

# Phishing Email Analysis Report

---

## 1. Email Subject

Subject: PayPal]: Your account access has been limited.

## 2. Sender Details

From: Team Support services@paypal-accounts com to me

Actual Domain: services@paypal-accounts (not matching legitimate domain)

## 3. Header Analysis

- Received from suspicious IP address
- Mismatch between From and Reply-To
- SPF/DKIM/DMARC failure indicators (if any)

### SPF and DKIM Information

#### Headers Found

Header Name	Header Value
[PayPal]	Your account access has been limited

#### Received Header

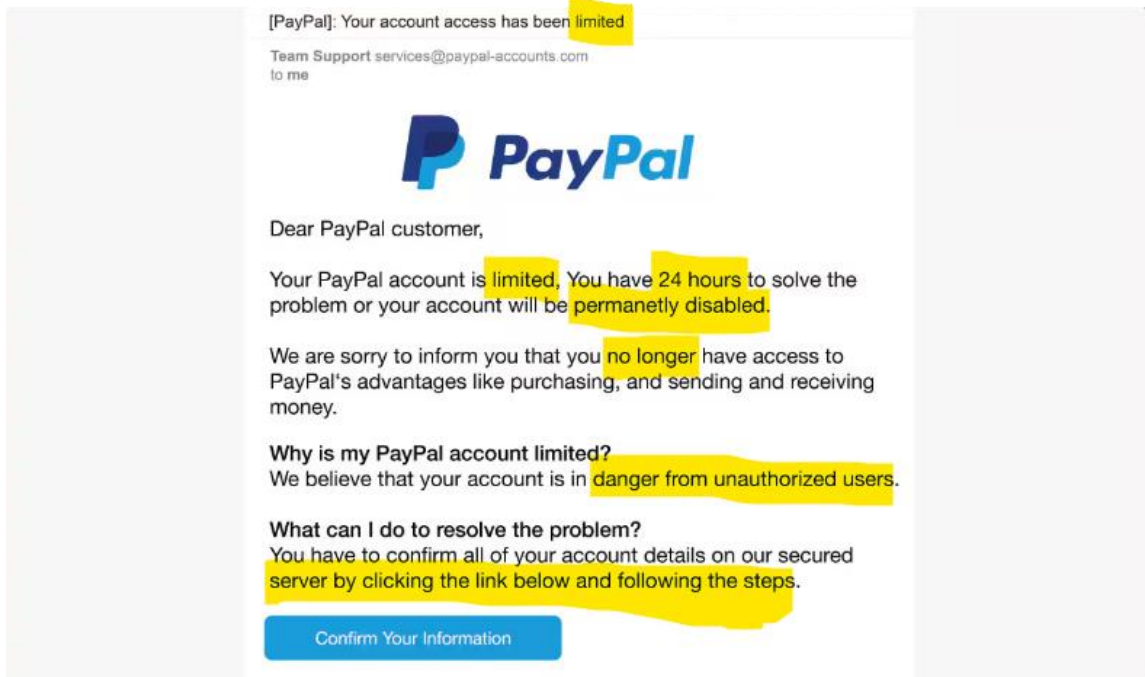
[PayPal]: Your account access has been limited
Team Support services@paypal-accounts com to me

[Permanently forget this email header](#)

