Phishing Email Analysis

Phishing Email “Body” Analysis

1. Unfamiliar Sender or Email Address:
    - The sender's email is listed as `promotions@amzon.com` instead of the legitimate `@amazon.com` domain. The misspelling is subtle, but it's a common tactic used by phishing emails.
2. Urgent or Alarming Language:
    - The language used in the email doesn’t seem overly urgent, but it does encourage the recipient to take advantage of special offers for a limited time from 21st Nov to 2nd Dec up to 40% off.
3. Suspicious Attachments or Links:
    - The email contains several links with a masked URL that points to `https://checka.tech:443/MjAyNDEyMDEyMjIyNTM5OTJlODM2YjI2ZS0zM2YxLTRlOTUtOTEwYS0xZDhmODAxNjc0Yzg=/`, which is not associated with Amazon Prime. This redirection is suspicious and could potentially lead to a phishing page.
4. Generic Greetings:
    - There is no personalized greeting like "Dear [Name]." Instead, the email goes straight into the content, which is a red flag for generic phishing attempts.
5. Spelling and Grammer mistakes:
    - No significant spelling or grammar mistakes were detected in the snippet, but subtle errors may exist in such phishing emails elsewhere in the full message.
6. Request for Personal or Financial Information:
    - There is no direct request for sensitive information in the email body, but the presence of suspicious links could indicate an attempt to collect this data on an external site.
7. Mismatch between Display Name and Email Address:
    - The display name is "Amazon," but the sender's address is @amzon.com. This discrepancy suggests it’s trying to impersonate the official Amazon communications.
8. Inconsistent or suspicious URLs:
    - All the links in the email use the checka.tech domain, which is not associated with Amazon, making the URLs highly suspicious.
9. Unexpected request for payments:
    - There is no direct request for payment in the email body, but the offer for a 40% off might be a lure to click on malicious links, named “See the deals” button, alongwith other underlined, hyperlinked buttons below that button.
10. Too good to be true offers:
    - The email promotes upto 40% off, which may seem appealing but could be unrealistic or misleading if not validated on the official site.
11. Unfamiliar or Odd Attachments:
    - The logo of Amazon Prime is very different from what the email has portrayed, as shown in the website screenshots. Amazon never uses the logo that’s provided in the email.

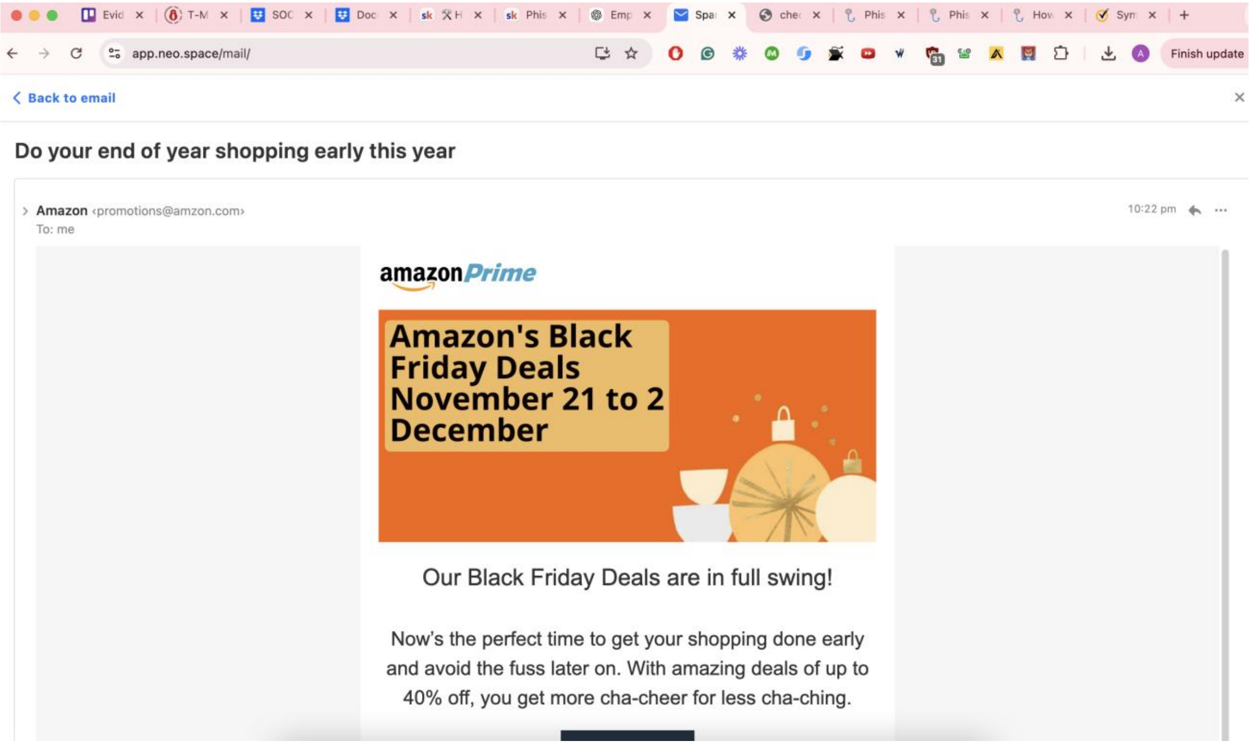
12. Lack of Company Branding:
    - The email does contain some branding elements (the Amazon logo), but it is inaccurate. Phishing emails often use copied branding to create a false sense of legitimacy. In this case, the logo is not legitimate at all.
13. Unusual sender’s Email domain:
    - The sender's domain @amzon.com is not a recognized Deliveroo domain, making it suspicious.
14. No Signature or Contact Information:
    - The snippet provided does not include a proper signature or legitimate contact details, which is a common sign of phishing emails.

