PHISHING EMAIL ANALYSIS REPORT

Prepared by: IMAN BEDRU

Program: Cybersecurity Internship / Training Task

Date: February 2026

Table of Contents

1.Introduction

Phishing is a cyberattack technique in which attackers impersonate trusted organizations to trick victims into revealing sensitive information such as passwords, financial details, or personal data.

Email remains one of the most common attack vectors for phishing campaigns. This report analyzes a suspicious email to determine its legitimacy using technical and manual investigation techniques.

2.Objective

The objective of this investigation is to:

- Identify phishing indicators
- Analyze email authentication mechanisms
- Examine header routing information
- Compare malicious and legitimate email security
- Provide security recommendations

3.Scope of Analysis

This analysis focuses on:

- Email header authentication results
- Sender identity verification
- Link inspection
- Social engineering indicators
- 2-Step Verification security comparison

The investigation does not include malware reverse engineering or deep forensic traffic analysis.

4.Tools Used

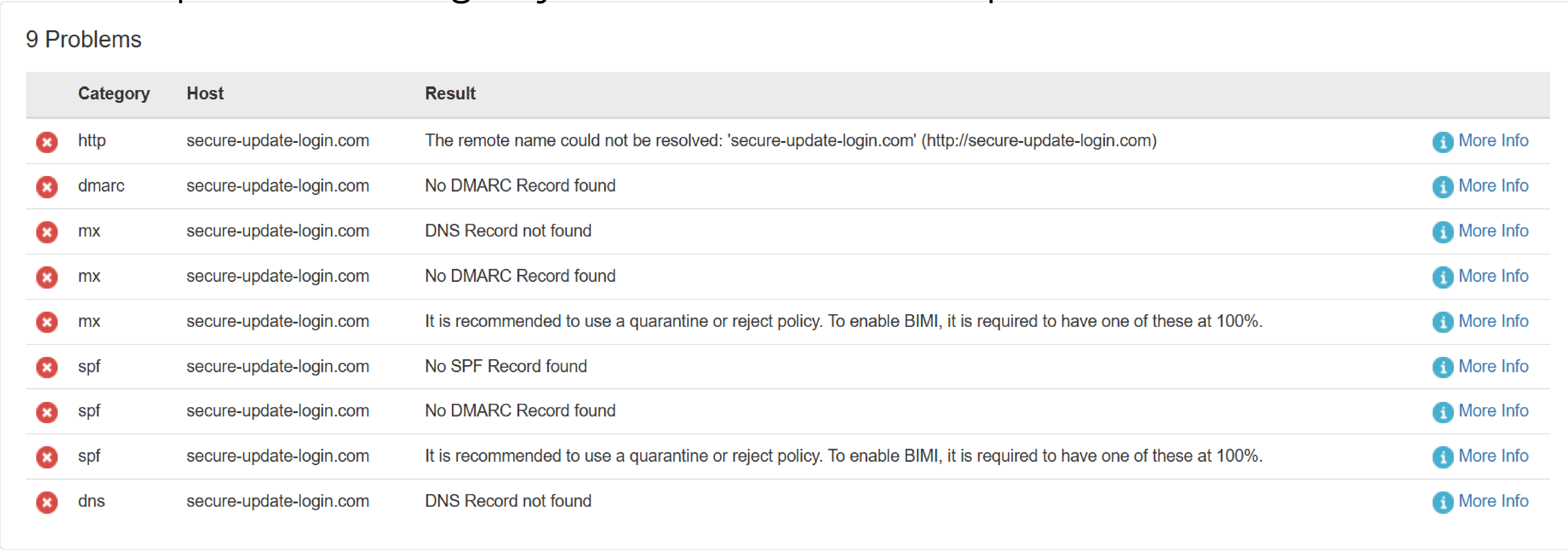
The following tools and techniques were used:

- Google Admin Toolbox – Message Header Analyzer
- Manual email header inspection
- Email client security settings
- 2-Step Verification (2SV) configuration review

5.Overview of the Suspicious Email

- Subject: Urgent: Account Verification Required
- Claimed Sender: support@secure-bank-alert.com
- Message Theme: Immediate account verification request
- Embedded Link: http://secure-update-login.com

The email attempts to create urgency and fear of account suspension.



