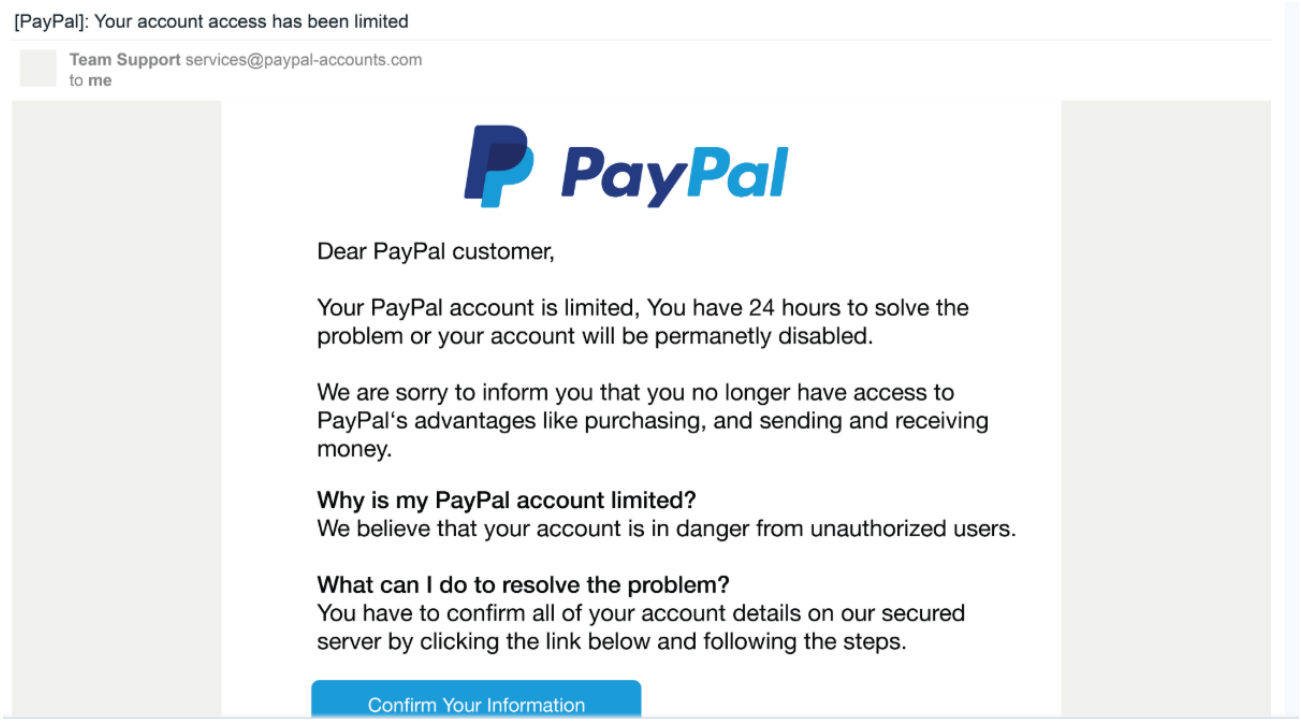
Task 2: Analyze a Phishing Email Sample.

Report

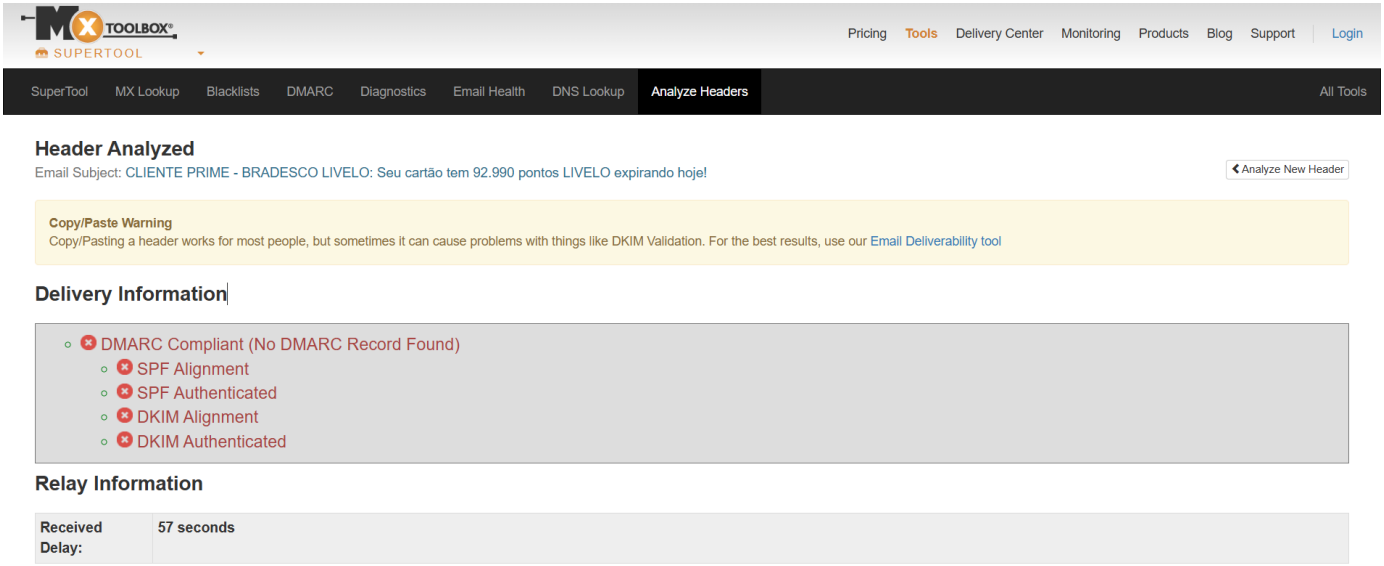
Phishing email example:



