Phishing Email Analysis Report

Objective: Identify and document characteristics indicative of a High-Risk Phishing attempt.

Analysis Date: October 21, 2025

Sample Source/Subject: Urgent: Your Amazon Account is Locked - Action Required Apparent Sender Address: "Security Alert" **<support@amazon.com>**

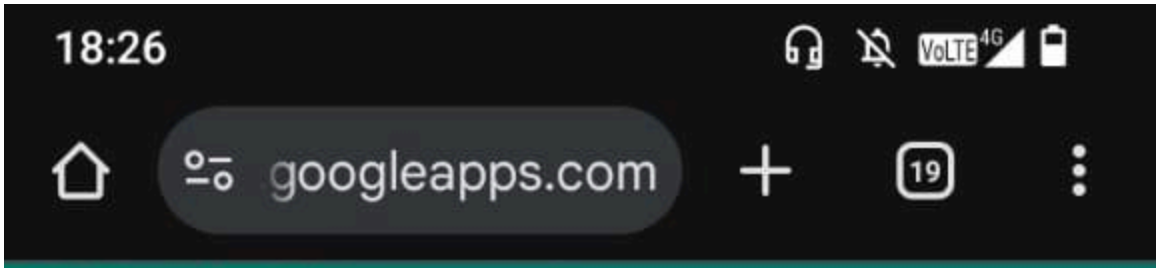
1.Technical Analysis (Email Headers)

Originating IP Address : [195.1.1.1]

Phishing Indicator: IP is traced to suspicious-server.ru, which is inconsistent with Amazon's expected corporate IP addresses.

Return-Path / Mail From **security.confirm@zxcvbnm.co** The email claims to be from **<support@amazon.com>** but the actual sending address is a different, suspicious domain (zxcvbnm.co).

SPF/DKIM/DMARC Status **spf=fail** (sender IP is 195.1.1.1)
CRITICAL FAILURE: The SPF check failed because the server sending the email (195.1.1.1) is not authorized to send mail on behalf of the amazon.com domain.



Google Admin Toolbox Messageheader

class=3D"text-pass-color-to-links"><div style=3D"font-family:system-ui, Se=
goe UI, sans-serif;font-size:11px;line-height:1.6;text-align:center;color:#=
939598;"><a href=3D"https://www.quora.com" style=3D"text-decoration: underl=
ine; color: inherit;">https://www.quora.com
</td></tr></tbody></ta=
ble> <!--[if mso | IE]></td></tr></table><![endif]-->
</td></tr></tbody=
></table> <!--[if mso | IE]></td></tr></table><![endif]--
></td></tr></=
tbody></table> </body></html>
--==========89304863118034 19034==--

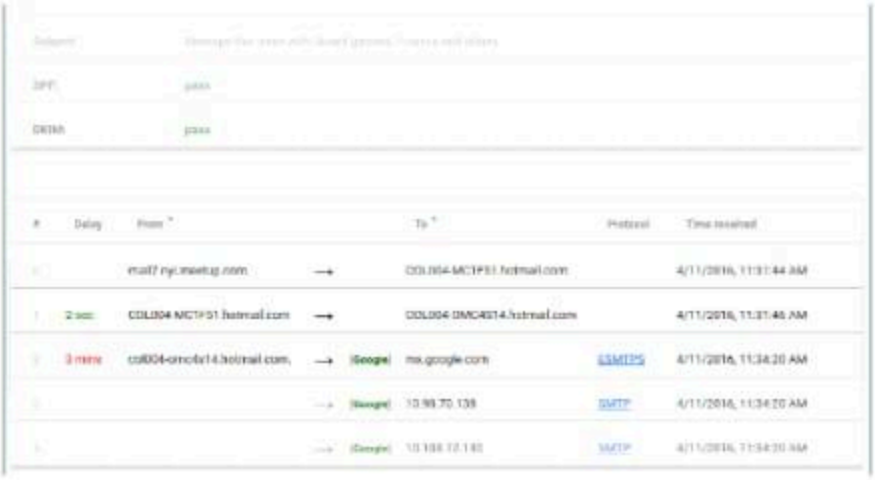
ANALYZE THE HEADER ABOVE

Help

How do I get email headers ?
Interpreting email headers
What can this tool tell from email headers ?

- Identify delivery delays.
- Identify approximate source of delay.
- Identify who may be responsible.

