Task 2: Analyze a Phishing Email Sample

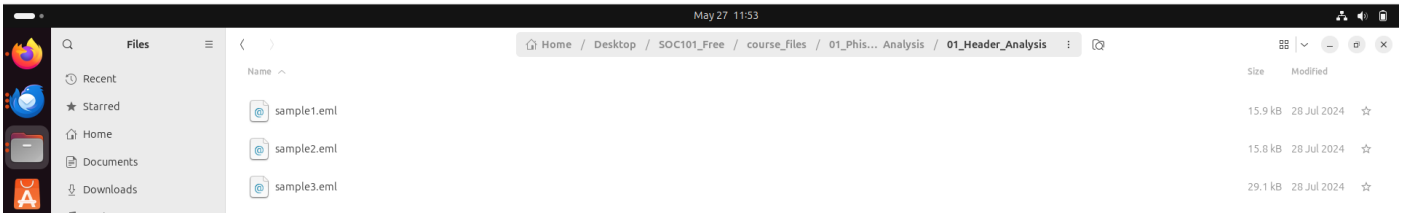
Objective: Identify phishing characteristics in a suspicious email sample.

Tools: Email client or saved email file (text), free online header analyzer.

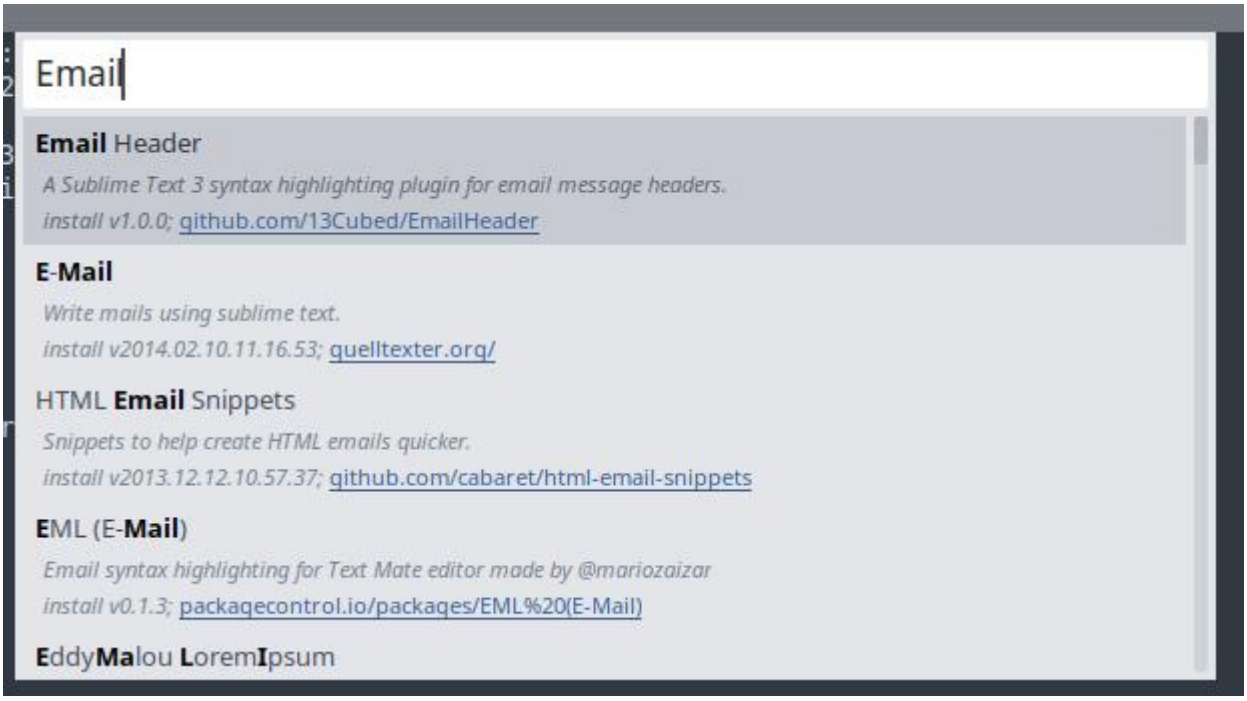
Deliverables: A report listing phishing indicators found

MANUAL APPROACH

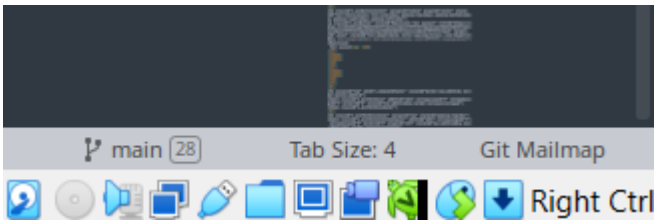
1. These are the phishing mail samples that I have got online that I can use for analysis of the headers, and we are focusing the sample named the sample1.eml