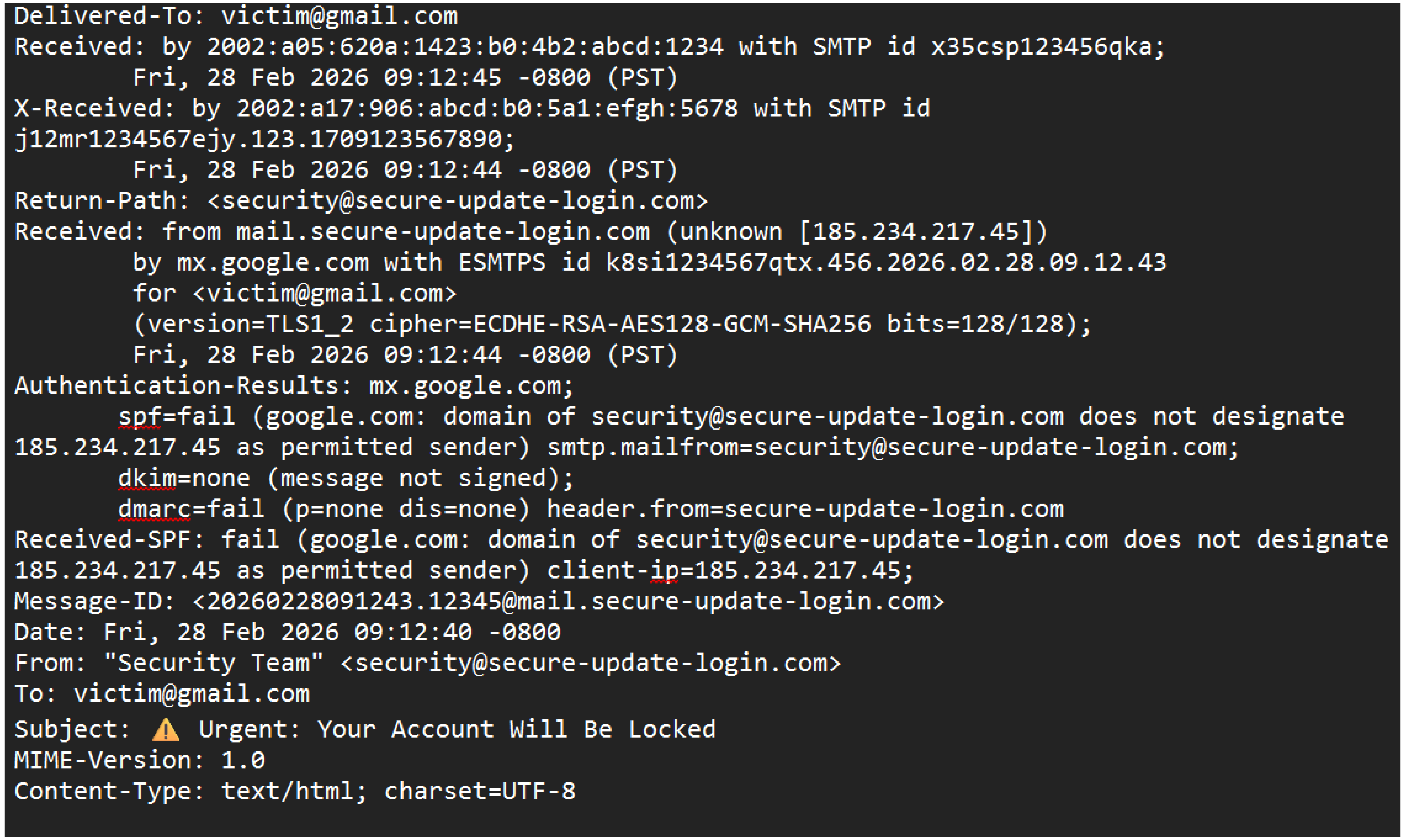
9 Problems

	Category	Host	Result	
⊗	http	secure-update-login.com	The remote name could not be resolved: 'secure-update-login.com' (http://secure-update-login.com)	ℹ More Info
⊗	dmarc	secure-update-login.com	No DMARC Record found	ℹ More Info
⊗	mx	secure-update-login.com	DNS Record not found	ℹ More Info
⊗	mx	secure-update-login.com	No DMARC Record found	ℹ More Info
⊗	mx	secure-update-login.com	It is recommended to use a quarantine or reject policy. To enable BIMI, it is required to have one of these at 100%.	ℹ More Info
⊗	spf	secure-update-login.com	No SPF Record found	ℹ More Info
⊗	spf	secure-update-login.com	No DMARC Record found	ℹ More Info
⊗	spf	secure-update-login.com	It is recommended to use a quarantine or reject policy. To enable BIMI, it is required to have one of these at 100%.	ℹ More Info
⊗	dns	secure-update-login.com	DNS Record not found	ℹ More Info

6.Email Header Analysis

- The email header was extracted and analyzed to determine sender authenticity.

