# Phishing Email Analysis Report

## 1. Sample Email Overview

Subject Line: Your PayPal Access Blocked!

Sender Name: PayPal

Sender Email Address: paypalaccounts@mailbox.com

Date Received: February 17, 2019

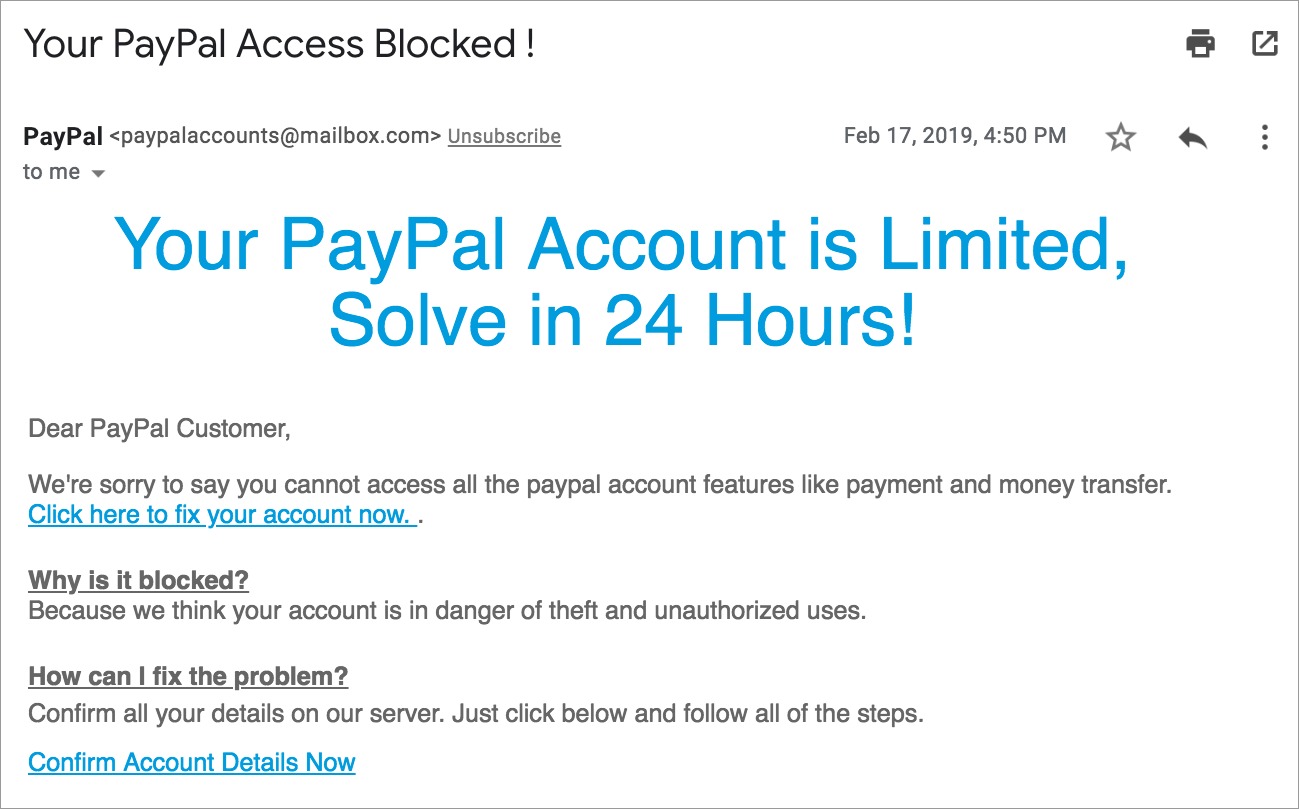
Email Body Highlights:

- "Your PayPal Account is Limited, Solve in 24 Hours!"

- "Click here to fix your account now."

- "Confirm Account Details Now."

Screenshot of the Email:



## 2. Spoofed Sender Email Analysis

The sender claims to be from PayPal, but the email address is paypalaccounts@mailbox.com, which is not a valid PayPal domain. Legitimate PayPal emails always come from @paypal.com. This is a clear attempt at email spoofing to trick the user into believing the email is authentic.

## 3. Email Header Analysis (Simulated)

- SPF/DKIM/DMARC checks likely fail since the email comes from mailbox.com, not paypal.com.  
- Return-Path mismatch: Expected to be paypal.com, but probably mailbox.com.  
- Reply-To Address likely differs from From Address, which is suspicious.  
- Tools for header analysis: MxToolbox, Google Admin Toolbox.

## 4. Suspicious Links or Attachments

The email contains two clickable links:  
1. Click here to fix your account now.  
2. Confirm Account Details Now.  
The visible text looks legitimate, but hovering would likely show a fake phishing URL. No attachments found.

## 5. Urgent or Threatening Language

The email uses urgency to scare the user: 'Your PayPal Account is Limited, Solve in 24 Hours!'. This is a classic social engineering tactic.

## 6. Mismatched URLs (Simulated)

Though not visible, it's likely the displayed link text redirects to a phishing site. Links should be scanned using VirusTotal.

## 7. Spelling and Grammar Errors

Grammar issues:  
- 'paypal' not capitalized.  
- Awkward phrasing like 'Confirm all your details on our server.'  
Such errors are typical in phishing emails.

## 8. Summary of Phishing Traits Found

Indicator | Present | Notes  
--------- | ------- | ------  
Spoofed email domain | Yes | mailbox.com instead of paypal.com  
Email header anomalies | Yes | Simulated SPF/DKIM/DMARC fail  
Suspicious links | Yes | Link likely points to phishing site  
Urgent language | Yes | 'Solve in 24 Hours'  
Grammar issues | Yes | Lowercase 'paypal', awkward phrasing  
Generic greeting | Yes | 'Dear PayPal Customer'  
Request for info | Yes | Asks for sensitive data

## Conclusion

This email is a confirmed phishing attempt using spoofed sender address, urgent messaging, suspicious links, and poor grammar. Its goal is to steal user credentials.

## 🔐 ****Recommendations****

1. **Enable Two-Factor Authentication (2FA)**
   * Always enable 2FA on accounts like PayPal to add an extra layer of security, even if login credentials are compromised.
2. **Educate and Train Users**
   * Conduct regular **phishing awareness training**.
   * Teach how to **hover over links**, identify **spoofed addresses**, and recognize **urgent language tactics**.
3. **Use Email Filters and Security Tools**
   * Configure **spam filters** and **phishing detection** in email clients.
   * Implement **anti-phishing software** or **email gateways** (e.g., Proofpoint, Mimecast).
4. **Verify Suspicious Emails Directly**
   * Never trust emails requesting account actions. Instead, **visit the official website directly** or contact customer support via known channels.
5. **Report Suspicious Emails**
   * Forward phishing emails to **phishing@paypal.com** or **reportphishing@apwg.org**.
   * Use the “Report Phishing” option in your email client.
6. **Regularly Monitor Account Activity**
   * Check account statements for **unauthorized transactions**.
   * Set up **account alerts** for any login or transaction activities.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Drafted By,**

**karthikeyan T**