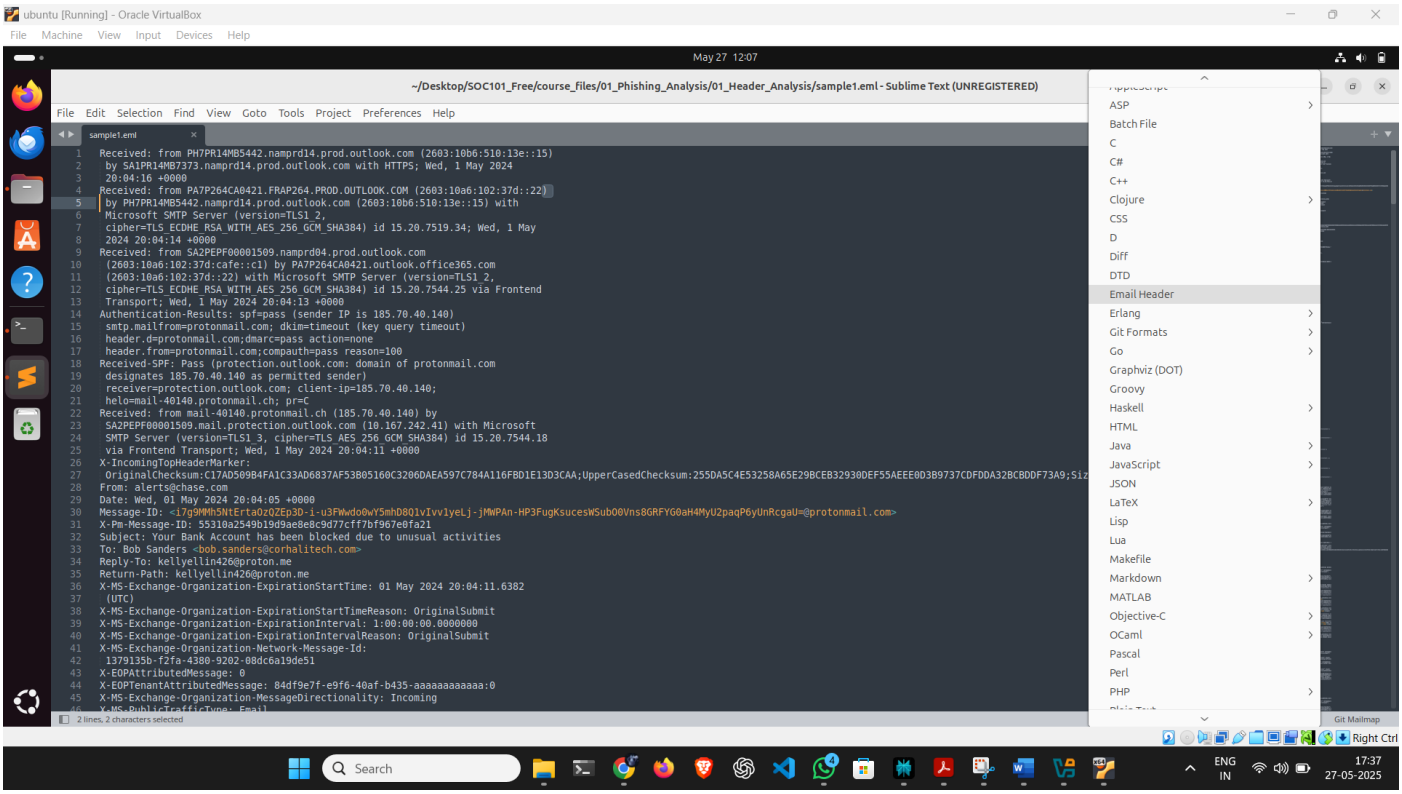


- I am using the Sublime Text document viewer to view the source code of the email, along with a package called "Email Header" that highlights the headers inside the source code.
- To install it, click on **Tools** in the Sublime Text toolbar and select **Install Package**. Then, press Ctrl + Shift + P to open the Command Palette, type "Install Package," and press Enter. Next, type "Email Header" (the syntax highlighting plugin) and install it.
- This process will enable syntax highlighting for email headers, making it easier to analyze and review the email's source code.