6.1 Header Fields Examination



```
Delivered-To: victim@gmail.com
Received: by 2002:a05:620a:1423:b0:4b2:abcd:1234 with SMTP id x35csp123456qka;
        Fri, 28 Feb 2026 09:12:45 -0800 (PST)
X-Received: by 2002:a17:906:abcd:b0:5a1:efgh:5678 with SMTP id
j12mr1234567ejy.123.1709123567890;
        Fri, 28 Feb 2026 09:12:44 -0800 (PST)
Return-Path: <security@secure-update-login.com>
Received: from mail.secure-update-login.com (unknown [185.234.217.45])
        by mx.google.com with ESMTPS id k8si1234567qtx.456.2026.02.28.09.12.43
        for <victim@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Fri, 28 Feb 2026 09:12:44 -0800 (PST)
Authentication-Results: mx.google.com;
       spf=fail (google.com: domain of security@secure-update-login.com does not designate
185.234.217.45 as permitted sender) smtp.mailfrom=security@secure-update-login.com;
       dkim=none (message not signed);
       dmarc=fail (p=none dis=none) header.from=secure-update-login.com
Received-SPF: fail (google.com: domain of security@secure-update-login.com does not designate
185.234.217.45 as permitted sender) client-ip=185.234.217.45;
Message-ID: <20260228091243.12345@mail.secure-update-login.com>
Date: Fri, 28 Feb 2026 09:12:40 -0800
From: "Security Team" <security@secure-update-login.com>
To: victim@gmail.com
Subject: ⚠️ Urgent: Your Account Will Be Locked
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
```

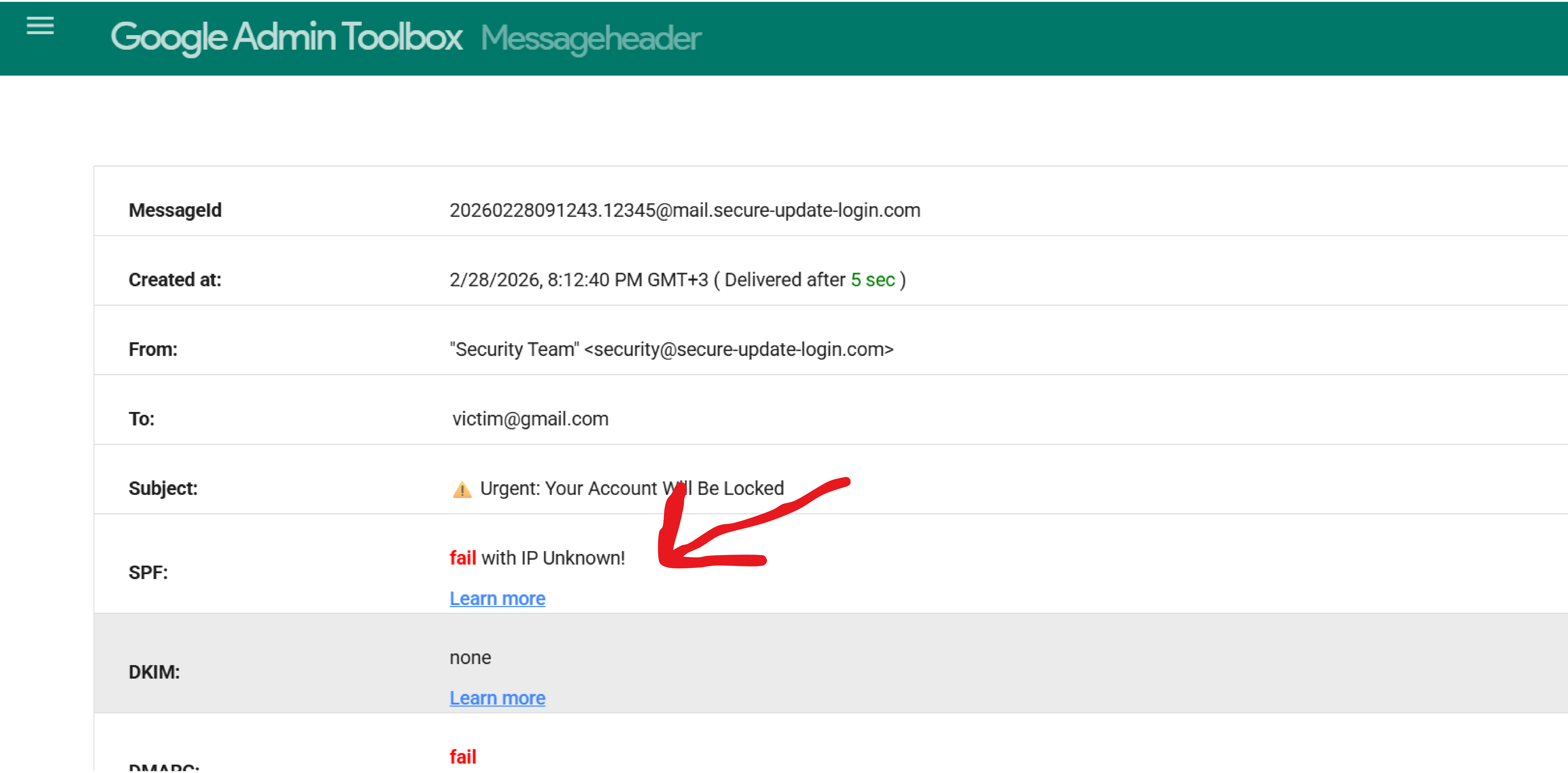
Header Field	Observed Result	Security Interpretation
Return-Path	Different domain	Possible spoofing
From	support@secure-bank-alert.com	Suspicious domain
Received	Multiple unknown servers	Possible relay manipulation
Message-ID	Randomized format	May indicate automated sending

