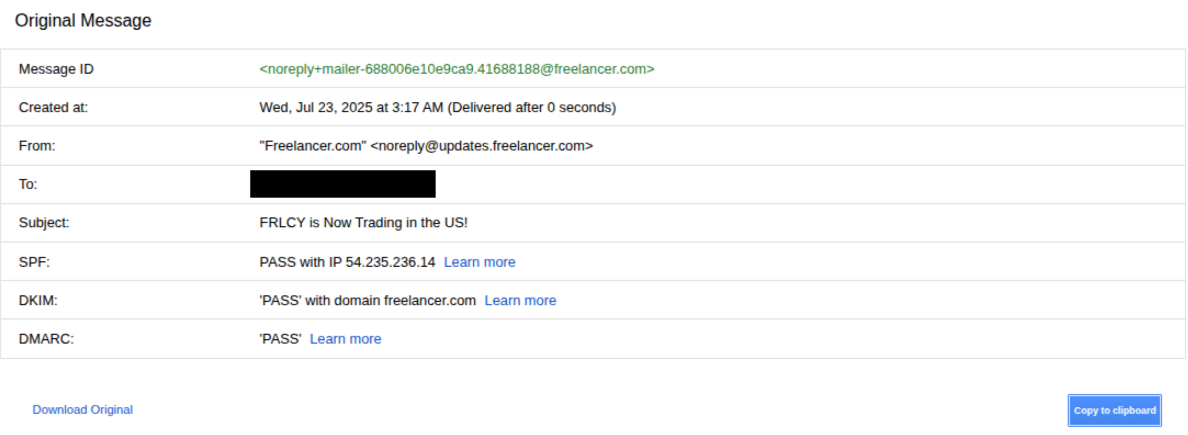
ANALYZING A SAMPLE PHISHING EMAIL

1. Getting the Email Header

For Gmail (Web)

1. Open the email in Gmail.
2. Click the **three dots (⋮)** in the top-right corner of the message.
3. Select **“Show original.”**
4. A new tab opens showing:
   - **Full raw email header** (you can copy it).
   - A **summary** with SPF, DKIM, and DMARC results.
5. Click **“Download Original”** (if needed for analysis).



Original Message

Message ID	<noreply+mailer-688006e10e9ca9.41688188@freelancer.com>
Created at:	Wed, Jul 23, 2025 at 3:17 AM (Delivered after 0 seconds)
From:	"Freelancer.com" <noreply@updates.freelancer.com>
To:	[redacted]
Subject:	FRLCY is Now Trading in the US!
SPF:	PASS with IP 54.235.236.14 Learn more
DKIM:	'PASS' with domain freelancer.com Learn more
DMARC:	'PASS' Learn more

