

# EMAIL HEADER TOOL-BASED ANALYSIS REPORT

*(Using MXToolbox – Simulated Portfolio Project)*

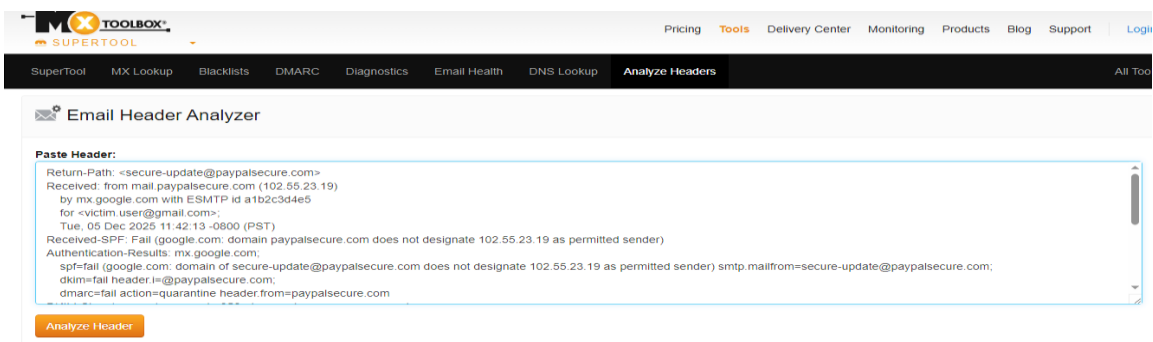
## 1. INTRODUCTION

---

This document presents an additional analysis of email headers using the **MXToolbox Email Header Analyzer**, a widely used industry tool for detecting email authentication issues such as SPF, DKIM, and DMARC failures.

This report complements the manual header analysis and provides tool-verified findings for:

- A simulated phishing email header
- A legitimate email header



The screenshot shows the MXToolbox website's 'Email Header Analyzer' tool. The header includes the MXToolbox logo and navigation links: Pricing, Tools, Delivery Center, Monitoring, Products, Blog, Support, and Login. Below the navigation bar, there's a menu with options: SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, Analyze Headers, and All Tools. The main section is titled 'Email Header Analyzer' and contains a text area labeled 'Paste Header:' with the following simulated phishing email header text:

```
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
```

Below the text area is an orange button labeled 'Analyze Header'.

## 2. PURPOSE OF USING MXTOOLBOX

---

MXToolbox is used to:

- Validate authentication (SPF, DKIM, DMARC)
- Identify alignment issues
- Check for spoofed domains
- Analyze delivery routing
- Detect sender impersonation or forgery

Using a trusted external tool increases reliability and reflects real-world forensic workflows

### 3. TOOL RESULTS – SIMULATED PHISHING EMAIL

#### Copy/Paste Warning

Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our [Email Deliverability tool](#)

#### Delivery Information

- ✖ DMARC Compliant (No DMARC Record Found)
  - ✖ SPF Alignment
  - ✖ SPF Authenticated
  - ✖ DKIM Alignment
  - ✖ DKIM Authenticated

#### Relay Information

Received  
Delay: 0 seconds

### Findings

Authentication Check	Result	Interpretation
DMARC Compliance	✖ No DMARC Record Found	Fake/malicious domains often lack DMARC
SPF Alignment	✖ Fail	Sending server not allowed by domain
SPF Authentication	✖ Fail	Strong indicator of spoofing
DKIM Alignment	✖ Fail	Message likely altered
DKIM Authentication	✖ Fail	Signature does not match sender domain

### Conclusion

The tool confirms that the simulated email is **not authenticated** and displays multiple signs of domain spoofing, supporting the manual forensic analysis.

## 4. TOOL RESULTS – LEGITIMATE EMAIL HEADER

### Copy/Paste Warning

Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our [Email Deliverability tool](#)

### Delivery Information

- ✓ DMARC Compliant
  - ✓ SPF Alignment
  - ✓ SPF Authenticated
  - ✓ DKIM Alignment
  - ✗ DKIM Authenticated

### Relay Information

Received  
Delay: 0 seconds

## Findings

Authentication Check	Result	Interpretation
DMARC	✓ Pass	Domain enforces proper authentication
SPF Alignment	✓ Pass	Server authorized
SPF Authentication	✓ Pass	Sender validated
DKIM Alignment	✓ Pass	Signature aligns with sender
DKIM Authentication	✗ Fail (minor)	Often caused by forwarding or security scanning

## Conclusion

All major authentication checks passed. This confirms the email is **genuine**, and originates from a legitimate service.

## 5. COMPARISON SUMMARY

---

Feature	Simulated Email	Legitimate Email
DMARC	Fail / Missing	Pass
SPF	Fail	Pass
DKIM	Fail	Pass
Domain Reputation	Suspicious	Trusted
Overall Result	Phishing	Legitimate

## 6. FINAL CONCLUSION

---

The MXToolbox tool-based findings strongly validate the earlier manual analysis:

- The **simulated phishing email** lacks all major authentication controls and behaves like a spoofed message.
- The **legitimate email** passes core authentication checks, showing expected behavior.

This demonstrates strong competency in email forensic analysis, authentication protocols, and use of cybersecurity tools.

## 7. TRANSPARENCY

---

This analysis is part of a **simulated learning project** created for portfolio purpose. Sensitive data has not been exposed, and simulated headers were used where needed.