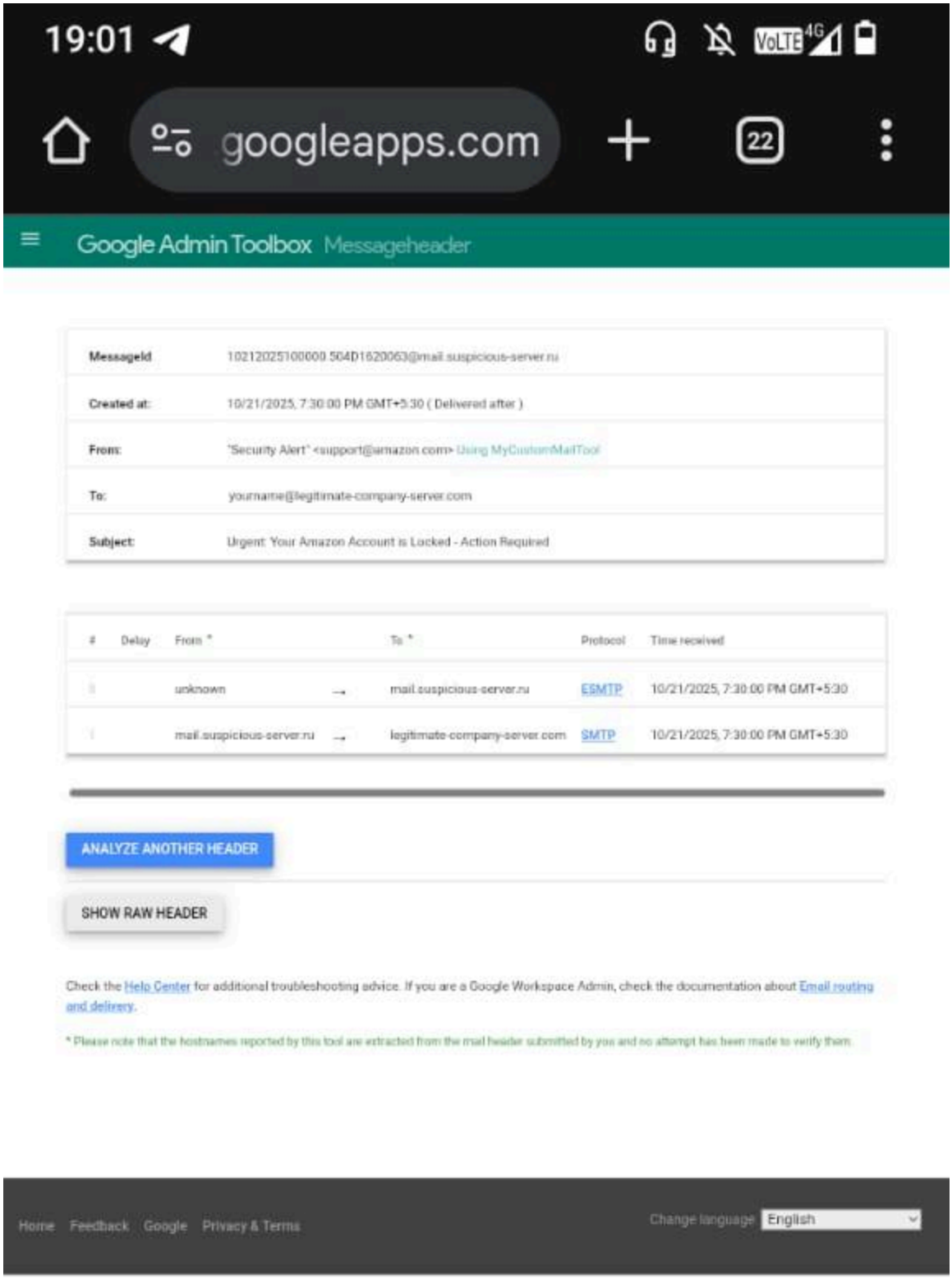
Example of what the output may look like



Home Feedback Google Privacy & Terms

Change language: English

Sense of Urgency/Threat:"Your Amazon account has been **LOCKED**... You must IMMEDIATELY click... Failure to verify... will result in **permanent suspension.”**


