**Phishing Email Analysis Report**

**Email Content Overview**

From: PayPal Security <support@paypa1.com>

To: anitosh@example.com

Subject: Urgent: Account Suspension Notice

Dear Customer,

We’ve detected unusual activity in your PayPal account. To protect your funds, your account has been temporarily suspended.

Please verify your information within 24 hours by clicking the link below:

👉 [Verify Your Account](http://secure-paypa1-confirmation.com/login)

Failure to act may result in permanent suspension.

Sincerely,

PayPal Security Team

**Email Header Snapshot**

Return-Path: <bounce@otherdomain.xyz>

Received: from smtp.fakeprovider.com ([185.12.111.22])

by mx.google.com with ESMTPS id abc123;

Fri, 24 May 2025 08:12:45 -0700 (PDT)

Received-SPF: fail (google.com: domain of bounce@otherdomain.xyz does not designate 185.12.111.22 as permitted sender)

Authentication-Results: mx.google.com;

dkim=fail header.i=@paypa1.com;

spf=fail (google.com: domain of bounce@otherdomain.xyz does not designate 185.12.111.22 as permitted sender)

From: PayPal Security <support@paypa1.com>

To: anitosh@example.com

Subject: Urgent: Account Suspension Notice

**Analysis Steps**

**1. Sender Address Review**

* **Claimed sender:** [support@paypa1.com](mailto:support@paypa1.com)
* **Expected domain:** paypal.com
* **Finding:** The domain uses a number **"1"** instead of letter **"l"**, known as **typosquatting**.
* **Verdict:** Spoofed domain name to trick users visually.

**2. Header Authentication Checks**

* **SPF (Sender Policy Framework):** FAIL
  + The sending IP is **not authorized** to send emails for the sender domain.
* **DKIM (DomainKeys Identified Mail):** FAIL
  + No valid signature to confirm legitimacy of the sender.
* **Return-Path Mismatch:** From bounce@otherdomain.xyz, not aligned with sender.
* **Verdict:** Fails email authentication — a common phishing indicator.

**3. Suspicious URL in Email Body**

* **Link shown:** http://secure-paypa1-confirmation.com/login
* **Hover link:** Same as above — appears unrelated to PayPal.
* **Finding:** Mimics legitimate domain but uses different TLD and structure.
* **Verdict:** Highly suspicious URL — phishing link.

**4. Language and Tone Check**

* **Urgency:** "Verify within 24 hours" and "permanent suspension"
* **Emotion trigger:** Fear of account lockout
* **Verdict:** Uses fear-based manipulation, typical in phishing emails.

**5. Spelling & Grammar**

* No glaring spelling issues, but slight awkwardness in phrasing — common in mass phishing.
* **Verdict:** Slight red flags in professionalism.

**Summary of Phishing Traits Identified**

| **Indicator** | **Evidence** | **Verdict** |
| --- | --- | --- |
| Spoofed Email Address | paypa1.com vs paypal.com | ❌ Suspicious |
| SPF/DKIM Authentication Failure | Both checks failed | ❌ High Risk |
| Mismatched/Phishy URL | Domain doesn’t belong to PayPal | ❌ Malicious |
| Urgent/Threatening Language | Immediate suspension warning | ⚠️ Emotional bait |
| Subtle Grammar/Phrasing Issues | Slightly unnatural phrasing | ⚠️ Minor Red Flag |

**Conclusion**

This email demonstrates multiple classic phishing characteristics including **spoofed sender information**, **failing email authentication**, and **malicious URLs**, paired with **social engineering tactics** to coerce user action. It should be marked as phishing and reported accordingly.