EMAIL HEADER ANALYSIS

(Simulated sample)

All data used in this report is fictional and created for portfolio purposes

Sample Email Header

```
Return-Path: <secure-update@paypalsecure.com>
Received: from mail.paypalsecure.com (102.55.23.19)
  by mx.google.com with ESMTP id a1b2c3d4e5
  for <victim.user@gmail.com>;
  Tue, 05 Dec 2025 11:42:13 -0800 (PST)
Received-SPF: Fail (google.com: domain paypalsecure.com does not designate
102.55.23.19 as permitted sender)
Authentication-Results: mx.google.com;
  spf=fail (google.com: domain of secure-update@paypalsecure.com does not
designate 102.55.23.19 as permitted sender) smtp.mailfrom=secure-
update@paypalsecure.com;
  dkim=fail header.i=@paypalsecure.com;
  dmarc=fail action=quarantine header.from=paypalsecure.com
DKIM-Signature: v=1; a=rsa-sha256; d=paypalsecure.com; s=google;
  h=from:to:subject:date:message-id:mime-version;
  bh=j8U9P/93ke8mfa93ks==;
  b=InvalidSignature12345
From: "PayPal Security Alert" <secure-update@paypalsecure.com>
To: <victim.user@gmail.com>
Subject: Urgent: Your PayPal account has been limited!
Date: Tue, 05 Dec 2025 11:42:10 -0800
Message-ID: <CAGJk4d9jsfkl93k4j2@mail.paypalsecure.com>
MIME-Version: 1.0
Content-Type: text/html; charset="UTF-8"
```

1. INTRODUCTION

The report analyzes a simulated phishing email using forensic techniques The goal is to identify technical indicators of phishing by examining the email header, authentication results, sender information, and routing path.

2. EMAIL SUMMARY

Describe the email in simple terms.

Field	***Details***
Subject	***Urgent: Your PayPal account has been limited!***
Sender (Displayed)	***PayPal Security Alert***
Sender (Actual Address)	***secure-update@paypalsecure.com***
Recipient	***victim.user@gmail.com***
Date	***Tue, 05 Dec 2025***

3. EMAIL HEADER USED (SIMULATED)

Return-Path: <secure-update@paypalsecure.com>

Received: from mail.paypalsecure.com (102.55.23.19)

4. ANALYSIS OF HEADER FIELDS

4.1 Return-Path Check -Does not match official PayPal domain → *Suspicious.*

4.2 IP Address Analysis- 102.55.23.19, Google domain does not designate the IP Address as a permitted sender.

4.3 SPF- FAIL

4.4 DKIM- FAIL

4.5 DMARC- FAIL

4.6 Subject Line- *Urgent: Your PayPal account has been limited! (Phishing Behavior)*

4.7 Domain Name is found to be not matching with the expected name

5. FINAL CONCLUSION

The email analyzed contains multiple indicators of phishing, including SPF/DKIM/DMARC authentication failures, a suspicious sending IP, a fake sender domain, and a subject line designed to create urgency. Based on the evidence, this email is a clear phishing attempt and should not be trusted.

6. RECOMMENDATIONS

- Do not click links or download attachments.
- Report the email as phishing if found suspicious.
- Verify sender domains before responding.
- Enable multi-factor authentication.
- Train users to recognize header-based indicators for finding red flags.

Transparency Note: *This email header was simulated for training purposes.*
No real personal emails or sensitive information were used.