

Mail header analysis



Address Details

Mail From:	security-update@amazon-account.com	Mail To:	victim@example.com
Mail From Name:	Amazon Security	Reply To:	support@amazon-account.com

Message Details

Subject:	Action Required: Account Access Suspended	Content-Type:	text/html charset=UTF-8
Date:	Wed, 6 Aug 2025 09:12:32 +0530	UTC Date	Wed Aug 6 03:42:32 2025
MessageID:	CAHk3+XYZ@example.com		

Message Transfer Agent (MTA) - Transfer Details

Mail Server From:	smtp-user.fakehost.net	Mail Server To:	
Mail Server From IP:	198.51.100.22	Mail Server To IP:	
Mail Country From:	 Country/Code/Continent: // Longitude:/ Latitude:	Mail Country To:	 Country/Code/Continent: // Longitude:/ Latitude:
AS Name From:		AS Name To:	
AS Number From:		AS Number To:	
Distance (All Hops/Summary):	0/ KM	Hops (All/Public):	2 /
MTA Encryption	Good (*)	Delivery Time:	0 days, 0 hours, 0 min, 1 sec
Your IP:	43.225.25.132	Your GeoLoc:	Lat:17.3724 Lon:78.4378

Daily hit counter = 7 of 25

Spam Scoring Details

Score	Spam Description
0.0	RBL: ADMINISTRATOR NOTICE: The query to
0.0	The body matches phrases such as "accounts
0.0	Missing DMARC policy
1.3	RBL: Relay in Validity RPBL,
-2	RBL: Sender in Validity Safe - Contact
-3	RBL: Sender in Validity Certification -
0.8	No valid author signature and domain not in DNS
0.0	SPF: HELO does not publish an SPF Record
1.3	Received: contains illegal IP address
0.1	BODY: Message only has text/html MIME parts
0.6	HTML-only message, but there is no HTML tag

Total Score (Max:5.0)	Spamassassin prediction
-0.898	No Spam = Good!

Hop Details

Hop 1/2	Public / Internal Mail Routing		
By MTA	inbound.example.com	By IP	UNKNOWN (*)
From AS Nbr		From AS Name	
From Geo	Lat: Lon:	From Next City	(*)
Date MTA	Wed, 6 Aug 2025 09:12:34 +0530	UTC Date	Wed Aug 6 03:42:34 2025
Epoch	1754467954	For	
MTA Encryption	Not encrypted (internal)		
MTA (Guess)	Postfix		
RAW MESSAGE	Received: from mx10.fakehost.net (mx10.fakehost.net [203.0.113.45]) by inbound.example.com (Postfix) with ESMTP id ABC123DEF; Wed, 6 Aug 2025 09:12:34 +0530 (IST)		

Hop 2/2	Public / Internal Mail Routing		
By MTA	mx10.fakehost.net	By IP	UNKNOWN (*)
From AS Nbr		From AS Name	
From Geo	Lat: Lon:	From Next City	(*)
Date MTA	Wed, 6 Aug 2025 09:12:33 +0530	UTC Date	Wed Aug 6 03:42:33 2025
Epoch	1754467953	For	
MTA Encryption	Not encrypted (internal)		
MTA (Guess)	Postfix		
RAW MESSAGE	Received: from smtp-user.fakehost.net (unknown [198.51.100.22]) by mx10.fakehost.net (Postfix) with ESMTP id XYZ789GHI; Wed, 6 Aug 2025 09:12:33 +0530 (IST) Received-SPF: fail (example.com: domain of amaz0n-		

account.com does not designate 203.0.113.45 as permitted sender)

X-Header

Mail header

```
Return-Path: <notification@amaz0n-account.com>
Received: from mx10.fakehost.net (mx10.fakehost.net [203.0.113.45])
    by inbound.example.com (Postfix) with ESMTP id ABC123DEF;
    Wed, 6 Aug 2025 09:12:34 +0530 (IST)
Received: from smtp-user.fakehost.net (unknown [198.51.100.22])
    by mx10.fakehost.net (Postfix) with ESMTP id XYZ789GHI;
    Wed, 6 Aug 2025 09:12:33 +0530 (IST)
Received-SPF: fail (example.com: domain of amaz0n-account.com does not designate
203.0.113.45 as permitted sender)
From: "Amazon Security" <security-update@amaz0n-account.com>
To: victim@example.com
Reply-To: support@amaz0n-account.com
Subject: Action Required: Account Access Suspended
Message-ID: <CAHk3+XYZ@example.com>
Date: Wed, 6 Aug 2025 09:12:32 +0530
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
```

[Go Back](#)[Send us your Feedback](#)[API-Wiki](#)[Privacy Policy](#)