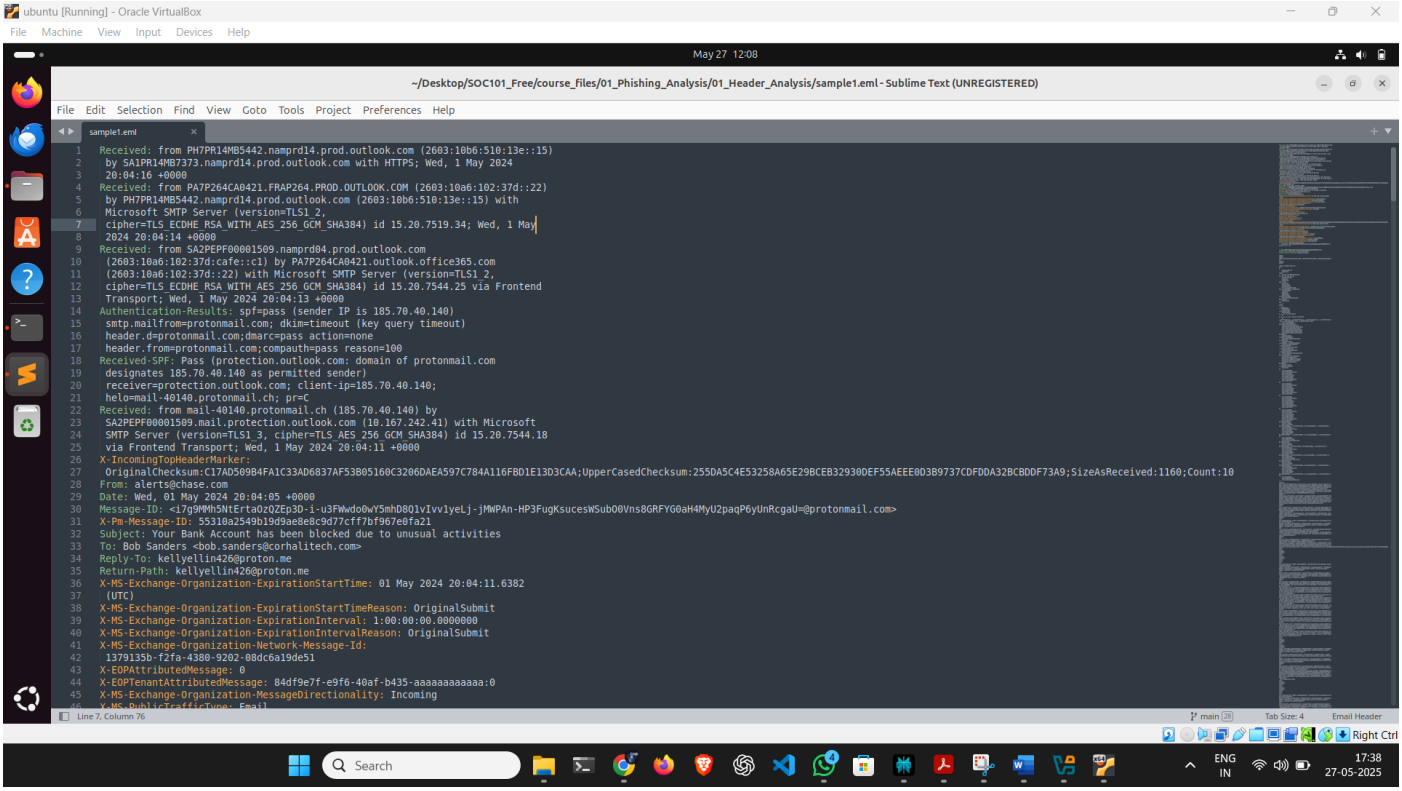


Then, click the **GitMap** option (note that this option might appear differently in some Sublime Text windows), and select **Email Header** from the list.





And you will see that the headers are highlighted, making it easier to identify important information such as the sender, recipient, subject, and other key details within the email. Highlighted headers help you quickly spot any inconsistencies or suspicious elements, which is especially useful when analysing emails for signs of phishing or spoofing.



The following findings from the phishing email were identified through manual analysis:

File Edit View Go Message Tools Help

Get Messages Write Tag

alerts@chase.com
alerts@chase.com

Reply Reply All

To Bob Sanders <bob.sanders@corhalitech.com>

Reply to kellyellin426@proton.me

Your Bank Account has been blocked due to unusual activities

Date Wed, 01 May 2024 20:04:05 +0000

Message ID <i7g9MMh5NtErtaOzQZEp3D-i-u3FWwdo0wY5mhD8Q1vIvv1yeLj-jMWPAn-HP3FugKsucesWSubO0Vns8GRFYG0aH4MyU2paqP6yUnRcgaU=@protonmail.com>

Received from PH7PR14MB5442.namprd14.prod.outlook.com (2603:10b6:510:13e::15) by SA1PR14MB7373.namprd14.prod.outlook.com with HTTPS; Wed, 1 May 2024 20:04:16 +0000

CHASE

Dear Customer,

Due to unusual activities on your account, we placed a tempory suspension until you verify your account.

What You Need To Do In Order To Restore Your Account.

To verify your account, Click on "Reactivate Your Account" below and complete the steps to verify recent account activity.