6.2 SPF (Sender Policy Framework) Analysis

Sender Policy Framework (SPF) is an email authentication method that helps prevent email spoofing. It allows a domain owner to specify which mail servers are allowed to send emails on behalf of their domain.

SPF result: Fail

This indicates that the sending server was not authorized to send emails on behalf of the claimed domain.



Google Admin Toolbox Messageheader

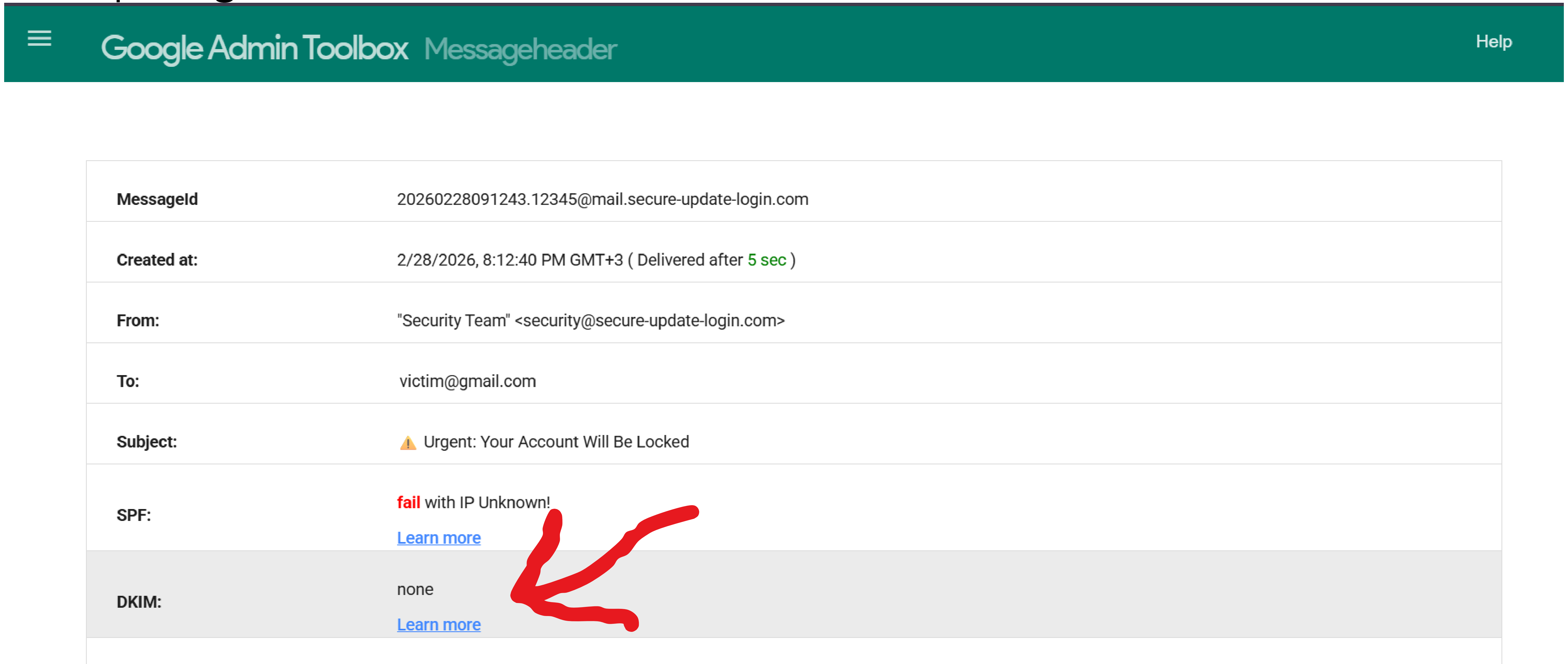
MessageId	20260228091243.12345@mail.secure-update-login.com
Created at:	2/28/2026, 8:12:40 PM GMT+3 (Delivered after 5 sec)
From:	"Security Team" <security@secure-update-login.com>
To:	victim@gmail.com
Subject:	⚠ Urgent: Your Account Will Be Locked
SPF:	fail with IP Unknown! Learn more
DKIM:	none Learn more
DMARC:	fail

6.3 DKIM (DomainKeys Identified Mail) Analysis

DKIM (DomainKeys Identified Mail) is an email authentication method that uses a digital signature to verify that an email was sent by the claimed domain and was not altered in transit.