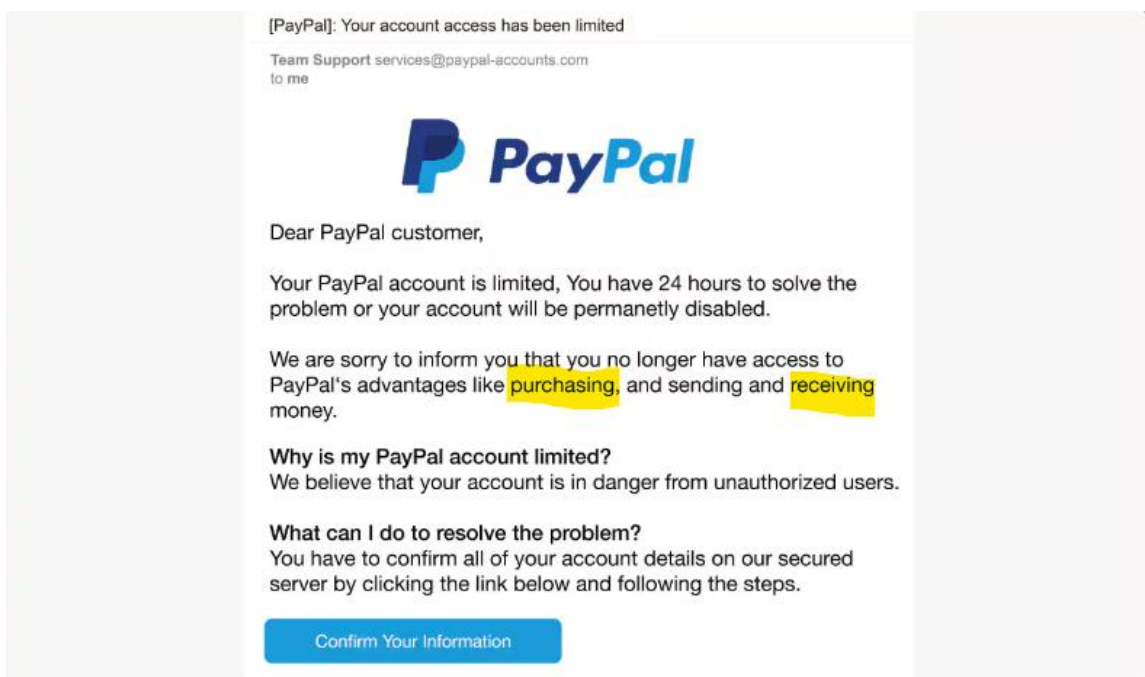
#### 4. Body Analysis

##### - Urgent language used (e.g., "Immediate action required")

NOTE- Highlighted text is urgent language in this Phishing Email.