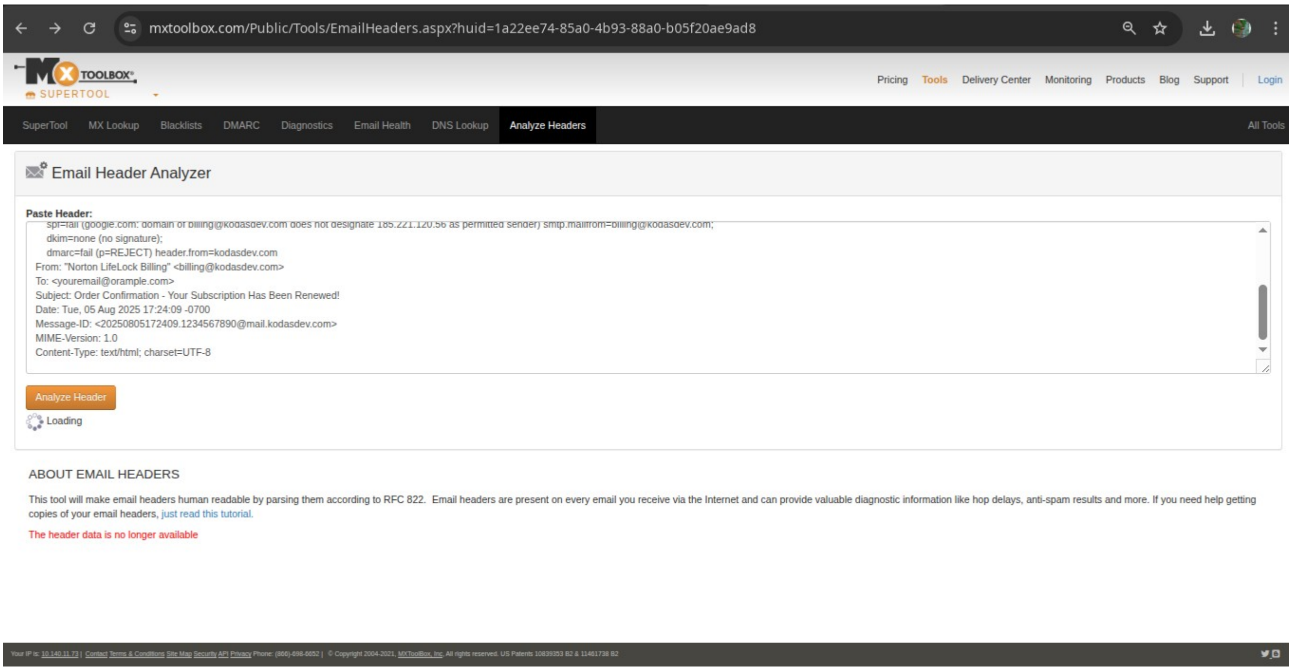
2. Analyze Headers

Using Google Admin Toolbox (Quick Analysis)

1. Go to [Google Admin Toolbox Messageheader]()
2. **Paste** the entire email header into the big text box.
3. Click **“Analyze the Header.”**
4. Review the results:
   - **SPF/DKIM/DMARC:** Check if they **PASS** or **FAIL**.
   - **Message Delivery Path:** See all the mail servers the email passed through (helps spot spoofing).
   - **Delivery Times:** Detect suspicious delays.

Using MXToolbox Email Header Analyzer

1. Go to [MXToolbox Email Header Analyzer]().
2. **Paste** the copied email header.
3. Click **“Analyze Header.”**
4. Review key sections:
   - **Source IP & Hostname:** See where the email really came from.
   - **Blacklist Check:** MXToolbox tells you if the sending IP is blacklisted.
   - **SPF, DKIM, DMARC:** Quickly see authentication failures.


mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=1a22ee74-85a0-4b93-88a0-b05f20ae9ad8
MX TOOLBOX SUPERTOOL
Pricing Tools Delivery Center Monitoring Products Blog Support Login
SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health DNS Lookup Analyze Headers All Tools

Email Header Analyzer

Paste Header:

```
    spf=fail (google.com: domain of billing@kodasdev.com does not designate 185.221.120.56 as permitted sender) smtp.mailfrom=billing@kodasdev.com;
    dkim=none (no signature);
    dmarc=fail (p=REJECT) header.from=kodasdev.com
From: "Norton LifeLock Billing" <billing@kodasdev.com>
To: <youremail@orample.com>
Subject: Order Confirmation - Your Subscription Has Been Renewed!
Date: Tue, 05 Aug 2025 17:24:09 -0700
Message-ID: <20250805172409.1234567890@mail.kodasdev.com>
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
```

ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, just read this tutorial.