DKIM result: None / Not Present

The absence of a DKIM signature means the email content was not cryptographically signed, increasing the risk of tampering

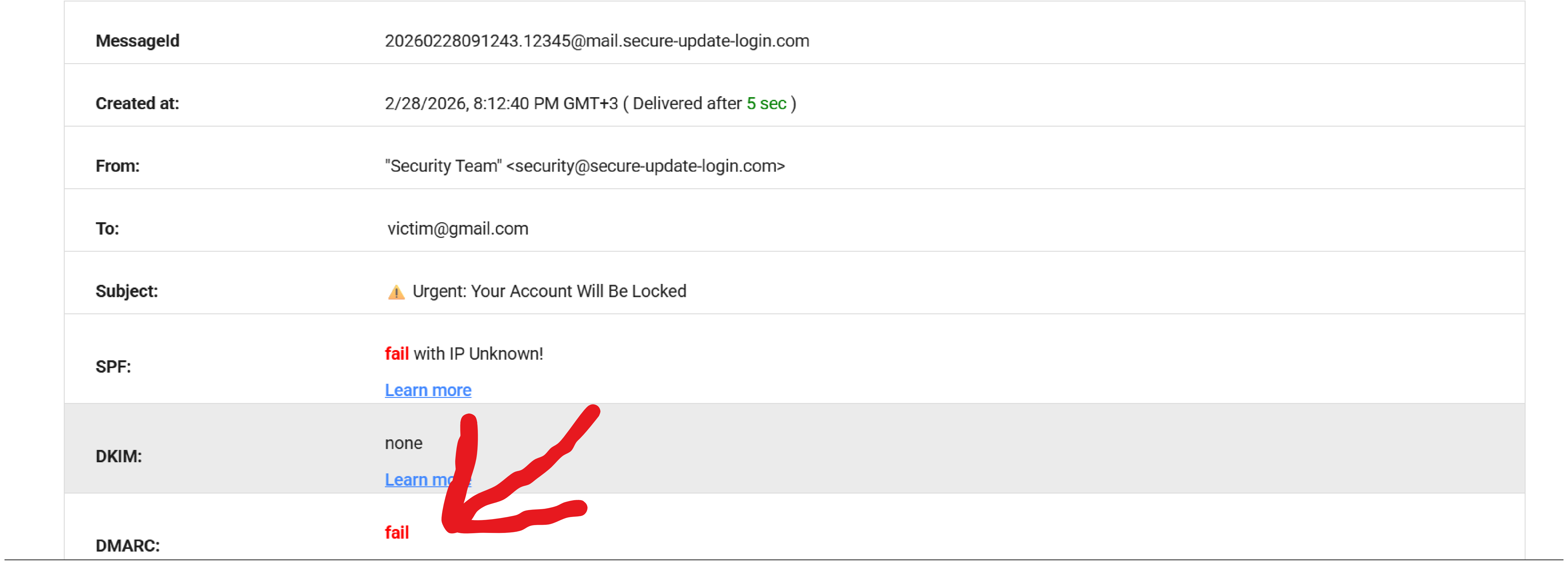


MessageId	20260228091243.12345@mail.secure-update-login.com
Created at:	2/28/2026, 8:12:40 PM GMT+3 (Delivered after 5 sec)
From:	"Security Team" <security@secure-update-login.com>
To:	victim@gmail.com
Subject:	⚠ Urgent: Your Account Will Be Locked
SPF:	fail with IP Unknown! Learn more
DKIM:	none Learn more

6.4 DMARC (Domain-based Message Authentication Reporting and Conformance)

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication protocol that helps protect domains from email spoofing.

DMARC result: Fail
This confirms that the message does not comply with the sender domain’s authentication policy.



MessageId	20260228091243.12345@mail.secure-update-login.com
Created at:	2/28/2026, 8:12:40 PM GMT+3 (Delivered after 5 sec)
From:	"Security Team" <security@secure-update-login.com>
To:	victim@gmail.com
Subject:	⚠ Urgent: Your Account Will Be Locked
SPF:	fail with IP Unknown! Learn more
DKIM:	none Learn more
DMARC:	fail

7.Email Content Analysis

The content of the suspicious email was examined to identify social engineering techniques and phishing indicators. While header analysis focuses on technical authentication, content analysis focuses on psychological manipulation and visual deception.