Phishing Email “Header” Analysis

1. “From” Address
    - From: "Amazon" <promotions@amzon.com>
    - The domain in the email address "amzon.com" seems suspicious because it is misspelt. The correct domain for Deliveroo should be "amazon.com". This is a common tactic in phishing emails to mimic legitimate brands.
2. “Reply-to Address”
    - "Amazon" <promotions@amzon.com>
    - The "Reply-To" address matches the suspicious "From" address. If clicked, responses would go to the scammer’s email address. This reinforces that the email is likely phishing.
    - Also, to keep in mind, phishing emails often use a different reply address than the "From" address, redirecting replies to the scammer.
3. “Received” Fields
    - The email passed through multiple legitimate Microsoft Outlook servers, but the key IP address in the chain belongs to 52.56.150.127, which is registered to tacklephishing.com which is not the same as amzon.com. This domain appears to be part of a phishing training tool (PhishingTackle), as mentioned in the X-PhishingTackle header.
4. IP Address and Domain Reputation
    - 52.56.150.127: This IP belongs to Amazon Web Services (AWS) in the EU region. You should use a tool like MXToolbox or IPVoid to check if this IP has any history of being associated with malicious activity.
    - tacklephishing.com: This domain is explicitly mentioned as related to phishing training.
5. External Links and Attachments
    - **Actual Link:** https://checka.tech:443/MjAyNDEyMDEyMjIyNTM5OTJlODM2YjI2ZS0zM2YxLTRlOTUtOTEwYS0xZDhmODAxNjc0Yzg=/
    - Link is confirmed to be associated with Phishing Tackle
    - Hover over any links to inspect their true destination. Ensure they match the expected domain (e.g., "amzon.com"). Use tools like VirusTotal or PhishTank to scan URLs for malware or phishing attempts.

- Do not download or open any attachments unless you are certain of their legitimacy. Suspicious attachments should be scanned using antivirus software or online services like VirusTotal to check for malware.