Reactivate Your Account

Sincerely,

Chase Online Service

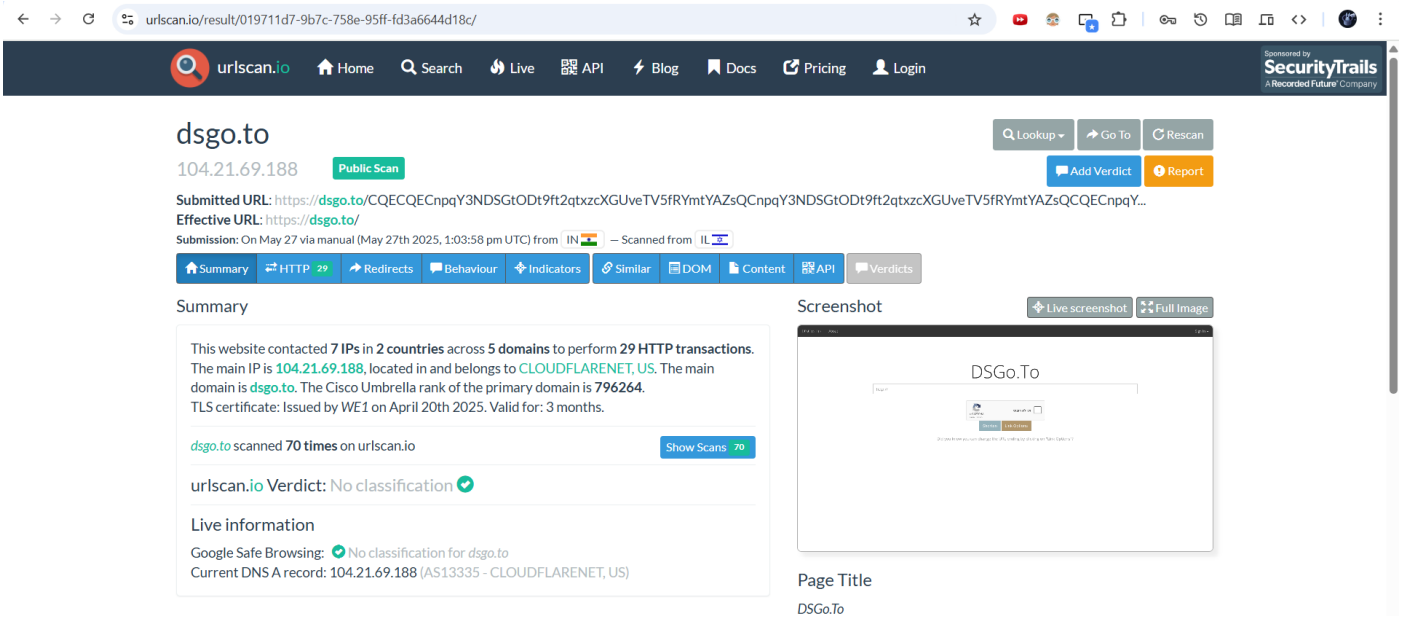
Summary of Phishing traits that are found in the mails are listed below

- The From field contains an address from the Chase Bank domain, but the Message-ID field claims to originate from the ProtonMail server. This means that the email did not come from Chase Bank's servers.
- The use of ProtonMail is often employed to hide the tracks of the sender. The email asks the user to reactivate their bank account, which is a common call-to-action technique used to create a sense of urgency, prompting the user to make a mistake and fall into the attacker's trap.
- A legitimate email should have consistency between the sender’s domain (the part after the @ in the From field) and the domain in the Message-ID header. If the Message-ID shows a different domain—especially one not associated with the organization being impersonated—it is a strong indicator of potential spoofing or phishing.
- Legitimate banks use formal, polite, and carefully worded language in their communications. Unprofessional or blunt language is a common sign of phishing or fraudulent emails.

This is a screenshot of the link that appears when you hover your cursor over the button. To learn more about the URL, you can use tools like Urlscan.io or a URL unshortening service.

- **Urlscan.io** is a security tool that scans URLs and provides detailed reports about the destination website, including screenshots, domain information, and any suspicious activity detected. You can submit the URL to Urlscan.io for a comprehensive analysis.
- **URL unshortening services** reveal the final destination of shortened links without requiring you to click on them. This helps you see where the link actually leads, which is useful for avoiding potentially malicious sites.