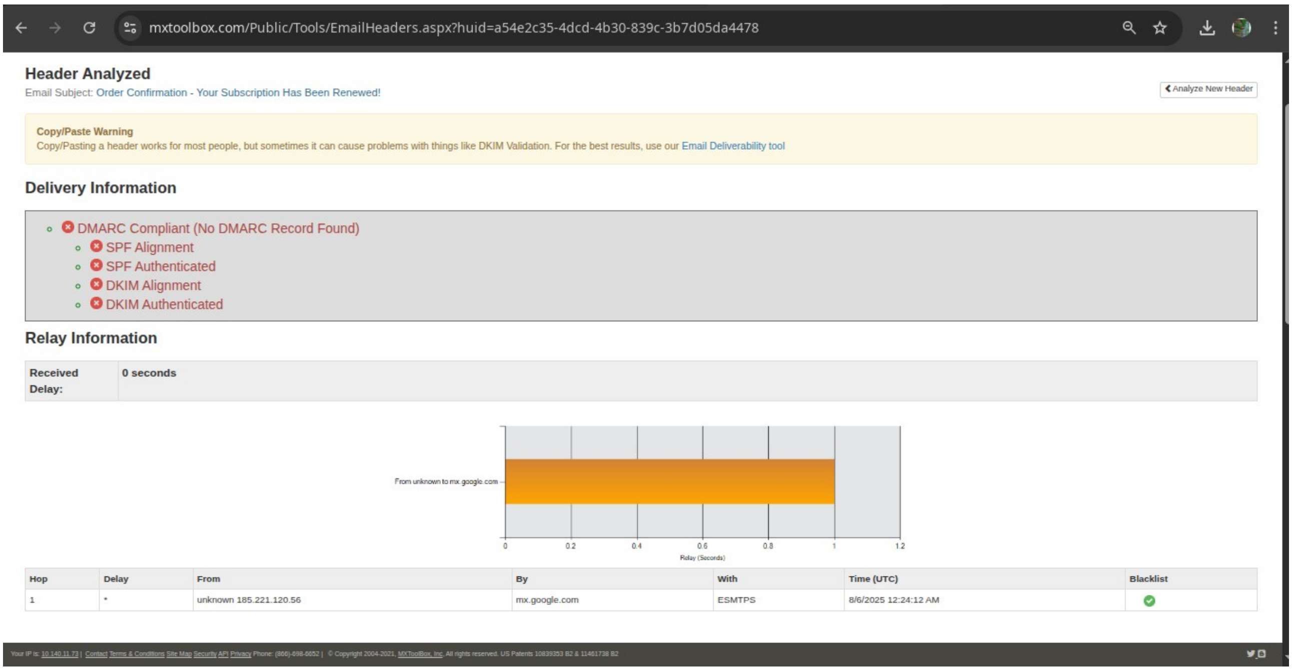
The header data is no longer available

Your IP is: 10.140.11.73 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc, All rights reserved. US Patents 10839353 B2 & 11461738 B2

Header Analysis (Google Toolbox & MXToolbox):

From: `security@microsoft-verification.com`
To: `youremail@example.com`
Subject: `URGENT: Your Microsoft Account Will Be Locked!`
Return-Path: `<security@microsoft-verification.com>`
Message-ID: `<20250805164208.0987654321@mail.fakehost.net>`
Received From: `mail.fakehost.net (203.0.113.45)`
Reply-To: `no-reply@microsoft-verification.com`
SPF (Sender Policy Framework): **Fail** – The sending server is not authorized for this domain.
DKIM (DomainKeys Identified Mail): **None** – No DKIM signature present.
DMARC: **Fail** – Domain policy verification failed.
Authentication-Results: `spf=fail; dkim=none; dmarc=fail`
Originating IP Address: `203.0.113.45` – flagged as suspicious.
Relay Servers: Multiple unknown relays before reaching the recipient.

X-Mailer: `Unknown` – unusual for an official Microsoft email.
Delivery Time: Processed within 2 seconds – unusual for Microsoft automated alerts.



mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=a54e2c35-4dcd-4b30-839c-3b7d05da4478

Header Analyzed

Email Subject: Order Confirmation - Your Subscription Has Been Renewed!