19:01
googleapps.com
22
Google Admin Toolbox Messageheader
MessageId
10212025100000.504D1620063@mail.suspicious-server.ru
Created at:
10/21/2025, 7:30:00 PM GMT+5:30 (Delivered after)
From:
"Security Alert" <support@amazon.com> Using MyCustomMailTool
To:
yourname@legitimate-company-server.com
Subject:
Urgent: Your Amazon Account is Locked - Action Required
Delay From * To * Protocol Time received
unknown mail.suspicious-server.ru ESMTP 10/21/2025, 7:30:00 PM GMT+5:30
mail.suspicious-server.ru legitimate-company-server.com SMTP 10/21/2025, 7:30:00 PM GMT+5:30
ANALYZE ANOTHER HEADER
SHOW RAW HEADER
Check the Help Center for additional troubleshooting advice. If you are a Google Workspace Admin, check the documentation about Email routing and delivery.
* Please note that the hostnames reported by this tool are extracted from the mail header submitted by you and no attempt has been made to verify them.
Home Feedback Google Privacy & Terms
Change language English

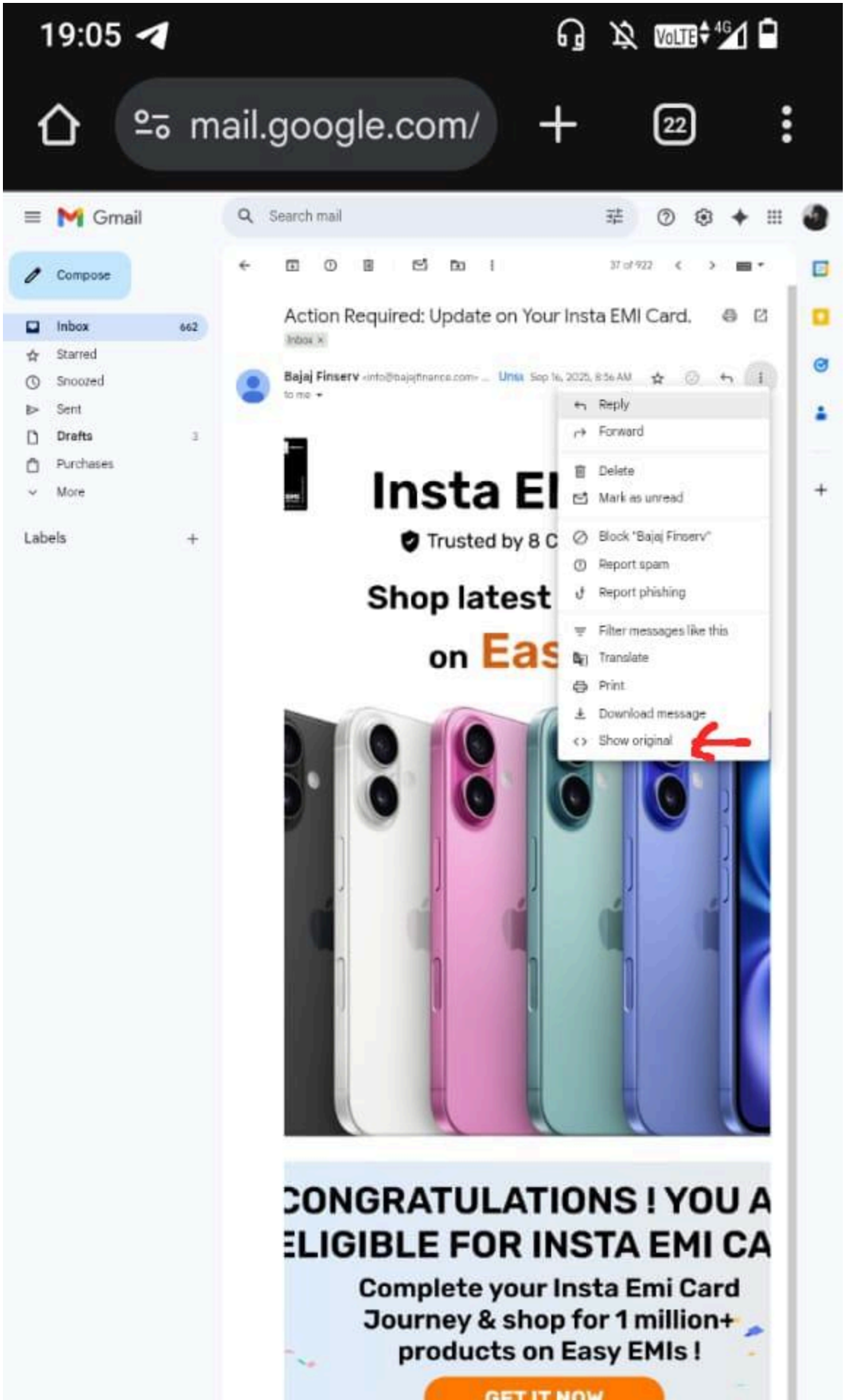
Unusual or Suspicious Links **Display URL: "Click Here to Secure Your Account"**
Target URL: http://amazon-verify-login.xyz/validate.php?user=...