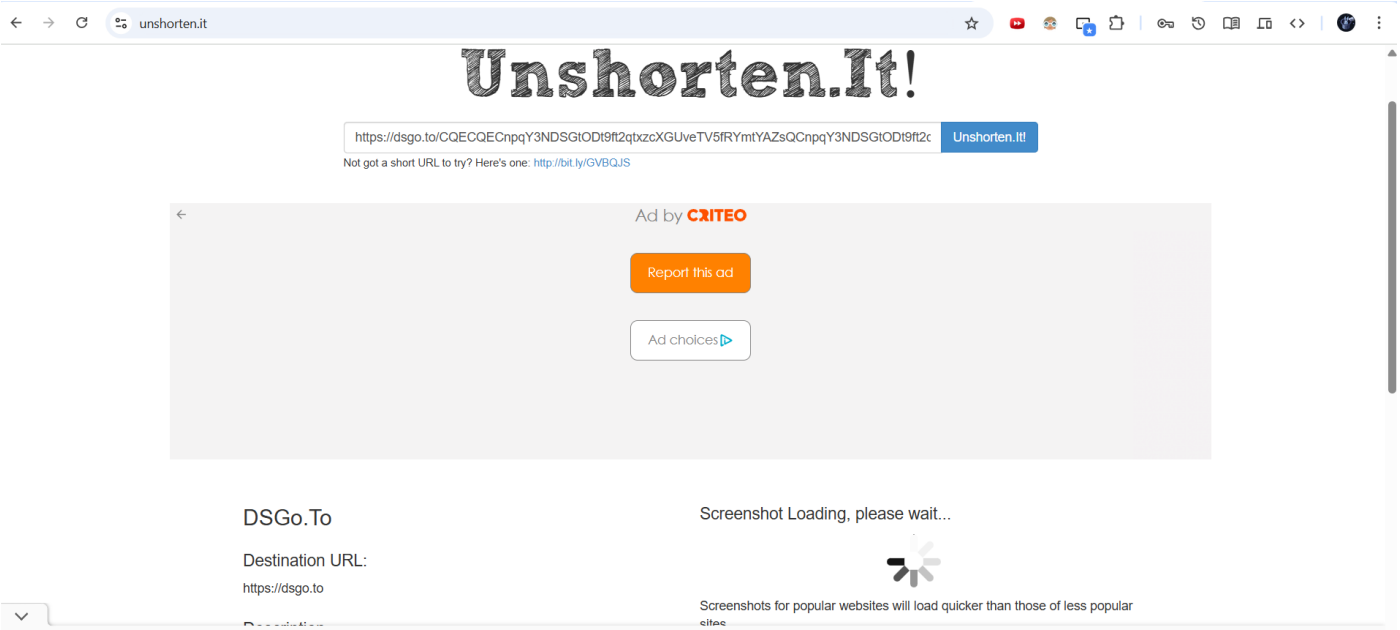
Using these tools allows you to safely investigate suspicious links and understand their destination and any associated risks before interacting with them.



Domain & IP information

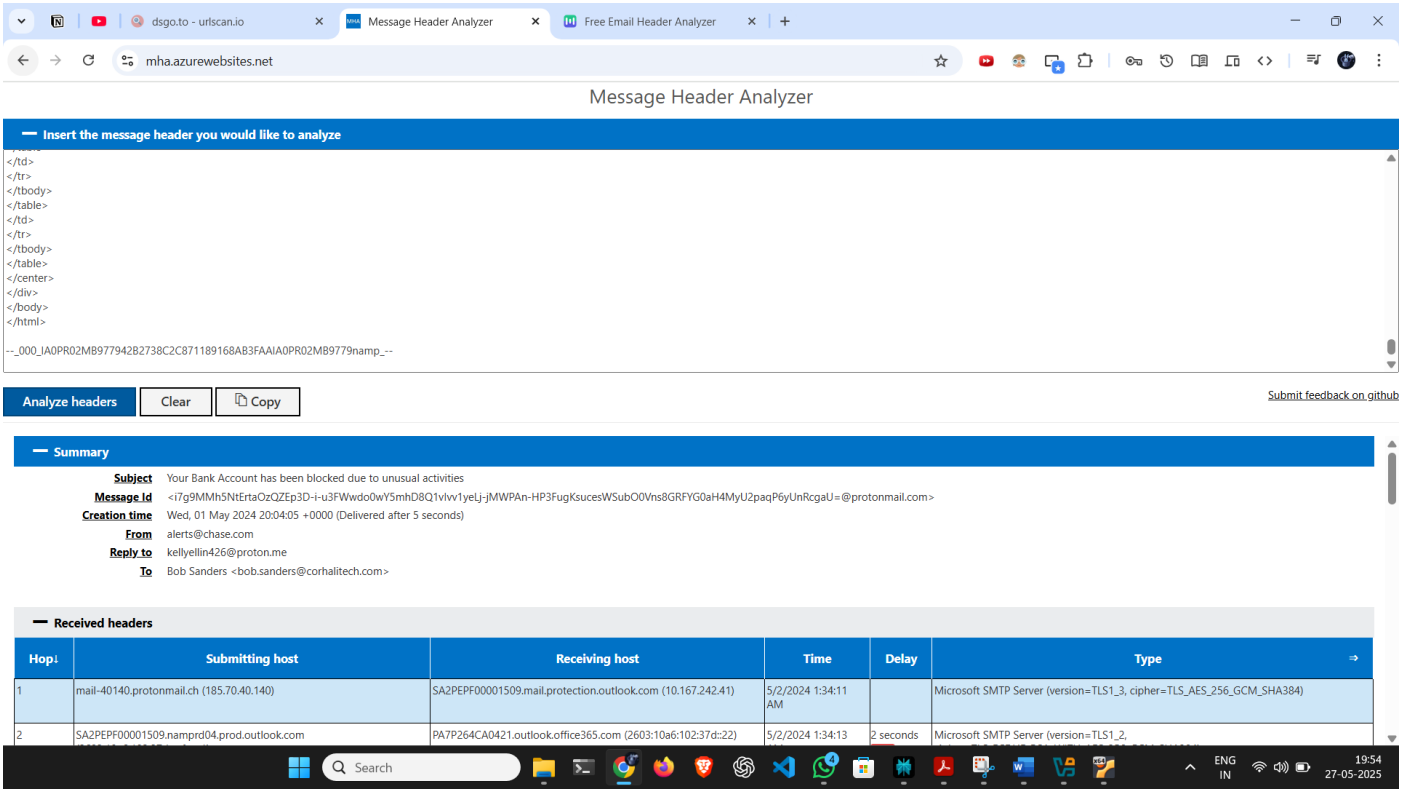
IP/ASNs | IP Detail | Domains | Domain Tree | Links | Certs | Frames

