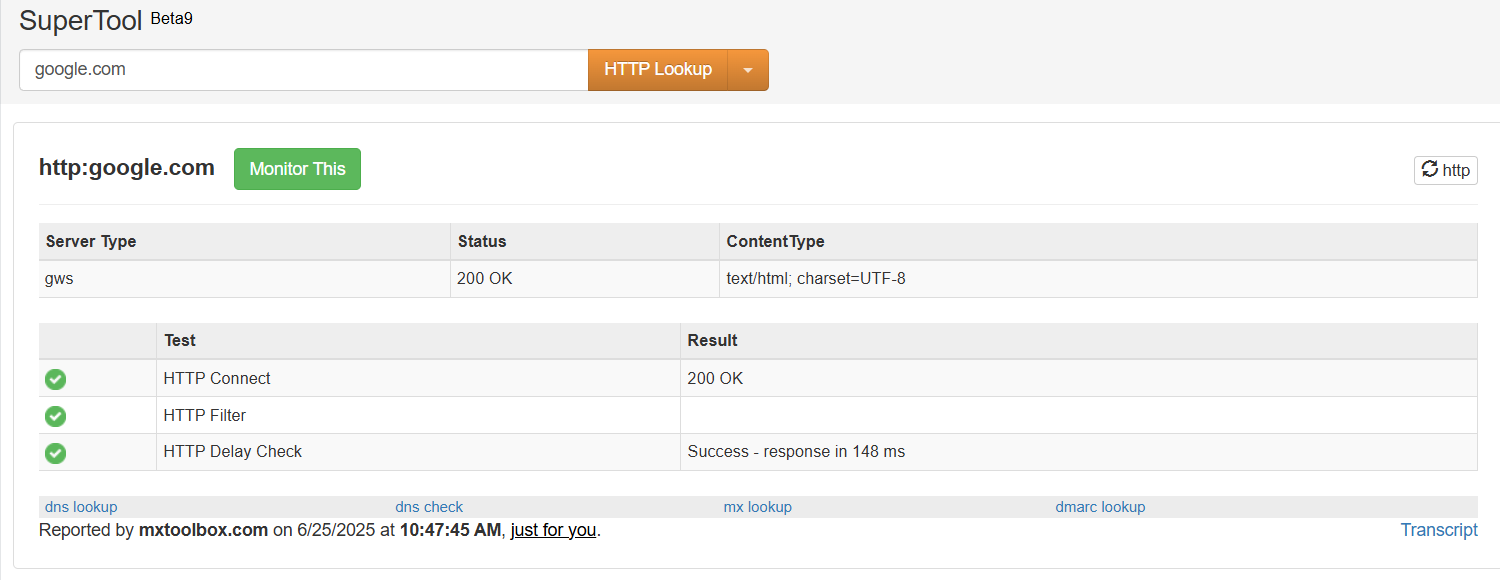
Dear Valued Customer,  
  
We have detected suspicious login attempts on your PayPal account from an unknown location.  
  
To protect your account from unauthorized access, we have temporarily suspended your account.  
  
Please verify your identity immediately to avoid permanent suspension.  
  
Click here to verify your account http://paypai-security-check.com/login  
  
Failure to complete the verification within 24 hours will result in account termination.  
  
Thank you for your prompt attention.  
  
Sincerely,  
PayPal Security Team  
© 2025 PayPal Inc.

# Phishing Indicators Identified:

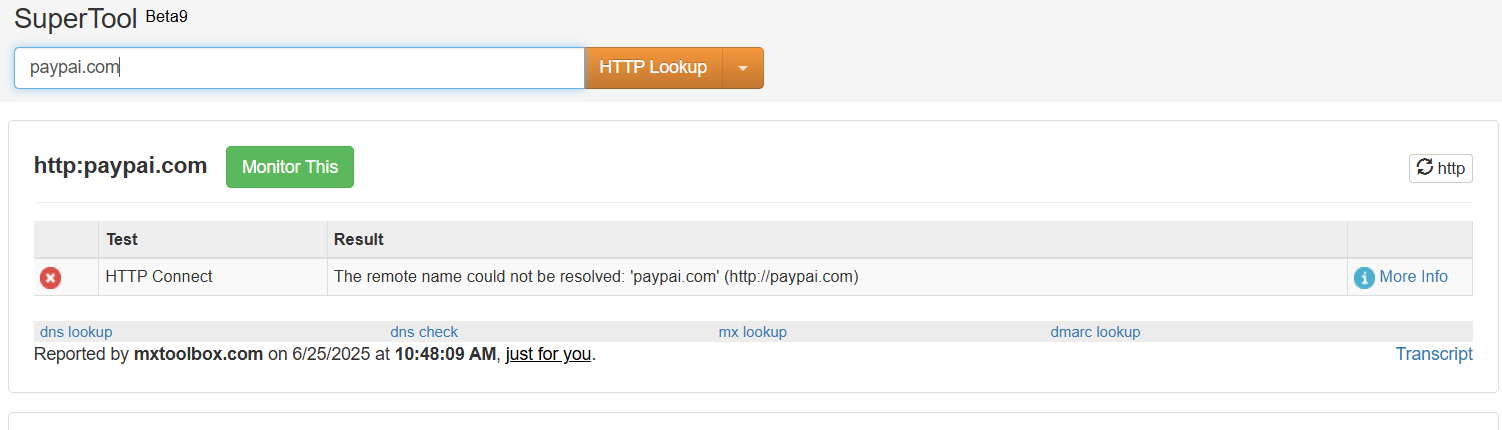
|  |  |
| --- | --- |
| Indicators | Description |
| Spoofed sender | @paypai-alerts.com looks similar to PayPal but is fake |
| Urgent language | Phrases like 'Immediate Action Required' and threats of termination |
| Suspicious link | The displayed link points to a fake domain (paypai-security-check.com) |
| Reply-to mismatch | Reply address is not from official PayPal domain |
| Generic greeting | 'Dear Valued Customer' instead of user’s real name |
| Spelling/grammar issues | 'Paypai' instead of 'PayPal', inconsistent punctuation |

# After analyzing it with MXTool

Result for an actual Domain.



Result for the fake domain.



With this it is clear that the email is a phishing email.

Once the user takes the bait, the attacker can gain all the information he needs to perform various cyber attacks.

The below phishing email is a little difficult to segragate whether it is a phing email or not.

This is because of how well the attackers have seen through the official company emails.