Subject Line Analysis

Subject: Urgent: Account Verification Required

Observations:

- Uses urgency ("Urgent")
- Implies immediate action is required
- Creates fear of account suspension

Security Interpretation:

Phishing emails commonly use urgent or threatening language to pressure victims into acting without thinking critically.

Sender Display Name vs Email Address

The email displayed:

Display Name: Secure Bank Support
Actual Email: support@secure-bank-alert.com

Observations:

- The domain does not match a legitimate bank domain
- The domain contains extra words like “alert” to mimic authenticity

Security Interpretation:

Attackers often use domains that look similar to real companies (domain spoofing / look-alike domains).

Greeting Style

The email begins with:

Dear Customer

Observations:

- Generic greeting
- No personalization (no full name)

Security Interpretation:

Legitimate financial institutions usually address customers by full name. Generic greetings are a common phishing indicator.

Example:

Your account will be permanently suspended unless you verify your details immediately.

Observations:

- Fear-based manipulation
- Strong call-to-action
- Deadline pressure

Security Interpretation:

This is a classic social engineering tactic designed to override rational thinking.

Hyperlink Analysis

The embedded link:

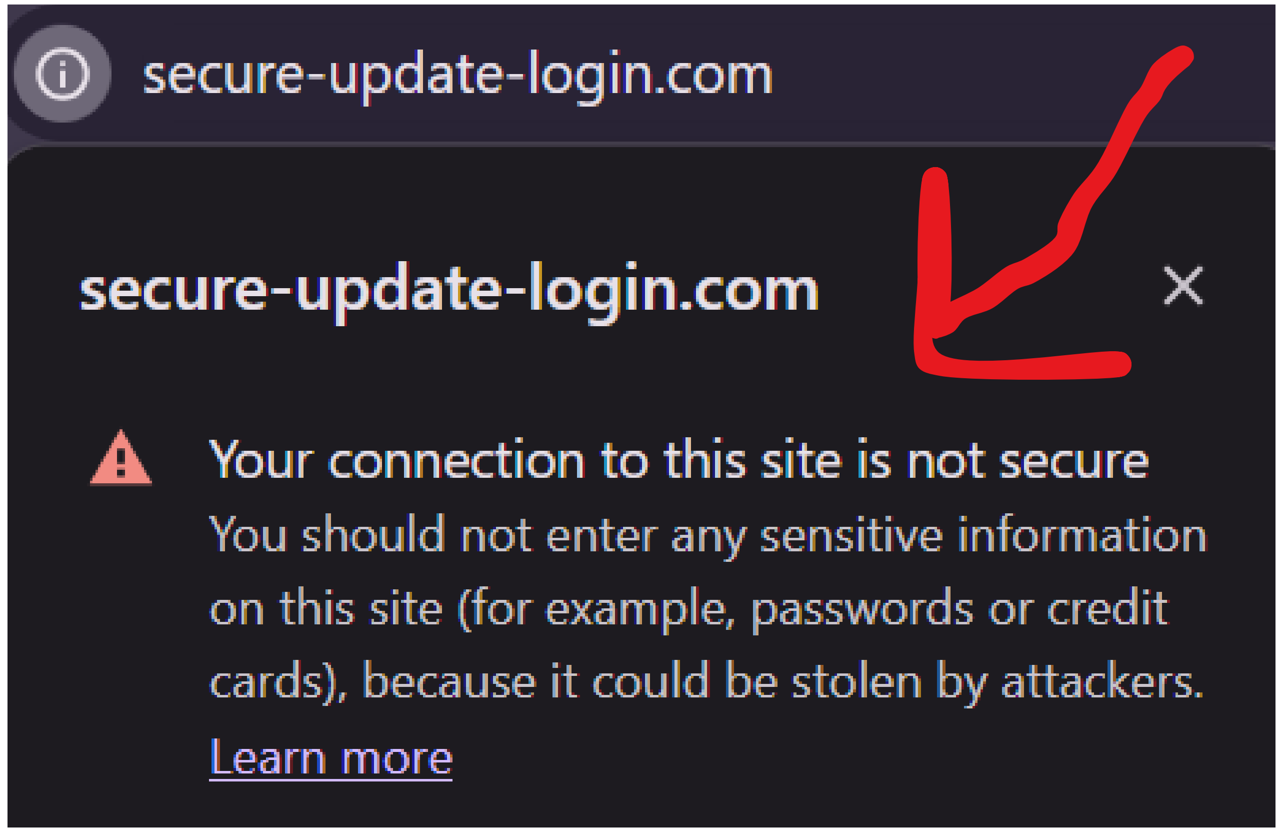
http://secure-update-login.com

Observations:

- Not HTTPS secured
- Domain unrelated to official institution
- Contains misleading keywords ("secure", "login")

Security Interpretation:

Phishing links often contain security-related words to appear legitimate. However, domain inspection reveals the link is not associated with a trusted organization.



secure-update-login.com

secure-update-login.com

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers.