	IP Address	AS Autonomous System
2 → 16	104.21.69.188	13335 (CLOUDFLARENET)
1	104.18.11.207	13335 (CLOUDFLARENET)
3	142.250.186.68	15169 (GOOGLE)
1	172.217.23.106	15169 (GOOGLE)
3	172.217.18.3	15169 (GOOGLE)
6	142.250.185.67	15169 (GOOGLE)
29	7	



Online header analysis

- **Message Header Analyzer**
- **URL - https://mha.azurewebsites.net/**



- **mxtoolbox.com**
- **URL - https://mxtoolbox.com/Public/Tools/EmailHeaders**

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

Header Analyzed

Email Subject: Your Bank Account has been blocked due to unusual activities

Analyze New Header

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

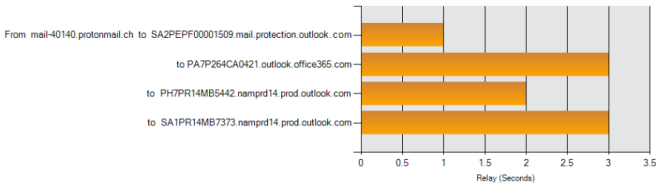
- DMARC Compliant
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

Relay Information

Received Delay:	5 seconds

Relay Information

Received Delay:	5 seconds



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	mail-40140.protonmail.ch 185.70.40.140	SA2PEPF00001509.mail.protection.outlook.com 10.167.242.41	Microsoft SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384)	5/1/2024 8:04:11 PM	✓
2	2 seconds	SA2PEPF00001509.namprd04.prod.outlook.com 2603:10a6:102:37d:cafe::c1	PA7P264CA0421.outlook.office365.com 2603:10a6:102:37d::22	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	5/1/2024 8:04:13 PM	✓
3	1 Second	PA7P264CA0421.FRAP264.PROD.OUTLOOK.COM 2603:10a6:102:37d::22	PH7PR14MB5442.namprd14.prod.outlook.com 2603:10b6:510:13e::15	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	5/1/2024 8:04:14 PM	✓
4	2 seconds	PH7PR14MB5442.namprd14.prod.outlook.com 2603:10b6:510:13e::15	SA1PR14MB7373.namprd14.prod.outlook.com	HTTPS	5/1/2024 8:04:16 PM	✓

SPF and DKIM Information

dmarc:chase.com Show Solve Email Delivery Problems

```
v=DMARC1; p=reject; pct=100; rua=mailto:d@rua.agari.com; ruf=mailto:d@ruf.agari.com;
```

spf:proton.me:185.70.40.140 Show

```
v=spf1 include:_spf.protonmail.ch ~all
```

Dkim Signature Error:
No DKIM-Signature header found - more info

Dkim Signature Error:
There must be at least one aligned DKIM-Signature for the message to be considered aligned. - more info

Headers Found

Header Name	Header Value
Authentication-Results	spf=pass (sender IP is 185.70.40.140) smtp.mailfrom=protonmail.com; dkim=timeout (key query timeout) header.d=protonmail.com;dmarc=pass action=none header.from=protonmail.com;compauth=pass reason=100
Received-SPF	Pass (protection.outlook.com: domain of protonmail.com designates 185.70.40.140 as permitted sender) receiver=protection.outlook.com; client-ip=185.70.40.140; helo=mail-40140.protonmail.ch; pr=C
X-IncomingTopHeaderMarker	OriginalChecksum:C17AD509B4FA1C33AD6837AF53B05160C3206DAEA597C784A116FBD1E13D3CAA;UpperCasedChecksum:255DA5C4E53258A65E29BCEB32930DEF55AEEE0D3B9737CDFDDA32BCBDDF73A9;SizeAsReceived:1160;Count:10
From	alerts@chase.com
Date	Wed, 01 May 2024 20:04:05 +0000
Message-ID	<i7g9MMh5NtErtaOzQZEp3D-i-u3FWwdo0wY5mhD8Q1vIvv1yeLj-jMWPAn-HP3FugKsucesWSubO0Vns8GRFYG0aH4MyU2paqP6yUnRcgaU=@protonmail.com>
X-Pm-Message-ID	55310a2549b19d9ae8e8c9d77cff7bf967e0fa21
Subject	Your Bank Account has been blocked due to unusual activities
To	Bob Sanders <bob.sanders@corhalitech.com>
Reply-To	kellyellin426@proton.me
Return-Path	kellyellin426@proton.me

