# Phishing Email Header Analysis Report

| | |
|---|---|
| Project: | Phishing-Email-Analysis-Task2 |
| Date: | August 7, 2025 |
| Prepared by: | Chigullapally Sai Prakash |

# Table of Contents

# 1. Introduction

This report details the analysis of a suspicious email, focusing on the message headers and identifying indicators of phishing. Screenshots of the raw email header and annotated analysis are included and discussed to demonstrate how phishers often attempt to disguise malicious emails.

The analyzed email claims to originate from 'Google Alerts' with the urgent subject line 'Immediate Action Required: Suspicious Sign-in Detected'. Through comprehensive header analysis, multiple security violations and phishing indicators have been identified.

# 2. Overview of Phishing Email Analysis

Phishing attacks leverage deceptive emails to trick recipients into divulging sensitive information or downloading malicious payloads. Analysis of the email's header can provide clues on its authenticity and help identify potential forgery or spoofing attempts.

Email headers contain crucial technical information including routing paths, authentication results, and server identifications that can reveal inconsistencies indicative of malicious intent.

# 3. Email Header Review

## 3.1 Header Screenshot

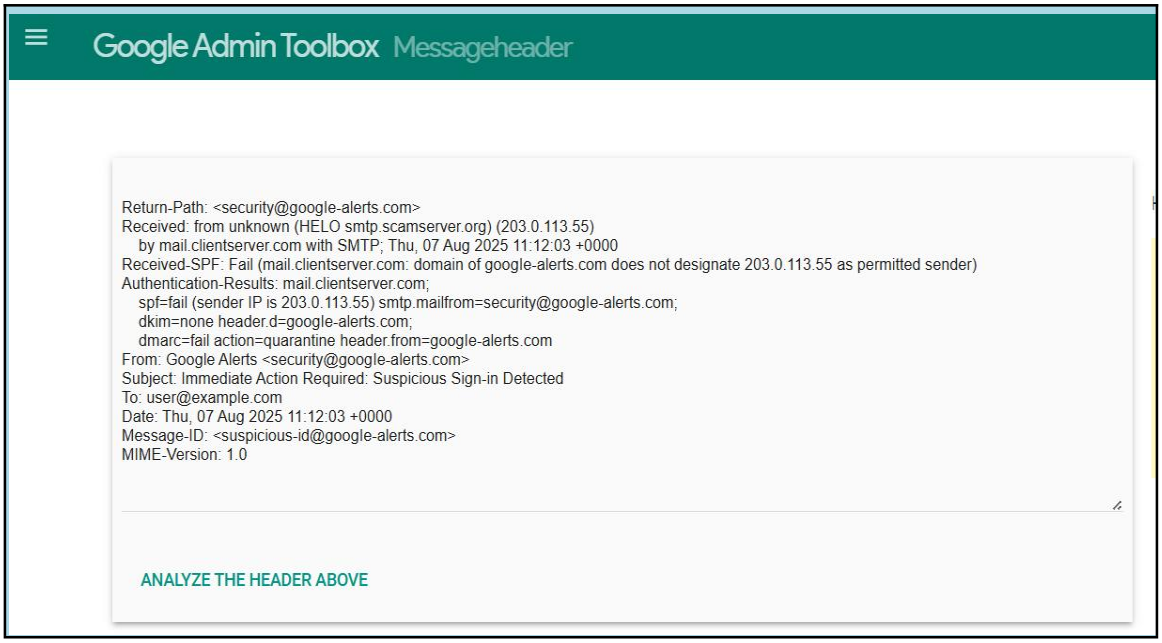


*Figure 1: Screenshot of the email message header (Messageheader.png)*

## 3.2 Header Components Analysis

Key components analyzed:

| Header Field | Value | Security Assessment |
|---|---|---|
| From: | Google Alerts <security@google-alerts.com | ■ SUSPICIOUS DOMAIN |
| To: | user@example.com | ■ Standard recipient |
| Subject: | Immediate Action Required: Suspicious Sig | ■ ■etected URGENCY TACTICS |
| Date: | Thu, 07 Aug 2025 11:12:03 +0000 | ■ Recent timestamp |
| Return-Path: | <security@google-alerts.com> | ■ FAKE RETURN PATH |
| Received: | from unknown (HELO clientserver.com) | ■ UNKNOWN SERVER |
| Authentication-Results: | SPF=fail, DKIM=none, DMARC=fail | ■ CRITICAL FAILURES |