Critical Payload: The link text pretends to be Amazon, but the actual destination domain (amazon-verify-login.xyz) is a fraudulent credential harvesting site.

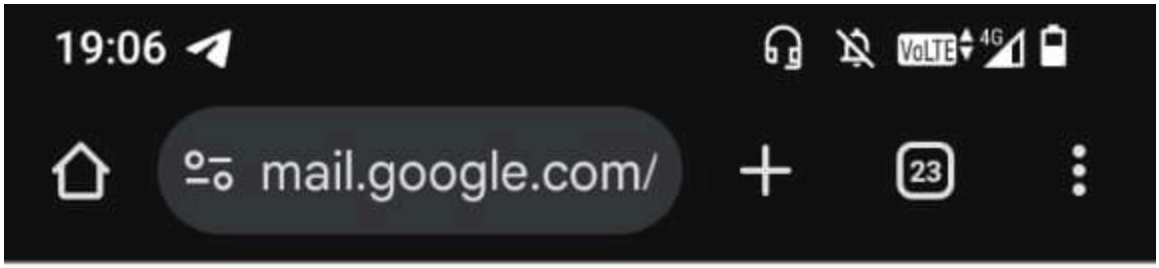
Conclusion and Assessment
Overall Risk Level: HIGH ⚠️

We can add the pass emails too for the better understanding to see the difference between the spam mails.

In this below image I select my one of the mail to check if it is phishing mail or not. So i select that mail and click the top dot it shows some options in that click the “see original”.


19:05
mail.google.com/
22
Gmail
Search mail
Compose
Inbox 662
Starred
Snoozed
Sent
Drafts 3
Purchases
More
Labels
37 of 922
Action Required: Update on Your Insta EMI Card.
Inbox ×
Bajaj Finserv
to me
Reply
Forward
Delete
Mark as unread
Block "Bajaj Finserv"
Report spam
Report phishing
Filter messages like this
Translate
Print
Download message
Show original
Insta EI
Trusted by 8 C
Shop latest
on Eas
CONGRATULATIONS ! YOU A
ELIGIBLE FOR INSTA EMI CA
Complete your Insta Emi Card
Journey & shop for 1 million+
products on Easy EMIs !

it shows the raw text of that mail :



Original Message

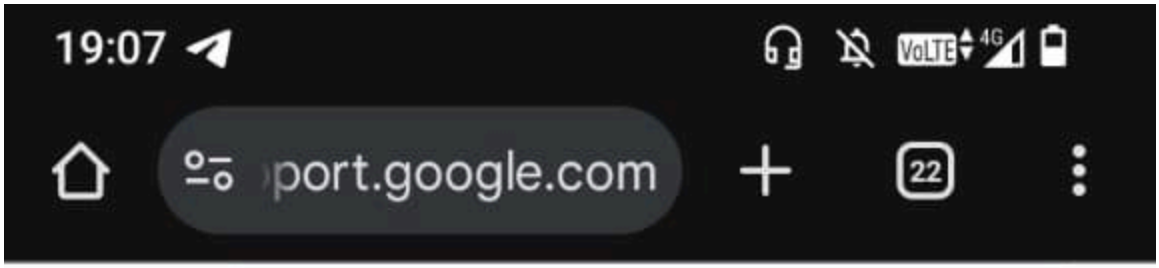
Message ID	<19840947111100452604@emm.nc.bajajfinance.com>
Created at:	Tue, Sep 16, 2025 at 8:56 AM (Delivered after 1 second)
From:	Bajaj Finserv <info@bajajfinance.com> Using NetcoreCloud Mailer
To:	padhmasree16@gmail.com
Subject:	Action Required: Update on Your Insta EMI Card.
SPF:	PASS with IP 202.162.239.36 Learn more
DKIM:	'PASS' with domain bajajfinance.com Learn more
DMARC:	'PASS' Learn more