Received Header

```
Received: from PH7PR14MB5442.namprd14.prod.outlook.com (2603:10b6:510:13e::15)
 by SA1PR14MB7373.namprd14.prod.outlook.com with HTTPS; Wed, 1 May 2024
 20:04:16 +0000
Received: from PA7P264CA0421.FRAP264.PROD.OUTLOOK.COM (2603:10a6:102:37d::22)
 by PH7PR14MB5442.namprd14.prod.outlook.com (2603:10b6:510:13e::15) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7519.34; Wed, 1 May
 2024 20:04:14 +0000
Received: from SA2PEPF00001509.namprd04.prod.outlook.com
 (2603:10a6:102:37d:cafe::c1) by PA7P264CA0421.outlook.office365.com
 (2603:10a6:102:37d::22) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7544.25 via Frontend
 Transport; Wed, 1 May 2024 20:04:13 +0000
Authentication-Results: spf=pass (sender IP is 185.70.40.140)
 smtp.mailfrom=protonmail.com; dkim=timeout (key query timeout)
 header.d=protonmail.com;dmarc=pass action=none
 header.from=protonmail.com;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of protonmail.com
 designates 185.70.40.140 as permitted sender)
 receiver=protection.outlook.com; client-ip=185.70.40.140;
 helo=mail-40140.protonmail.ch; pr=C
Received: from mail-40140.protonmail.ch (185.70.40.140) by
 SA2PEPF00001509.mail.protection.outlook.com (10.167.242.41) with Microsoft
 SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384) id 15.20.7544.18
 via Frontend Transport; Wed, 1 May 2024 20:04:11 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:C17AD509B4FA1C33AD6837AF53B05160C3206DAEA597C784A116FBD1E13D3CAA;UpperCasedChecksum:255DA5C4E53258A65E29BCEB32930DEF55AEEE0D3B9737CDFDDA32BCBDDF73A9;SizeAsReceived:1160;Count:10
From: alerts@chase.com
Date: Wed, 01 May 2024 20:04:05 +0000
Message-ID: <i7g9MMh5NtErtaOzQZEp3D-i-u3FWwdo0wY5mhD8Q1vIvv1yeLj-jMWPAn-HP3FugKsucesWSubO0Vns8GRFYG0aH4MyU2paqP6yUnRcgaU=@protonmail.com>
X-Pm-Message-ID: 55310a2549b19d9ae8e8c9d77cff7bf967e0fa21
Subject: Your Bank Account has been blocked due to unusual activities
```

- **Using Mailmodo**
- **URL - https://www.mailmodo.com/tools/email-header-analyzer/**

mailmodo Platform Resources Pricing Explore Interactive Emails Login Try Mailmodo for free

Summary	
Subject	Your Bank Account has been blocked due to unusual activities
Message Id	<i7g9MMh5NtErtaOzQZEp3D-i-u3FWwdo0wY5mhD8Q1vIvv1yeLj-jMWPAn-HP3FugKsucesWSubO0Vns8GRFYG0aH4MyU2paqP6yUnRcgaU=@protonmail.com>
Creation time	5/2/2024, 1:34:05 AM GMT+5:30
From	<alerts@chase.com>
To	Bob Sanders <bob.sanders@corhalitech.com>
List-Unsubscribe	Unavailable
SPF	PASS
DKIM	PASS
DMARC	PASS
ARC	PASS

Detailed analysis

Common Headers

Header	Value
from	alerts@chase.com
date	Wed, 01 May 2024 20:04:05 +0000
message-id	<i7g9MMh5NtErtaOzQZEp3D-i-u3FWwdo0wY5mhD8Q1vIvv1yeLj-jMWPAn-HP3FugKsucesWSubO0Vns8GRFYG0aH4MyU2paqP6yUnRcgaU=@protonmail.com>
subject	Your Bank Account has been blocked due to unusual activities
to	Bob Sanders <bob.sanders@corhalitech.com>
reply-to	kellyellin426@proton.me
return-path	kellyellin426@proton.me
content-type	multipart/alternative; boundary="_000_IA0PR02MB977942B2738C2C871189168AB3FAAIA0PR02MB9779namp_"
mime-version	1.0

Authentication Headers

Header	Value
authentication-results	spf=pass (sender IP is 185.70.40.140) smtp.mailfrom=protonmail.com; dkim=timeout (key query timeout) header.d=protonmail.com;dmarc=pass action=none header.from=protonmail.com;compauth=pass reason=100
received-spf	Pass (protection.outlook.com: domain of protonmail.com designates 185.70.40.140 as permitted sender) receiver=protection.outlook.com; client-ip=185.70.40.140; helo=mail-40140.protonmail.ch; pr=C