6. DKIM Signature (DomainKeys Identified Mail)
    - DKIM verifies if the email was sent by the legitimate domain. Check if the DKIM signature in the header is valid and aligned with the domain of the email sender.
    - As seen in the screenshot, the email passed DKIM checks with a valid signature from **tacklephishing.com**, confirming that the email has not been altered in transit and was sent by an authorised server for that domain.
7. SPF Record (Sender Policy Framework)
    - Looking for an SPF record result in the header, indicates if the email passed or failed SPF authentication. A pass means the email came from an authorised server for that domain.
    - If it fails, it's a sign the email may be forged.
    - In this case, the email passed SPF checks because tacklephishing.com is listed as an authorised sender for the domain. IP 52.56.150.127 is authorised to send emails on this domain
    - Amzon.com also passed but IP 52.56.150.127 is not authorised to send emails from this domain
8. DMARC Authentication
    - DMARC (Domain-based Message Authentication, Reporting & Conformance) ensures the email's authenticity. I looked for pass or fail results, which indicate whether the message aligns with SPF and DKIM policies.
    - As seen in the DMARC screenshot, the email failed DMARC checks with a reason="(p=reject sp= dis=none)" status. This means there was an issue with alignment or policy enforcement for this email, which is another red flag.
9. Message-ID
    - Every legitimate email has a unique **Message-ID**. I checked for strange patterns in this field, such as missing, repeated, or generic message IDs, which can indicate spoofing.
    - As seen in the screenshot, the unique message ID seems valid and specific, so there's no obvious manipulation here.
10. Subject Encoding and Language
    - I reviewed the subject line for suspicious characters, encoding issues, or misspellings. Malicious actors often use strange encoding or poorly constructed subjects to bypass filters.
    - As seen in the screenshot, Subject: Do your end of year shopping early this year
    - The subject seems generic but not suspicious by itself. There are no encoding issues or strange characters here, but the content could be social engineering.
11. MIME-Version
    - I checked the MIME-Version field to see how the email's format is structured. Irregular MIME types or missing headers may indicate an attempt to manipulate the format for malicious purposes.
    - As seen in the screenshot, the MIME-Version field looks typical for HTML-formatted emails, with no obvious manipulation.



Do your end of year shopping early this year

Amazon ‹promotions@amzon.com›
To: me

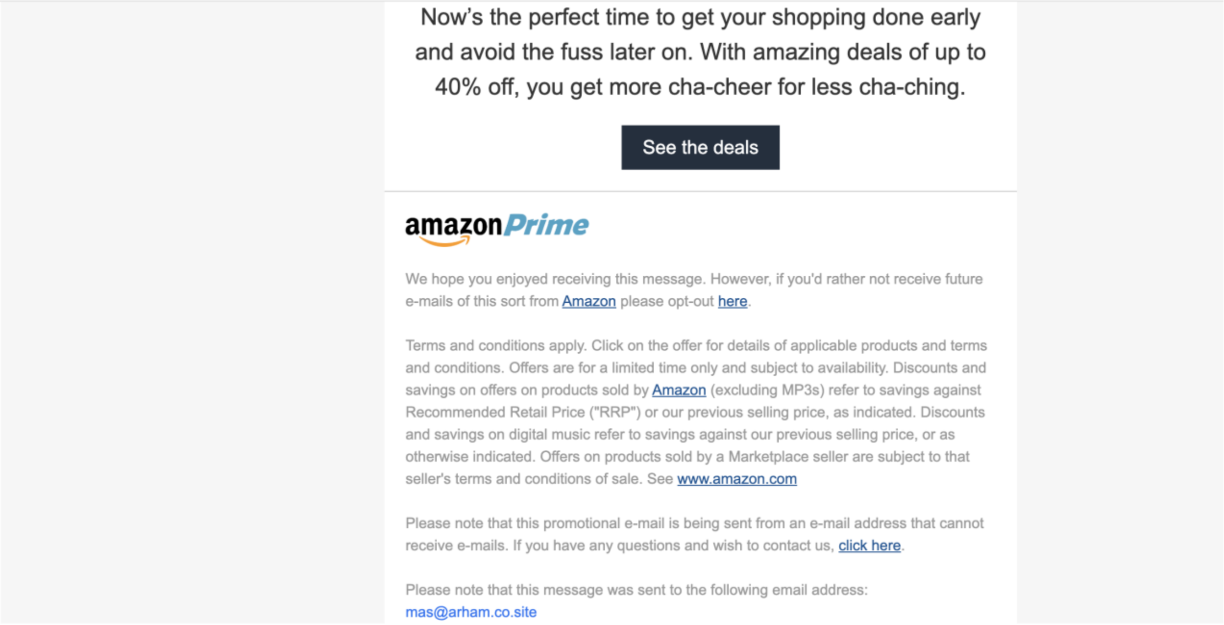
10:22 pm

amazon Prime

Amazon's Black Friday Deals November 21 to 2 December

Our Black Friday Deals are in full swing!