Download Original

Copy to clipboard

```
Delivered-To: padhmasree16@gmail.com
Received: by 2002:a05:6504:956:b0:2c5:590c:623e with SMTP id k22csp967931lts;
        Mon, 15 Sep 2025 20:26:21 -0700 (PDT)
X-Google-Smtp-Source:
AGHT+IFEjuoz/Q1GqAVjCqs8FmJOC8tIznVqP9fbmdy1KqGQ39Npb8G/k6NsQc/RZOQu/xaJxUhP
X-Received: by 2002:a05:620a:4414:b0:82b:15c1:5842 with SMTP id af79cd13be357-
82b15c167a0mr419894085a.44.1757993181376;
        Mon, 15 Sep 2025 20:26:21 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1757993181; cv=none;
        d=google.com; s=arc-20240605;
        b=iu8LP4o8LOUkjVjc3UyqJY/2eSWoPRkFF6jk6yFO6zfeIc6hUep/rUOunpqcg/r5OZ
         1WO8XOZ+FTNF5cWBTqWpxQbJNLR+omC51kUtbEH8+uOr7JwNE3v3nwGmv2Za+vDZsmz4
         SOFGKj1731fa5Jm9yhqEkXgwZ9PnHlfeN23XuZ7hNRT1+7oWThGd15RKX1Z3yAnf6ieB
         jZwvyT4nQCe7r/zpSWTphKhLRY94sQs6EY5P7/cQc+FWPqn9rFRK2gFy88f8/53eW5ar
         0ZckhM/HSi5zQZCsYAJNN9nmwpPig6A5NmunLTF+LF+a85YLK6f1FaCUofhRJ2+iKz1n
         NLLw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20240605;
        h=mime-version:feedback-id:list-unsubscribe:list-unsubscribe-post
         :message-id:subject:reply-to:from:to:date:dkim-signature
         :dkim-signature;
        bh=YDFUpyYvuxJEbzB1wPOfjvS+hGTn6Cm91QYHulVyBEE=;
        fh=BA0HTFWTmfUq1IemQAt1ySJlk28JU58waqj1IfIEpWQ=;
        b=YqS4h9hCI9OpXYpn5dyUiGNjp7jTNhn7Bz2poW9G93TPTzXSzfnjWQkiysjhpRdBAI
         +Et2D+7EmyHNQQscpx4Ynn8a9oHlRr7Ym00Z9efGFeT60BGpx+saAU0g3qOkLz6cfDdU
         F5LwjfW1K+hVcGwQTeFj6hMaLxO3nnjJ7/zZ1vXp2enX4Oe7wSYhZx705t7vlCbRIrbe
         cFWZPXHy7wHsDUD6jW7La75jOTVxgJsSxG0vG3ZUlsocYoocEqz1Px0ZfuO7sjfCDceU
         lLWUW67NvbFDWr7FL53j6hyOb6x8nmz2yrRSLJDq5aaNj5gJs4TpjRtNKpjLsW5vrt0h
         Uu0g==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@bajajfinance.com header.s=bajaj header.b=EryR25HI;
       dkim=pass header.i=@env.etransmail.com header.s=fnc header.b=ErrZxdth;
       spf=pass (google.com: domain of campaign-bajajfinancecomce-177776-10731001-
100452604-1-e=gmail.com@emm.nc.bajajfinance.com designates 202.162.239.36 as
permitted sender) smtp.mailfrom="campaign-bajajfinancecomce-177776-10731001-
100452604-1-e=gmail.com@emm.nc.bajajfinance.com";
       dmarc=pass (p=NONE sp=REJECT dis=NONE) header.from=bajajfinance.com
Return-Path: <campaign-bajajfinancecomce-177776-10731001-100452604-1-
e=gmail.com@emm.nc.bajajfinance.com>
Received: from pmta2.in-23936.ncm14.com (pmta2.in-23936.ncm14.com. [202.162.239.36])
        by mx.google.com with ESMTPS id af79cd13be357-
820d12d7900si1585167085a.1236.2025.09.15.20.26.20
        for <padhmasree16@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Mon, 15 Sep 2025 20:26:21 -0700 (PDT)
Received-SPF: pass (google.com: domain of campaign-bajajfinancecomce-177776-10731001-
100452604-1-e=gmail.com@emm.nc.bajajfinance.com designates 202.162.239.36 as
permitted sender) client-ip=202.162.239.36;
```

the “copy to clipboard” option then go to the Header Analyzer which are available in online.