Servers Headers

Header	Value
x-sender-ip	185.70.40.140
x-pm-message-id	55310a2549b19d9ae8e8c9d77cff7bf967e0fa21
x-ms-publictraffictype	Email
x-ms-exchange-transport-endtoendlatency	00:00:05.3190916
x-ms-exchange-transport-crosstenantheadersstamped	PH7PR14MB5442
x-ms-exchange-processed-by-bccfoldering	15.20.7519.031
x-ms-exchange-organization-scl	1
x-ms-exchange-organization-pcl	2
x-ms-exchange-organization-network-message-id	1379135b-f2fa-4380-9202-08dc6a19de51
x-ms-exchange-organization-messagedirectionality	Incoming
x-ms-exchange-organization-expirationstarttimereason	OriginalSubmit
x-ms-exchange-organization-expirationstarttime	01 May 2024 20:04:11.6382 (UTC)
x-ms-exchange-organization-expirationintervalreason	OriginalSubmit
x-ms-exchange-organization-expirationinterval	1:00:00:00.0000000
x-ms-exchange-organization-authsource	SA2PEPF00001509.namprd04.prod.outlook.com
x-ms-exchange-eopdirect	true
x-ms-exchange-crosstenant-rms-persistedconsumerorg	00000000-0000-0000-0000-000000000000
x-ms-exchange-crosstenant-originalarrivaltime	01 May 2024 20:04:11.3100 (UTC)
x-ms-exchange-crosstenant-network-message-id	1379135b-f2fa-4380-9202-08dc6a19de51

x-ms-exchange-crosstenant-id	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa
x-ms-exchange-crosstenant-fromentityheader	Internet
x-ms-exchange-crosstenant-authsource	SA2PEPF00001509.namprd04.prod.outlook.com
x-ms-exchange-crosstenant-authas	Anonymous
x-microsoft-antispam	BCL:0;ARA:1444111002|970799045|2700799017|461199019|58200799006|47200799009|9800799003|440099019|3412199016|1122599004|1380799021|1360799021|1370799021|1290799018;
x-incomingtopheadermarker	OriginalChecksum:C17AD509B4FA1C33AD6837AF53B05160C3206DAEA597C784A116FBD1E13D3CAA;UpperCasedChecksum:255DA5C4E53258A65E29BCEB32930DEF55AEEE0D3B9737CDFDDA32BCBDDF73A9;SizeAsReceived:1160;Count:10
x-eoptenantattributedmessage	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0
x-eopattributedmessage	0
received from	PH7PR14MB5442.namprd14.prod.outlook.com (2603:10b6:510:13e::15) by SA1PR14MB7373.namprd14.prod.outlook.com with HTTPS; Wed, 1 May 2024 20:04:16 +0000
received from	PA7P264CA0421.FRAP264.PROD.OUTLOOK.COM (2603:10a6:102:37d::22) by PH7PR14MB5442.namprd14.prod.outlook.com (2603:10b6:510:13e::15) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7519.34; Wed, 1 May 2024 20:04:14 +0000

received from	SA2PEPF00001509.namprd04.prod.outlook.com (2603:10a6:102:37d:cafe::c1) by PA7P264CA0421.outlook.office365.com (2603:10a6:102:37d::22) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7544.25 via Frontend Transport; Wed, 1 May 2024 20:04:13 +0000
received from	mail-40140.protonmail.ch (185.70.40.140) by SA2PEPF00001509.mail.protection.outlook.com (10.167.242.41) with Microsoft SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384) id 15.20.7544.18 via Frontend Transport; Wed, 1 May 2024 20:04:11 +0000

Key Email Headers of Interest in Phishing Analysis

1. **Message-ID**

   This is a unique identifier generated by the sending SMTP server for each email. It helps track the delivery and origin of messages. While Message-IDs are meant to be unique, sophisticated attackers may attempt to forge them; however, inconsistencies or anomalies in the Message-ID can raise suspicion.

2. **From**

   Indicates the claimed sender of the email. This field is often spoofed in phishing attempts, so it is important to compare it with other headers and note any discrepancies.

3. **To**

   Specifies the intended recipient(s) of the email. Reviewing this field can help determine if the email targets specific individuals or a broader group.

4. **Date**

   Shows when the email was sent. Unusual timestamps or discrepancies with other headers may indicate manipulation.

5. **Subject**

   Summarizes the content or intent of the email. Phishing emails often use urgent or emotionally charged subjects to prompt immediate action from the recipient.

6. **Reply-To**

   Defines the address where replies will be sent. In phishing emails, this address is often different from the "From" address and may point to an attacker-controlled account.

7. **Return-Path**

   Indicates the address to which bounce-back (non-delivery) messages are sent. Differences between the Return-Path and the From address can be a red flag for phishing.

8. **Received**

   Each mail server that processes the email adds a Received header, creating a traceable path from sender to recipient. Examining these headers can reveal the true origin of the message and help detect spoofing.

9. **X-Sender-IP**

   Displays the sender’s IP address, which can be used for further investigation, such as reverse IP lookup, to assess the legitimacy of the sender.