EMAIL HEADER TOOL-BASED ANALYSIS REPORT

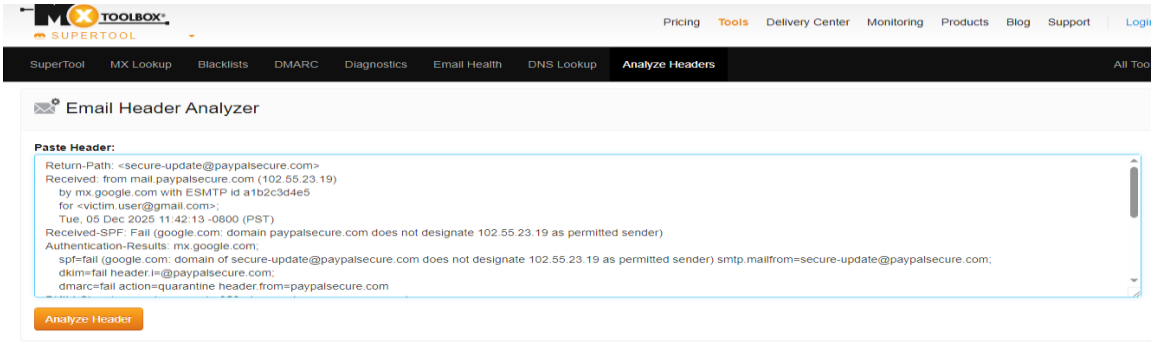
(Using MXToolbox – Simulated Portfolio Project)

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**



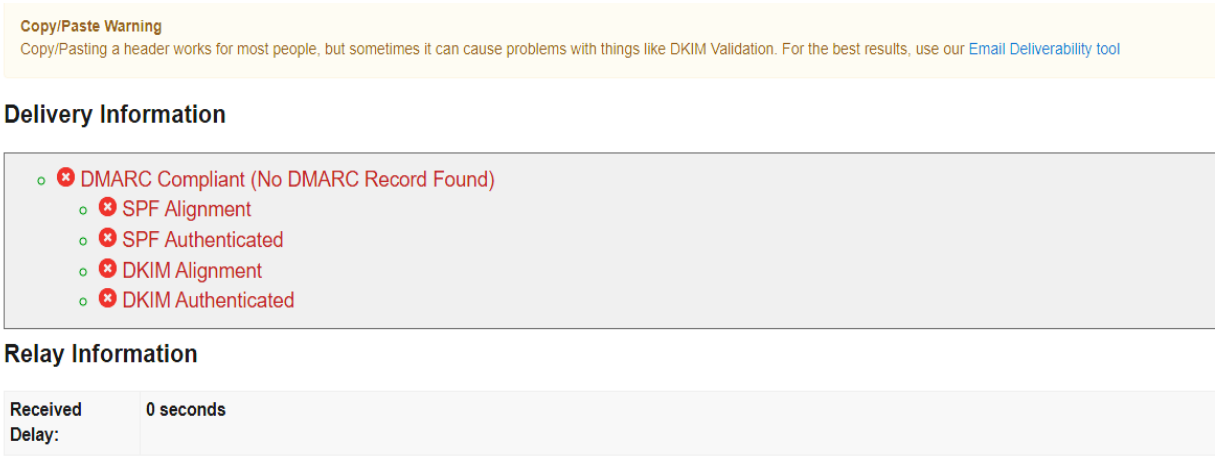
2. PURPOSE OF USING MXTOOLBOX

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

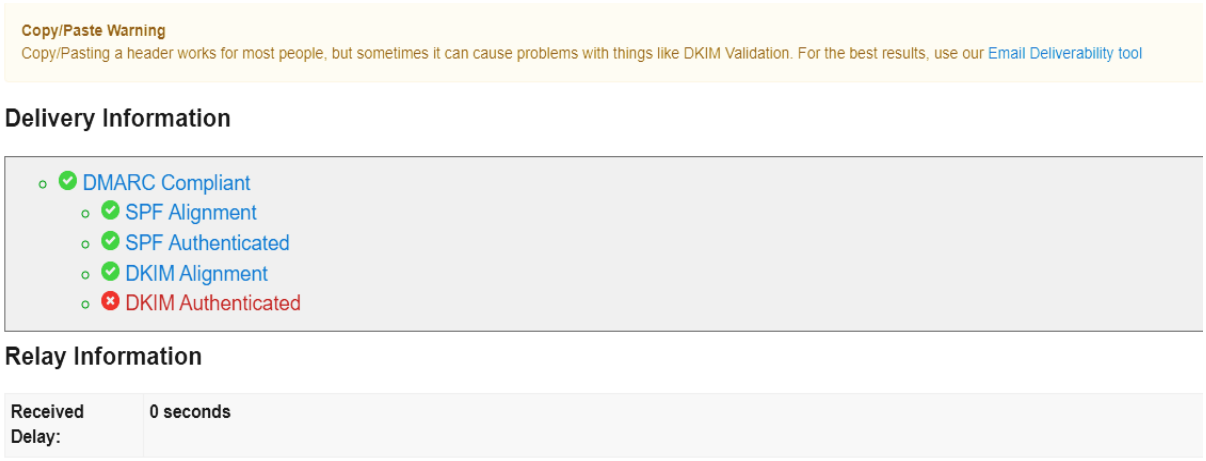
Findings

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



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.