

Task 2: Analyze a Phishing Email Sample.

Report

Phishing email example:

[PayPal]: Your account access has been limited

Team Support services@paypal-accounts.com
to me



Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanetly disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

Why is my PayPal account limited?

We believe that your account is in danger from unauthorized users.

What can I do to resolve the problem?

You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

[Confirm Your Information](#)

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:

The screenshot displays the MX Toolbox 'Analyze Headers' tool interface. The header section shows the email subject: 'CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!'. Below this, a 'Copy/Paste Warning' message states: 'Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our [Email Deliverability tool](#)'. The 'Delivery Information' section lists several failed checks, each marked with a red star icon: 'DMARC Compliant (No DMARC Record Found)', 'SPF Alignment', 'SPF Authenticated', 'DKIM Alignment', and 'DKIM Authenticated'. The 'Relay Information' section shows the email was received with a delay of 57 seconds.

Header Analyzed
Email Subject: CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!

Copy/Paste Warning
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our [Email Deliverability tool](#)

Delivery Information

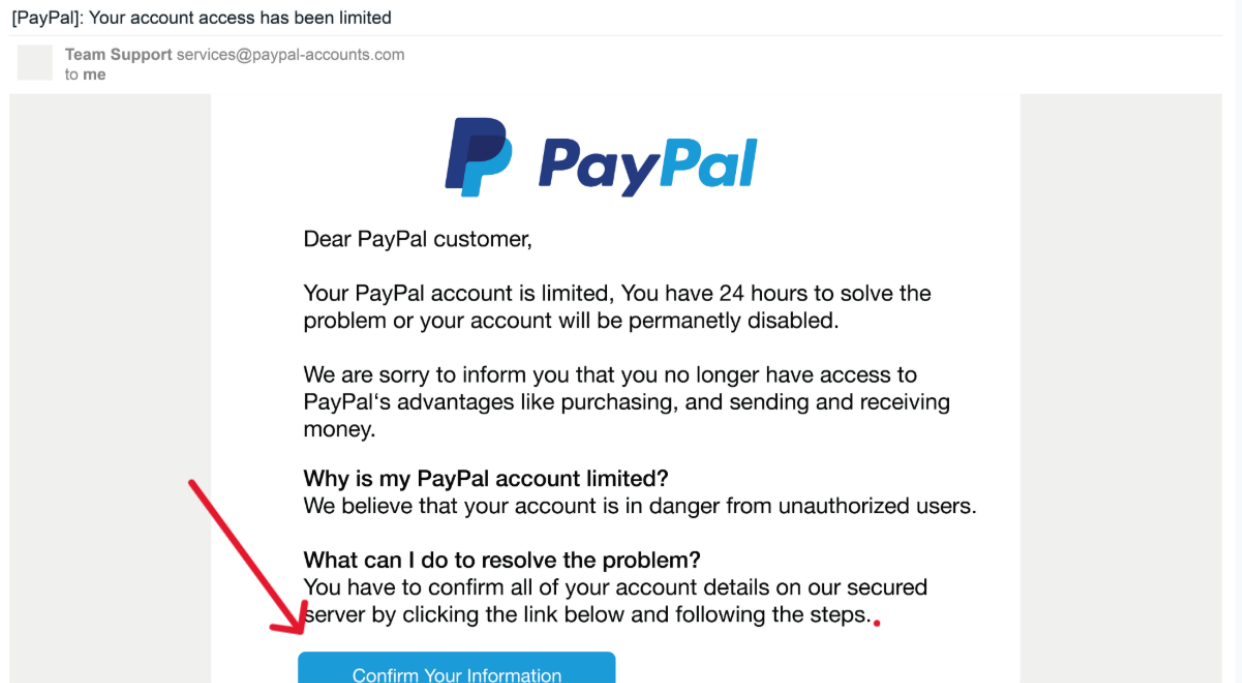
- ✖ DMARC Compliant (No DMARC Record Found)
 - ✖ SPF Alignment
 - ✖ SPF Authenticated
 - ✖ DKIM Alignment
 - ✖ DKIM Authenticated

Relay Information

| | |
|-----------------|------------|
| Received Delay: | 57 seconds |
|-----------------|------------|

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" |