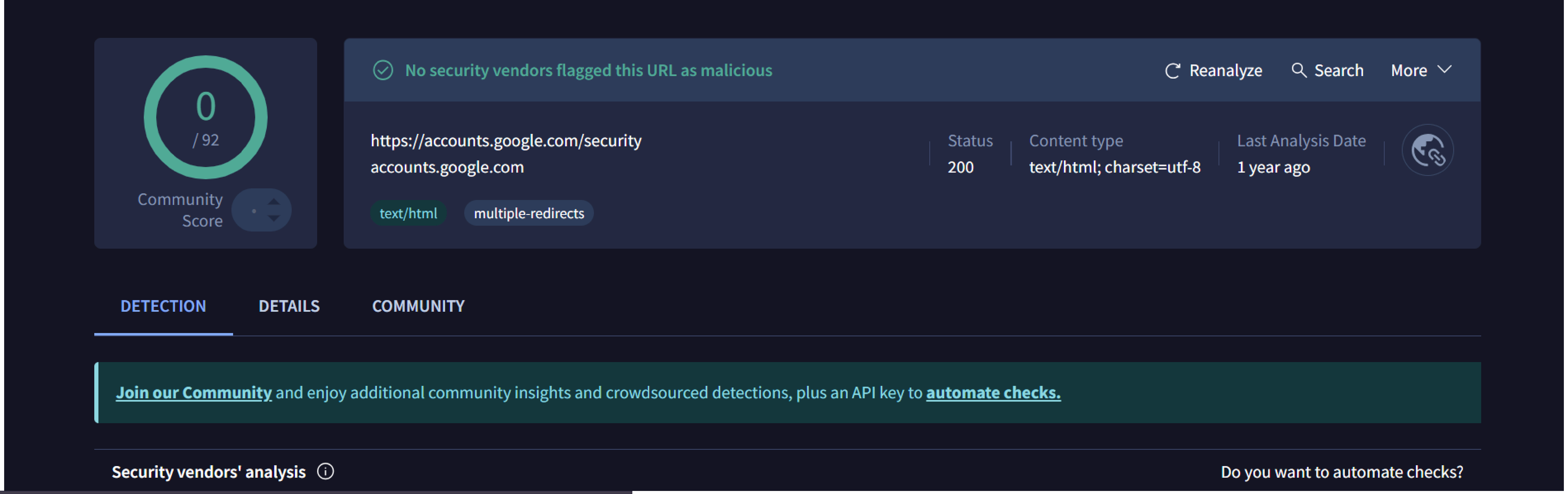
Learn more

8.Safe Email Comparison (With 2-Step Verification Enabled)

A legitimate email account with 2-Step Verification enabled was examined for comparison.

Security Feature	Suspicious Email	Legitimate Email
SPF	Fail	Pass
DKIM	None	Pass
DMARC	Fail	Pass
HTTPS Link	No	Yes
2-Step Verification	Not enforced	Enabled

The legitimate email demonstrates proper authentication and domain security configuration