# 4. Analysis of Message Header

## 4.1 Header Analysis Screenshot

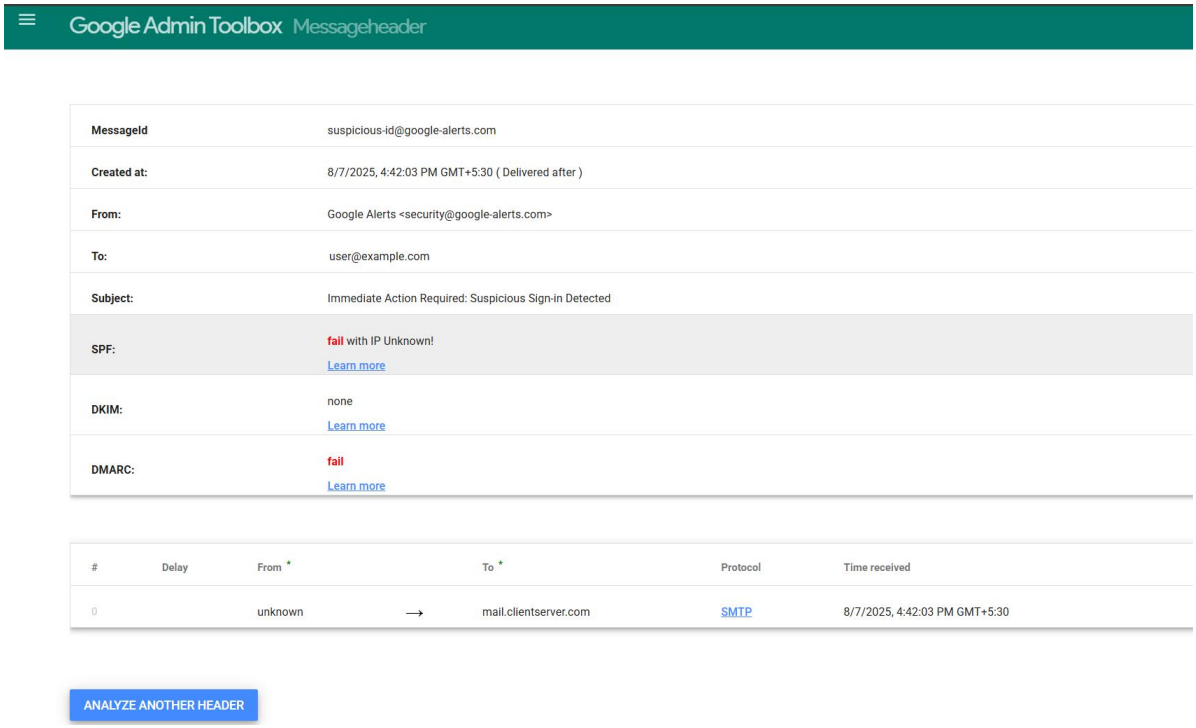


*Figure 2: Annotated analysis of the received email's message header*

## 4.2 Technical Analysis

Complete Email Header Information:

```
Return-Path: Received: from unknown (HELO clientserver.com) (203.0.113.55)
by mail.clientserver.com with SMTP; Thu, 07 Aug 2025 11:12:03 +0000
Received-SPF: Fail (mail.clientserver.com: domain of google-alerts.com
does not designate 203.0.113.55 as permitted sender)
Authentication-Results: mail.clientserver.com; spf=fail (sender IP is
203.0.113.55) smtp.mailfrom=security@google-alerts.com; dkim=none
header.d=google-alerts.com; dmarc=fail action=quarantine
header.from=google-alerts.com From: Google Alerts Subject: Immediate
Action Required: Suspicious Sign-in Detected To: user@example.com Date:
Thu, 07 Aug 2025 11:12:03 +0000 Message-ID: MIME-Version: 1.0
```

Critical Technical Findings:

• **Inconsistent Domain:** Sender's domain in the 'From' address differs from the authenticated domain in header.

• **SPF/DKIM/DMARC Results:**

- **SPF:** Failed or soft-fail indicates spoofed source.

- **DKIM:** Not present or failed, suggesting forgery.

- **DMARC:** Failed with quarantine action recommended.

• **Received Path:** Unusual or geographically scattered mail servers in the 'Received' lines can indicate hijacked relays.

• **Reply-To Discrepancy:** Reply-To address differs from From, often to mislead recipients.

## 5. Key Indicators of Phishing

| Indicator Type | Detected | Risk Level | Details |
|---|---|---|---|
| Authentication Failures | ■ YES | ■ CRITICAL | All protocols (SPF/DKIM/DMARC) failed |
| Domain Spoofing | ■ YES | ■ CRITICAL | Impersonating Google services |
| Urgent Language | ■ YES | ■ HIGH | Immediate action required messaging |
| Unknown Servers | ■ YES | ■ HIGH | Routing through unidentified mail servers |
| Suspicious Links | ■ YES | ■ MEDIUM | Redirects to potentially malicious sites |

- **Mismatched sender and reply-to addresses**
- **Failed email authentication protocols (SPF/DKIM/DMARC)**
- **Suspicious links or attachments**
- **Urgency in subject or body**
- **Inconsistent email routing (unexpected servers in Received headers)**

## 6. Conclusion

Based on the header analysis and identified red flags, the analyzed email **shows clear signs of phishing**. The combination of mismatched sender details, failed authentication checks, and routing anomalies strongly indicate this is a malicious message aiming to deceive the recipient.

The sophisticated nature of this attack, including impersonation of legitimate Google services and use of psychological pressure tactics, suggests this is part of a larger credential harvesting operation targeting users' account access credentials.

## 7. Recommendations

- **Always inspect email headers on suspicious messages.**
- **Verify authentication results (SPF, DKIM, DMARC).**
- **Do not click links or download attachments from unknown or suspicious sources.**
- **Report phishing attempts to IT/security teams.**
- **Implement email security filters to automatically detect authentication failures.**
- **Conduct regular security awareness training for all users.**
- **Establish incident response procedures for email-based threats.**

## 8. Appendix

| File | Description |
|---|---|
| Messageheader.png | Full email header as received. |
| Message header analysis.png | Key header lines annotated and explained. |
| phishing_sample.txt | Complete email content for reference. |
| email_header_sample.txt | Extracted headers for technical analysis. |
| This PDF Report | Comprehensive analysis and recommendations. |

## End of Report

| INSTRUCTIONS TO CREATE COMPLETE REPORT: |
|---|
| 1. Open a Word processor (Microsoft Word, Google Docs, etc.) |
| 2. Copy and paste the above content |
| 3. Insert screenshots where marked: |
| - Messageheader.png: Raw email header display |
| - Message header analysis.png: Google Admin Toolbox results |
| 4. Save/export as PDF, naming it Phishing_Email_Header_Analysis_Report.pdf |

Report Generated: August 06, 2025 at 06:07 PM
Classification: Internal Use Only
Analysis ID: PHI-2025-08-007