Phishing Email Analysis Report

# Sample Email Summary

Subject: Urgent Account Verification Needed  
Sender: support@paypa1.com  
Date Received: May 26, 2025  
Email Client Used: Thunderbird  
Header Analyzer Tool: MxToolbox Email Header Analyzer (https://mxtoolbox.com/EmailHeaders.aspx)

# 1. Sender Address Analysis

Displayed Email: support@paypa1.com  
Issue Identified: Looks like “paypal.com” but uses number “1” instead of letter “l” – a classic spoofing trick.

# 2. Email Header Discrepancies

Analyzed With: MxToolbox  
Findings:  
- Return-Path: suspicious IP not matching official PayPal mail servers.  
- SPF/DKIM/DMARC: Fail or missing – signs of unauthorized sending.  
- Received from: Host domain is registered in an unrelated country.

# 3. Suspicious Links/Attachments

Link Displayed: https://paypal.com/login  
Actual URL (on hover): http://secure-paypal-login.ru/verify  
Attachment: HTML file named Account\_Reactivation.html  
Verdict: Phishing site with a fake login page, designed to steal credentials.

# 4. Urgent/Threatening Language

Examples:  
- “Your account will be suspended in 24 hours.”  
- “Immediate action required to avoid termination.”  
Purpose: Creates panic to bypass rational judgment.

# 5. Mismatched URLs

Links embedded with deceptive text (displayed URL vs real target differs). Hyperlinks redirect to unrelated or malicious domains.

# 6. Spelling & Grammar Errors

Phrases like “We need you verify your account informations.” Poor grammar common in phishing scams to filter non-vulnerable users.

# 7. Summary of Phishing Indicators

|  |  |
| --- | --- |
| Indicator | Description |
| Spoofed sender address | “paypa1.com” instead of “paypal.com” |
| Failing authentication headers | SPF/DKIM/DMARC failed |
| Suspicious links | Link text doesn’t match real destination |
| Fake urgency | Pressure to act quickly |
| Attachment with fake form | HTML file likely used to steal login credentials |
| Spelling/grammar issues | Unprofessional language and errors |

# Conclusion

This email is a classic phishing attempt. It uses spoofed domains, misleading links, urgency, and poor grammar to deceive recipients. Do not click on links or download attachments. Report to the appropriate IT or security team.