0 / 92

Community Score

No security vendors flagged this URL as malicious

https://accounts.google.com/security
accounts.google.com

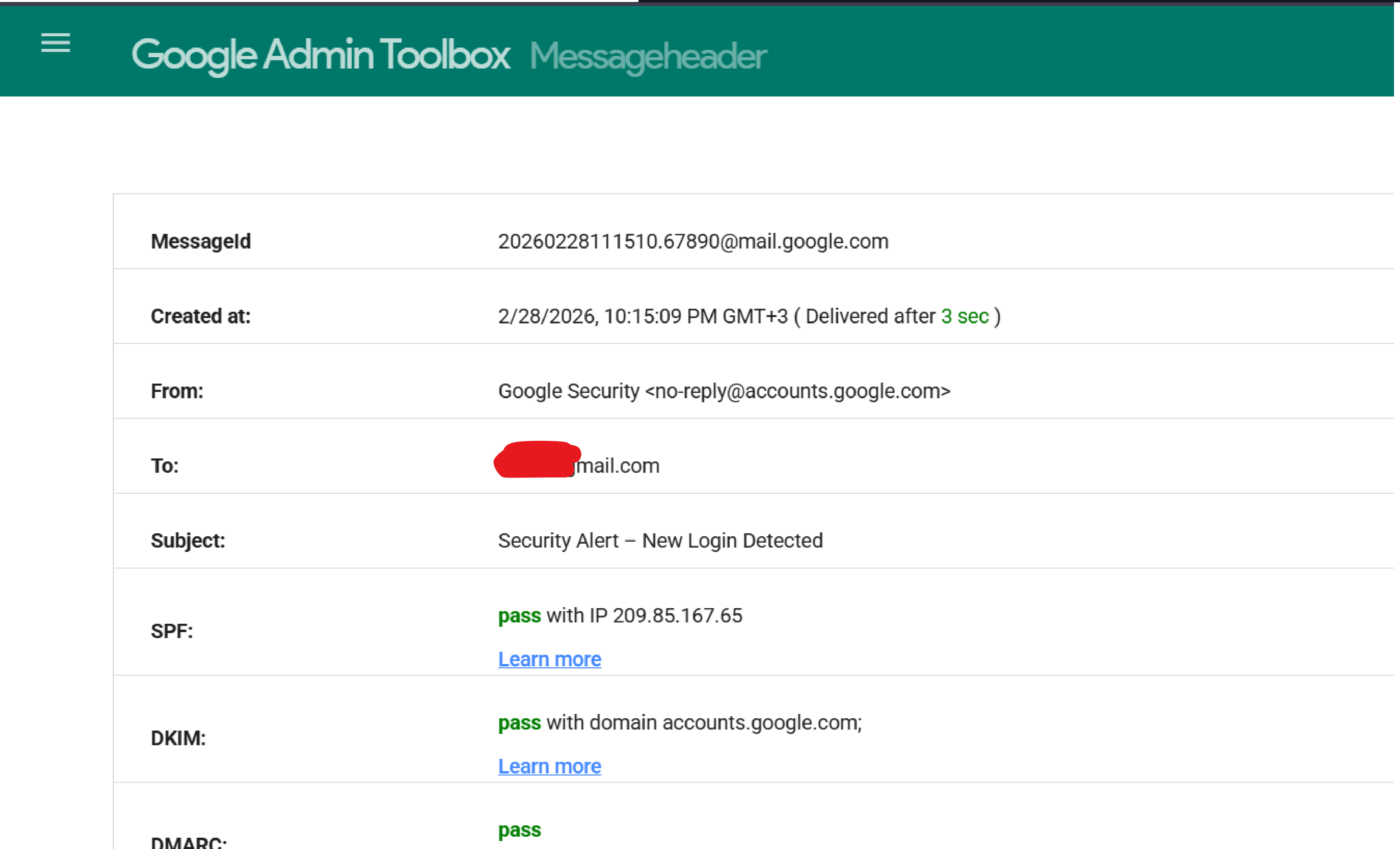
Status	Content type	Last Analysis Date
200	text/html; charset=utf-8	1 year ago

text/html multiple-redirects

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?



Google Admin Toolbox Messageheader

MessageId	20260228111510.67890@mail.google.com
Created at:	2/28/2026, 10:15:09 PM GMT+3 (Delivered after 3 sec)
From:	Google Security <no-reply@accounts.google.com>
To:	[redacted]mail.com
Subject:	Security Alert – New Login Detected
SPF:	**pass** with IP 209.85.167.65 Learn more
DKIM:	**pass** with domain accounts.google.com; Learn more
DMARC:	**pass**

9.Risk Assessment

Based on header authentication failures and content analysis, the email is classified as:

High Risk – Confirmed Phishing Attempt

The email demonstrates spoofing behavior and social engineering techniques designed to steal user credentials.

10.Security Recommendations

To mitigate phishing risks:

- Enable 2-Step Verification (2SV) on all accounts
- Verify sender domain before clicking links
- Inspect email headers when suspicious
- Avoid clicking unknown links
- Implement SPF, DKIM, and DMARC in organizational domains
- Report phishing emails to security teams

11.Conclusion

The investigation confirms that the analyzed email is a phishing attempt.
Authentication failures (SPF, DKIM, DMARC), suspicious routing paths, and social engineering indicators strongly suggest malicious intent. Users and organizations must implement layered email security controls to prevent credential compromise.

12. Disclaimer

This report was prepared for academic and cybersecurity training purposes only. The email samples, header data, and analysis presented in this document are used strictly for educational investigation and awareness development.
No real financial institutions or individuals were intentionally targeted or harmed during this analysis. Any domain names, email addresses, or links referenced in this report are either simulated or used solely for demonstration purposes.
The findings in this report are based on the available evidence at the time of analysis and are intended to demonstrate phishing detection techniques and email security evaluation methods.