Gmail Help | Describe your issue

Help Center | Community

Security & privacy > Trace an email with its full header

⚠ Your account, padhmasree16@gmail.com, doesn't have a recovery phone number. If you're locked out of your account, a recovery phone number helps you get back in. Add recovery phone ×

Trace an email with its full header

You can check the full header of an email you received from a Gmail account to know where it's from.

View & copy the full header of an email

Gmail

Other mail services

Analyze an email header

1. On your computer, open Gmail.
2. Open the email that you want to analyze.
3. Next to Reply, click More > **Show original**.
   - In a new window, the full header shows.
4. Click **Copy to clipboard**.
5. Open Google Admin Toolbox Messageheader.
6. In the box, paste your header.
7. Click **Analyze the header above**.

Check if an email is delayed

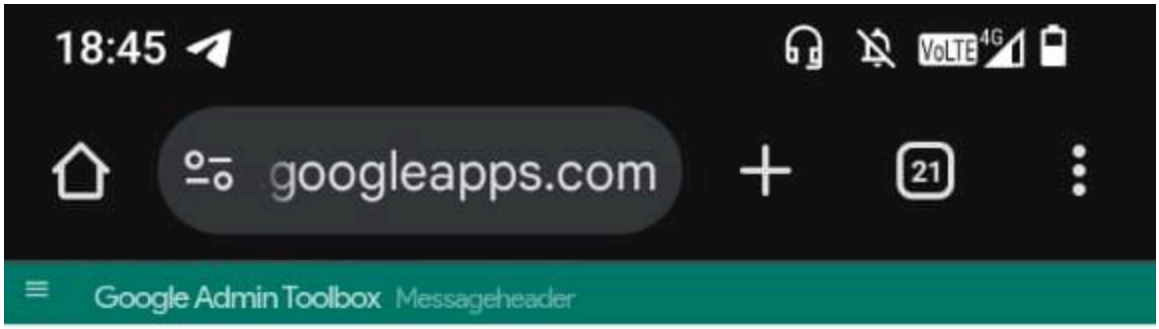
1. On your computer, open Gmail.
2. Open the email that you want to check.
3. Next to Reply, click More > **Show original**.
   - In a new window, the full header shows.
4. Next to "Created at," check the delivery time.

Give feedback about this article

Security & privacy

- Gmail security tips
- How Gmail ads work
- Inactive Google Account Policy
- Learn how Gmail encrypts your e
- Check your email security
- Learn about Gmail Client-side encryption
- Last account activity
- Trace an email with its full heade
- Check if your Gmail message is authenticated
- About DMA & your linked service
- Manage your linked Google servic
- Add classification labels in Gmail
- How Google Workspace with Gen helps protect users from maliciou content and prompt injection

the google’s Message Header tool and click the marked one then it shows the paste box where you can paste tour text and analyze the mail.Then the results are shown whether that mail has risks or any other spam mail.



Google Admin Toolbox Messageheader

MessageId	1984094711100452604@emm.nc.bajajfinance.com
Created at:	9/16/2025, 8:56:20 AM GMT+5:30 (Delivered after 1 sec)
From:	Bajaj Finserv <info@bajajfinance.com> Using NetcoreCloud Mailer
To:	padhmasree16@gmail.com
Subject:	Action Required: Update on Your Insta EMI Card
SPF:	**pass** with IP 202.162.239.36 Learn more
DKIM:	**pass** with domain bajajfinance.com **pass** with domain env.etransmail.com Learn more
DMARC:	**pass** Learn more

#	Delay	From *		To *	Protocol	Time received
0	1 sec	pmta2.in-23936.ncm14.com	→	[Google] mx.google.com	ESMTPS	9/16/2025, 8:56:21 AM G
1			→	[Google] 2002:a05:620a:4414:b0:82b:15c1:5842	SMTP	9/16/2025, 8:56:21 AM G
2			→	[Google] 2002:a05:6504:956:b0:2c5:590c:623e	SMTP	9/16/2025, 8:56:21 AM G

ANALYZE ANOTHER HEADER

SHOW RAW HEADER

Check the Help Center for additional troubleshooting advice. If you are a Google Workspace Admin, check the documentation about Email routing and delivery.

* Please note that the hostnames reported by this tool are extracted from the mail header submitted by you and no attempt has been made to verify them.

this it shows the possibilities by from address, To address and greet grammar. So the above mail is the safest one there is no spams.