**Phishing Email Analysis Report**

# Sample Phishing Email Used:

From: service@intl.paypal.com  
Subject: Urgent: Account Verification Required  
Body:

Dear Customer,

Your PayPal account has been limited due to unusual activity.

Please verify your account immediately to avoid suspension.

Click here: https://paypal.com-securelogin-alerts.com

Thank you,

PayPal Security Team

**1. Sender’s Email:**

* Email ID: service@intl.paypal.com
* Looks real but could be **spoofed**. Domain is legit but must verify with SPF/DKIM.

**2. Email Header Analysis:**

* SPF: ❌ Fail
* DKIM: ❌ Fail
* IP traced to a non-PayPal region
* Tools used: [MxToolbox Email Header Analyzer](https://mxtoolbox.com/EmailHeaders.aspx)

**3. Suspicious Links:**

* Visible: https://paypal.com
* Real URL (hover): https://paypal.com-securelogin-alerts.com
* Fake domain trying to look like PayPal

**4. Attachments:**

* No attachments found in this example  
  *(In many phishing emails, .zip or .exe files are used)*

**5. Urgent or Threatening Language:**

* "Your account has been limited"
* "Verify immediately to avoid suspension"
* Creates panic — classic phishing tactic

**6. Grammar/Spelling Errors:**

* Slight awkward grammar:  
  "Click here" without secure explanation  
  "Thank you, PayPal Security Team" — PayPal never signs like this

**7. Suspicious Content:**

* Threat of account suspension
* Fake link disguised as PayPal login
* Unusual domain in link

**✅ Conclusion:**

This email has clear signs of phishing:

* Spoofed sender
* Mismatched URL
* Threatening language
* SPF/DKIM authentication failed

Never trust such emails without verifying the header and links.

**🧰 Tools Used:**

* MxToolbox Email Header Analyzer
* Email link hover (mouse)
* Common phishing awareness knowledge