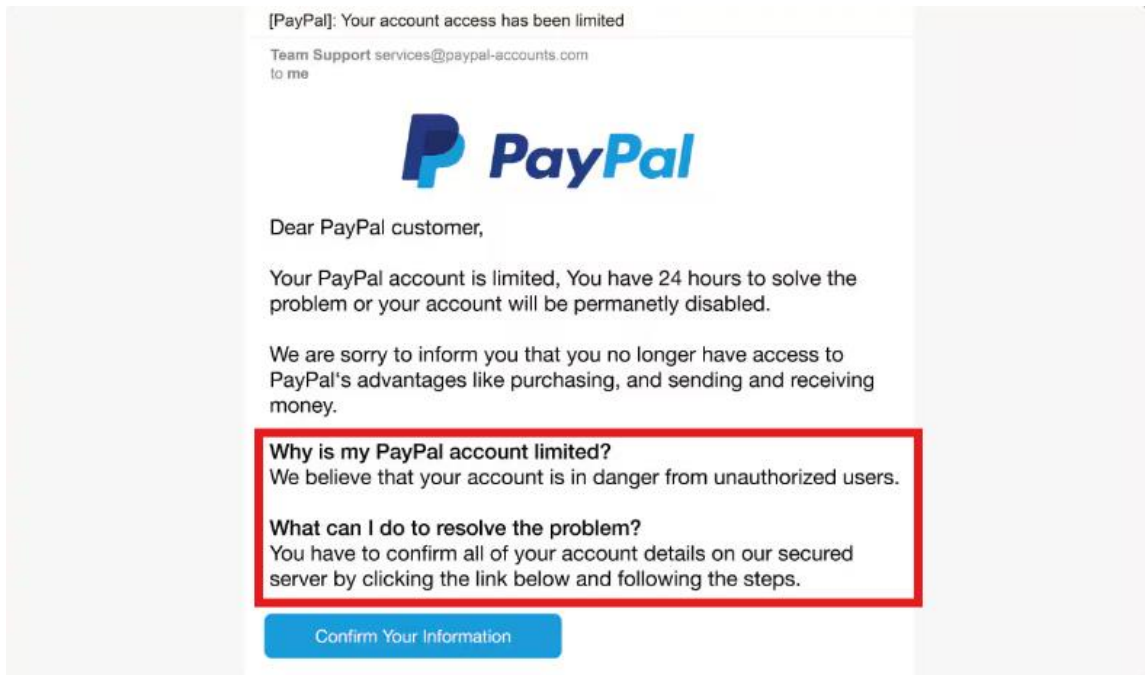


##### - Spelling and grammar errors



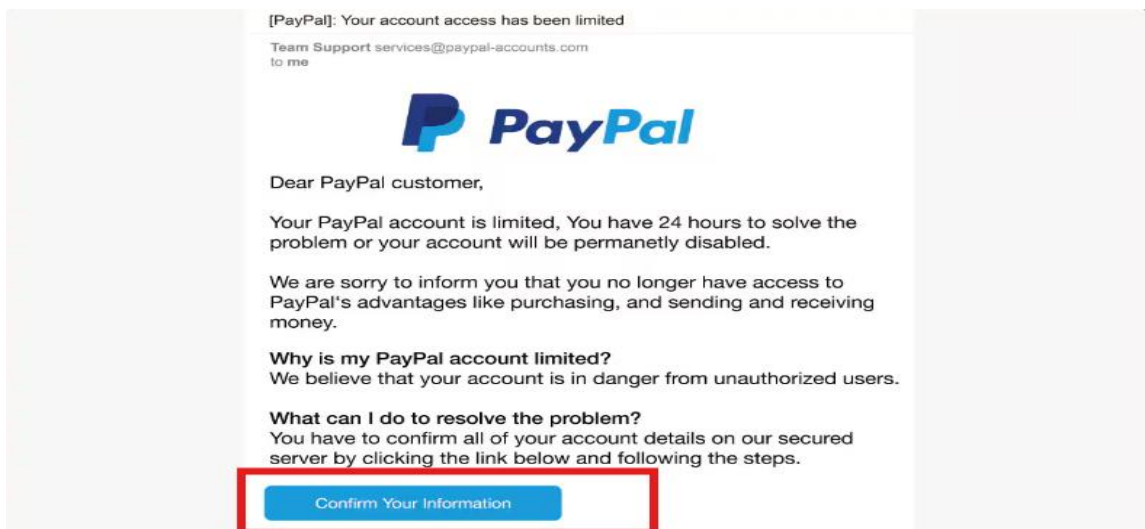
## - Inconsistent formatting

NOTE- Text under shape figure is Inconsistent format in this Phishing Email.



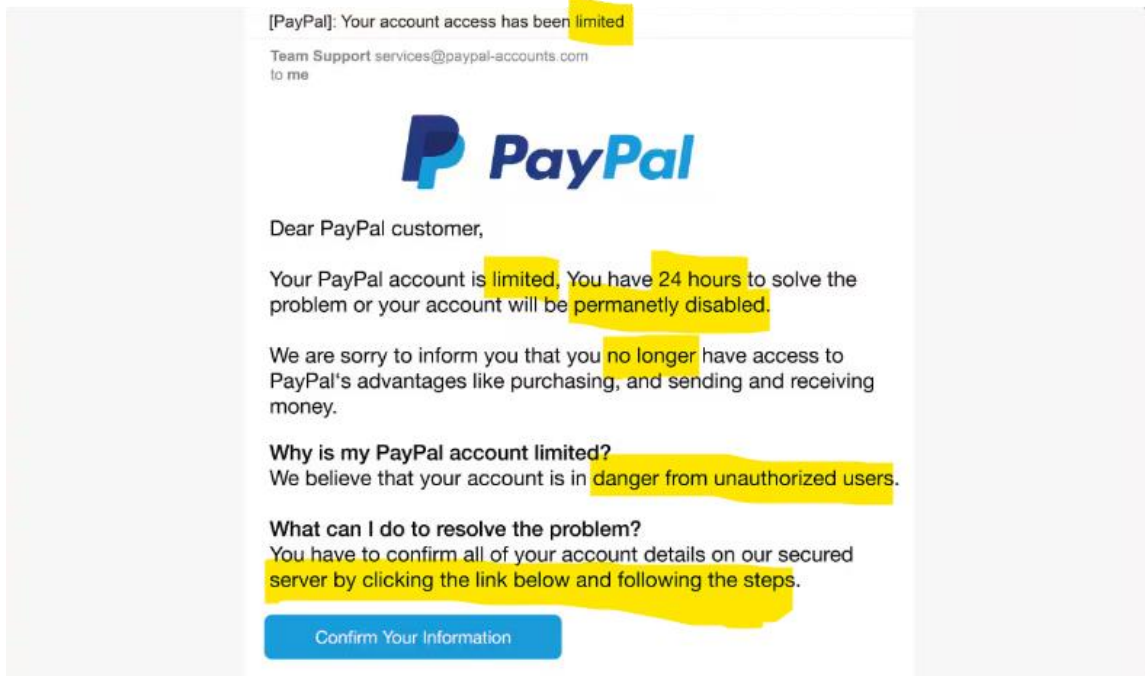
## 5. Links/Attachments

- Hovered link shows: <http://maliciouswebsite.com>
- Link text mismatch
- Suspicious attachment: invoice.docm

