1. Sender’s Email Address
Observed sender: support@paypa1.com
Legitimate domain should be paypal.com.
Indicator: Domain spoofing with a lookalike domain (paypa1.com instead of paypal.com).

2. Email Headers
Findings from header analyzer:
SPF check: Failed
DKIM: Not aligned
Received path: Originated from an IP address in a suspicious region, not owned by PayPal.
Indicator: Authentication failures suggest spoofed sender identity.

SPF and DKIM Information

Headers Found

Header Name	Header Value
Date	Thu, 24 Sep 2025 08:05:23 +0530
From	"Paypa1 Support" <support@paypa1.com>
Reply-To	no-reply@fake-domain.com
Subject	Urgent: Verify Your Account Immediately
SPF	FAIL with IP 203.0.113.45
DKIM	None

Received Header

```
Received: from unknown (HELO mail.example.com) (192.168.1.10)
  by smtp.gmail.com with ESMTPS id x12sm456789qkf.12.2025.09.24.08.05.23
  for <youremail@gmail.com>;
Date: Thu, 24 Sep 2025 08:05:23 +0530
From: "Paypa1 Support" <support@paypa1.com>
Reply-To: no-reply@fake-domain.com
Subject: Urgent: Verify Your Account Immediately
SPF: FAIL with IP 203.0.113.45
DKIM: None
```

MXToolbox Email Header Analyzer

3. Suspicious Links or Attachments
Email contains a link labeled “Verify Your Account” → Redirects to http://security-update-paypal-login.com.
No legitimate PayPal HTTPS domain.
Indicator: Phishing link attempting credential harvesting.

4. Urgent / Threatening Language
“Your account will be permanently suspended within 24 hours unless you verify your details immediately.”
Indicator: Use of urgency to pressure victim into clicking.

5. Mismatched URLs
Hovering over “Login to PayPal” shows hidden URL: http://fake-paypal-support.ru instead of https://www.paypal.com.
Indicator: Mismatched, malicious link.

6. Spelling and Grammar Errors
Body text includes errors such as: “Your accont informations is not verifyed properly.”
Indicator: Poor grammar & spelling, common in phishing attempts.

7. Attachments
The email includes a .zip file named Invoice.zip.
Likely malicious (possible malware dropper)
Indicator: suspicious attachment with executable risk.

Summary of Phishing Traits Found
Spoofed sender email domain.
Authentication failures (SPF/DKIM).
Suspicious external links not matching legitimate domains.
Use of urgency and threats.
Spelling/grammar mistakes.
Presence of potentially malicious attachment.