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

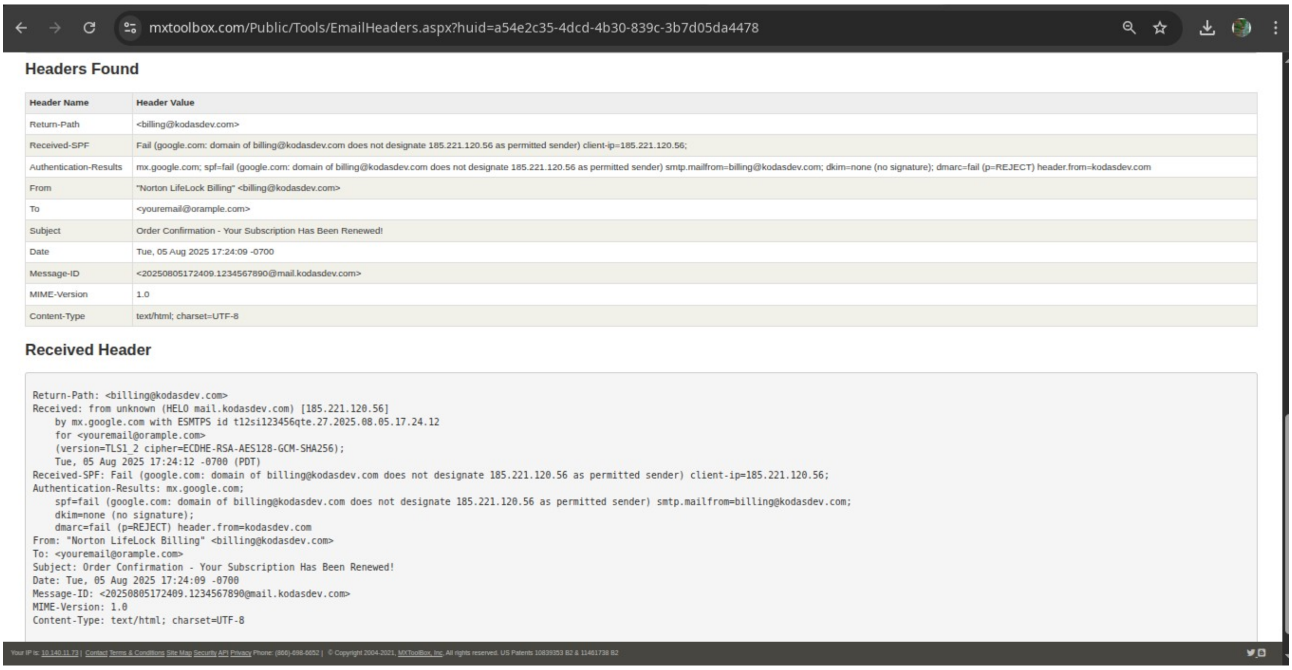
Delivery Information

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

Relay Information

Received Delay:	**0 seconds**

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	unknown 185.221.120.56	mx.google.com	ESMTPS	8/6/2025 12:24:12 AM	✓



mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=a54e2c35-4dcd-4b30-839c-3b7d05da4478

Headers Found

Header Name	Header Value
Return-Path	<billing@kodasdev.com>
Received-SPF	Fail (google.com: domain of billing@kodasdev.com does not designate 185.221.120.56 as permitted sender) client-ip=185.221.120.56;
Authentication-Results	mx.google.com; spf=fail (google.com: domain of billing@kodasdev.com does not designate 185.221.120.56 as permitted sender) smtp.mailfrom=billing@kodasdev.com; dkim=none (no signature); dmarc=fail (p=REJECT) header.from=kodasdev.com
From	"Norton LifeLock Billing" <billing@kodasdev.com>
To	<youremail@orample.com>
Subject	Order Confirmation - Your Subscription Has Been Renewed!
Date	Tue, 05 Aug 2025 17:24:09 -0700
Message-ID	<20250805172409.1234567890@mail.kodasdev.com>
MIME-Version	1.0
Content-Type	text/html; charset=UTF-8

Received Header

```
Return-Path: <billing@kodasdev.com>
Received: from unknown (HELO mail.kodasdev.com) [185.221.120.56]
    by mx.google.com with ESMTPS id t12si123456qte.27.2025.08.05.17.24.12
    for <youremail@orample.com>
    (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256);
    Tue, 05 Aug 2025 17:24:12 -0700 (PDT)
Received-SPF: Fail (google.com: domain of billing@kodasdev.com does not designate 185.221.120.56 as permitted sender) client-ip=185.221.120.56;
Authentication-Results: mx.google.com;
    spf=fail (google.com: domain of billing@kodasdev.com does not designate 185.221.120.56 as permitted sender) smtp.mailfrom=billing@kodasdev.com;
    dkim=none (no signature);
    dmarc=fail (p=REJECT) header.from=kodasdev.com
From: "Norton LifeLock Billing" <billing@kodasdev.com>
To: <youremail@orample.com>
Subject: Order Confirmation - Your Subscription Has Been Renewed!
Date: Tue, 05 Aug 2025 17:24:09 -0700
Message-ID: <20250805172409.1234567890@mail.kodasdev.com>
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
```