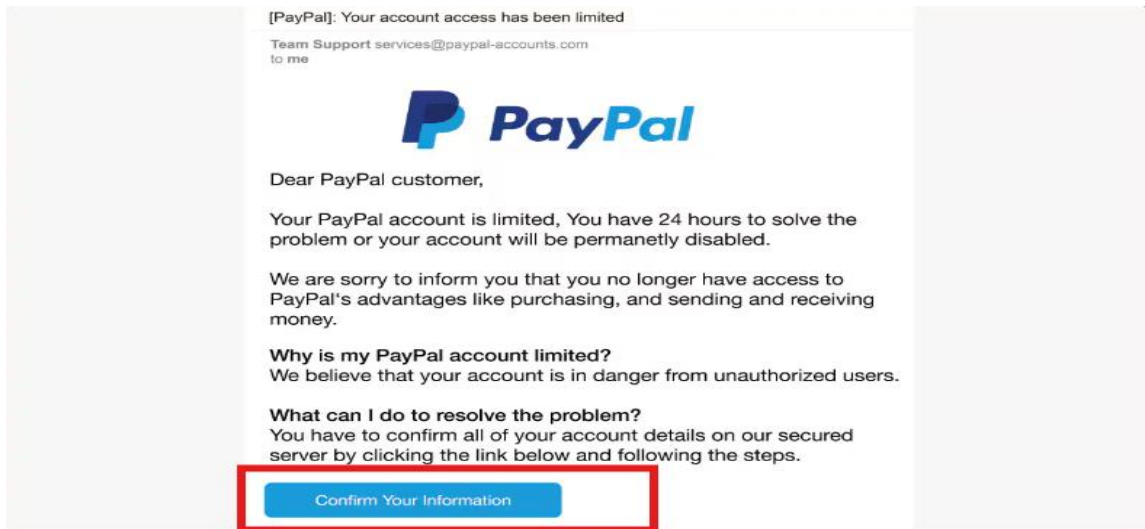


## 6. Summary of Phishing Traits Found

- Spoofed sender address
- Threatening tone in message



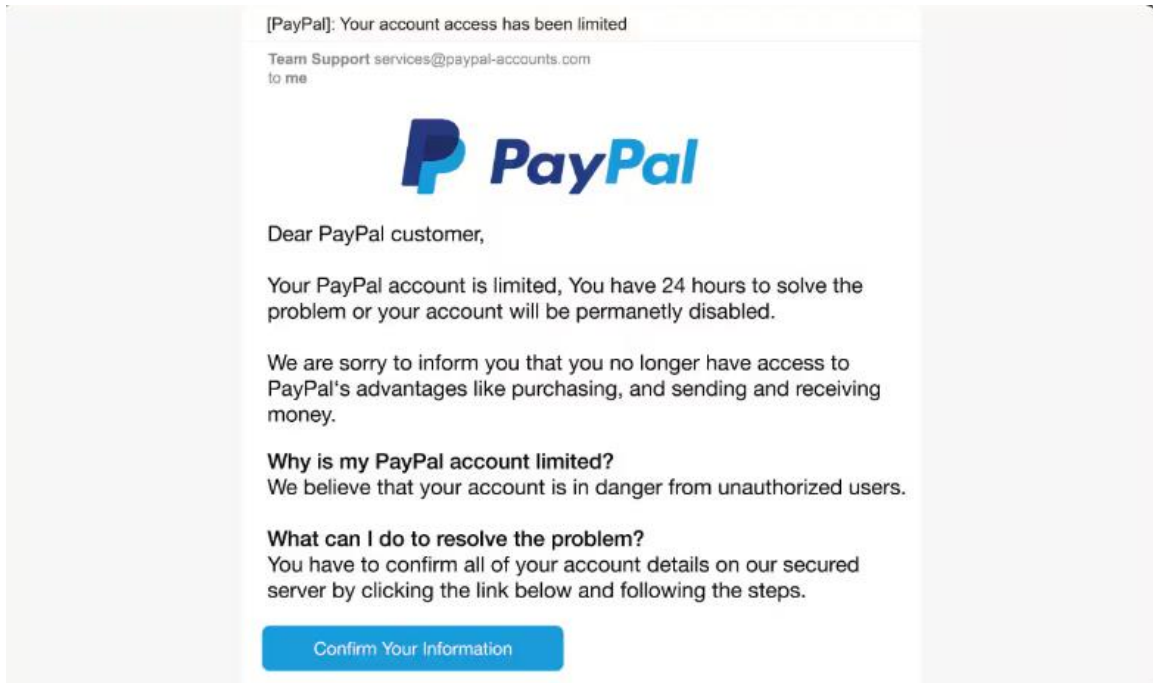
- Suspicious file attachment



- Grammar/spelling issues

## 7. Conclusion

This email displays multiple common phishing indicators. Users should avoid clicking on any links or downloading attachments.



**This Whole Email is an Example of Phishing Attack.**