1st Indicator: The sender's email is 'services@paypal-account.com', which does not match PayPal's official domain **enquiry @paypal.com** This is a spoofing indicator.

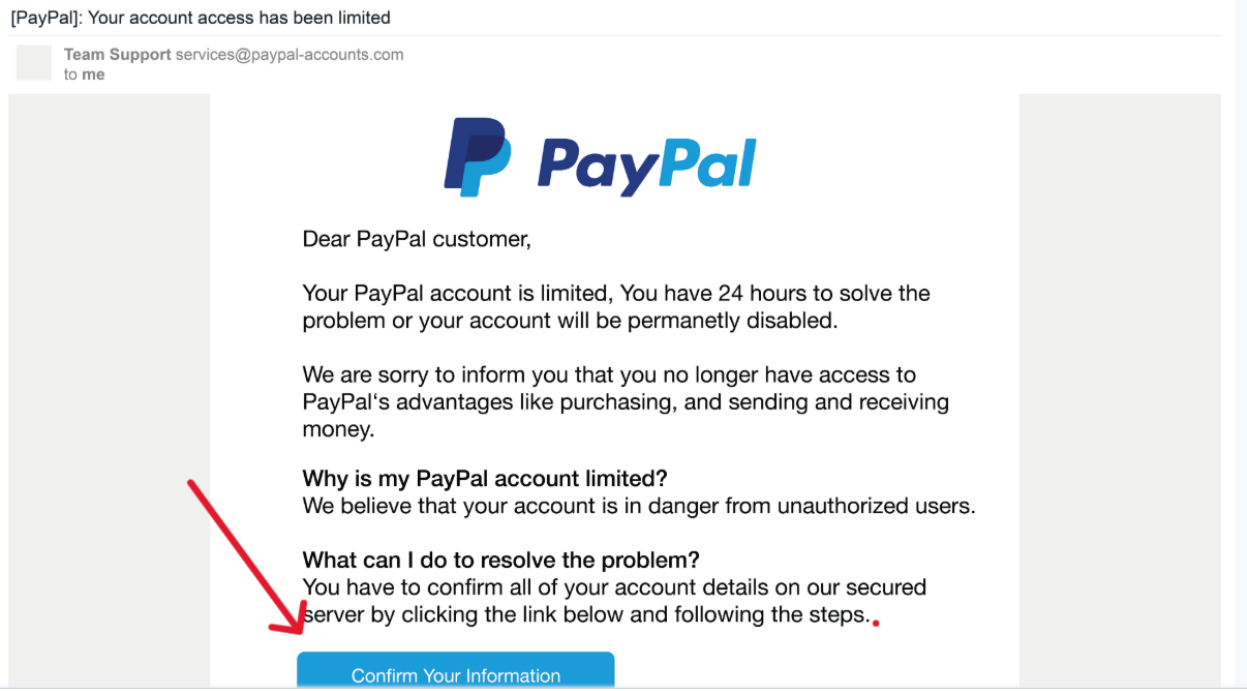
2nd Indicator: Analyzing the email header by using mx analyzer tool

Result:



This shows the failure of SPF, DKIM, DMARC protocols check failed. The Return-Path domain does not match the sender's domain, indicating a spoofed sender.

3rd Indicator: Suspicious Links or Attachments



The link text says, "Confirm your Password," but it points to http://secure-login-paypa1.com. This is a mismatched and misleading URL.

4th Indicator: Check for Urgent or Threatening Language

"We are sorry to inform you that you have no longer access to your account" which is a classic phishing tactic to create urgency.

Summarize All Identified Phishing Indication

Indicator	Description
• Spoofed Email Address	services@paypal-account.com’ pretending to be PayPal.
• Header Discrepancy	SPF and DKIM failed in the header analysis
• Mismatched URL	Visible link points to fake login at secure-login-paypa1.com
• Urgent Language	“Your account will be permanently locked”