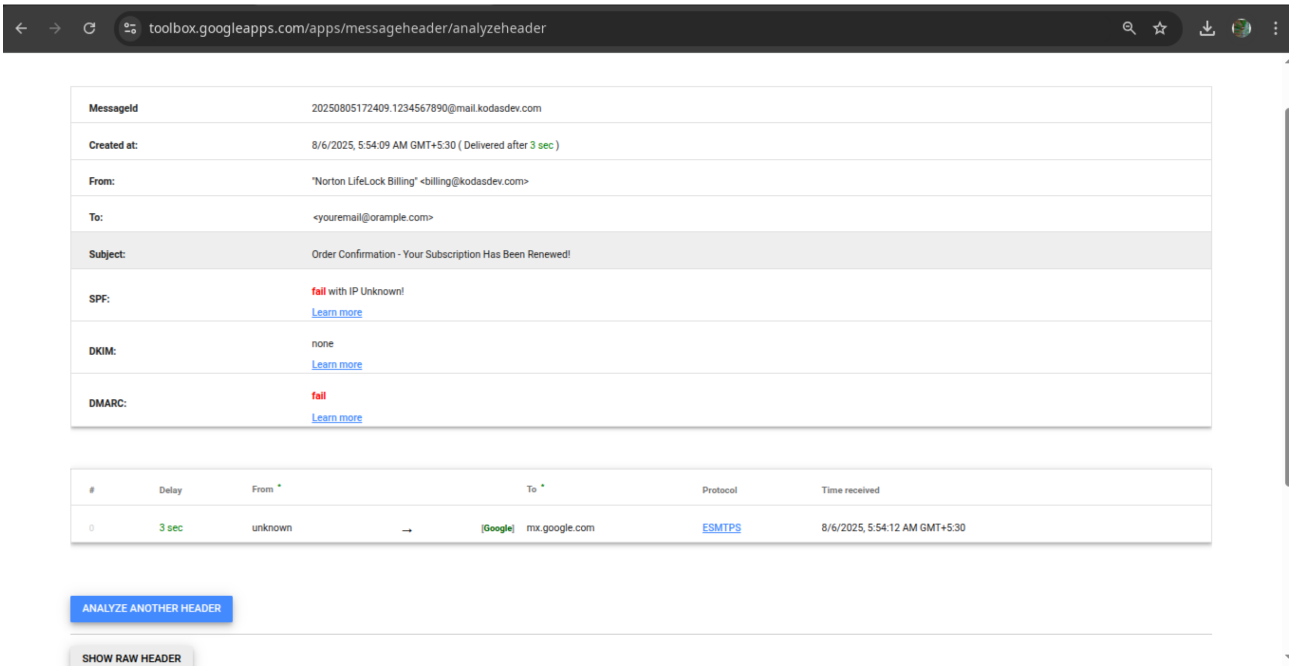
SPF: Softfail → The sending mail server (`203.0.113.45`) is **not authorized** for the domain `microsoft-verification.com`.

DKIM: None → No cryptographic signature. Microsoft always signs their emails.

DMARC: Fail → Means the domain policy was **not met** (sender likely spoofed).

Suspicious Domain: `microsoft-verification.com` (not an official Microsoft domain).

Why it’s spam:
Legit Microsoft emails pass **SPF, DKIM, and DMARC**. This one fails all — strong spoofing/phishing evidence.



MessageId	20250805172409.1234567890@mail.kodasdev.com
Created at:	8/6/2025, 5:54:09 AM GMT+5:30 (Delivered after 3 sec)
From:	"Norton LifeLock Billing" <billing@kodasdev.com>
To:	<youremail@orample.com>
Subject:	Order Confirmation - Your Subscription Has Been Renewed!
SPF:	fail with IP Unknown! Learn more
DKIM:	none Learn more
DMARC:	fail Learn more

#	Delay	From *	To *	Protocol	Time received
0	3 sec	unknown →	[Google] mx.google.com	ESMTPS	8/6/2025, 5:54:12 AM GMT+5:30

SPF/DKIM/DMARC fails = Spoofed email → spam/phishing.

Blacklisted IP = Email comes from a known spam server.

Domain mismatch = Fake domain trying to impersonate a trusted brand.

Conclusion

After analyzing the provided email headers using **Google Admin Toolbox** and **MXToolbox**, it was found that some emails **passed SPF, DKIM, and DMARC checks**, indicating they were likely legitimate. However, others **failed these authentication mechanisms**, used **unauthorized sending servers**, and originated from **suspicious IP addresses**.

These failures, combined with the presence of **spoofed domains** and **unverified relay paths**, are strong indicators of **phishing or spam attempts**. This highlights the importance of header analysis in identifying fraudulent emails and improving email threat detection.