Now's the perfect time to get your shopping done early and avoid the fuss later on. With amazing deals of up to 40% off, you get more cha-cheer for less cha-ching.


Now's the perfect time to get your shopping done early and avoid the fuss later on. With amazing deals of up to 40% off, you get more cha-cheer for less cha-ching.

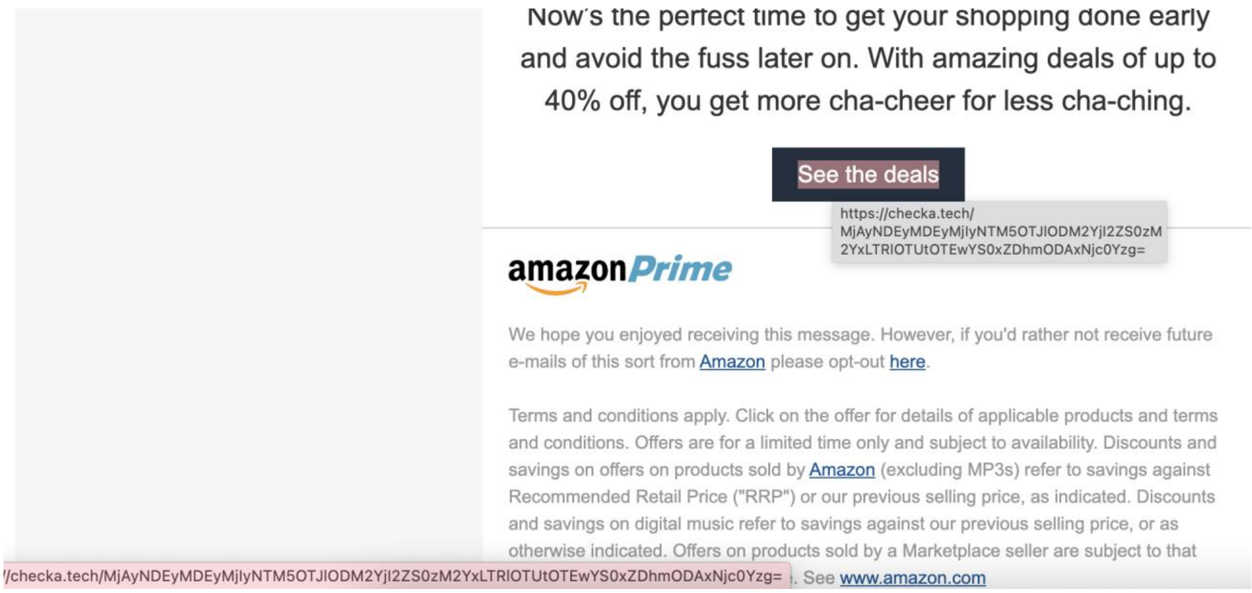
amazon Prime

We hope you enjoyed receiving this message. However, if you'd rather not receive future e-mails of this sort from Amazon please opt-out here.

Terms and conditions apply. Click on the offer for details of applicable products and terms and conditions. Offers are for a limited time only and subject to availability. Discounts and savings on offers on products sold by Amazon (excluding MP3s) refer to savings against Recommended Retail Price ("RRP") or our previous selling price, as indicated. Discounts and savings on digital music refer to savings against our previous selling price, or as otherwise indicated. Offers on products sold by a Marketplace seller are subject to that seller's terms and conditions of sale. See www.amazon.com

Please note that this promotional e-mail is being sent from an e-mail address that cannot receive e-mails. If you have any questions and wish to contact us, click here.

Please note that this message was sent to the following email address: mas@arham.co.site



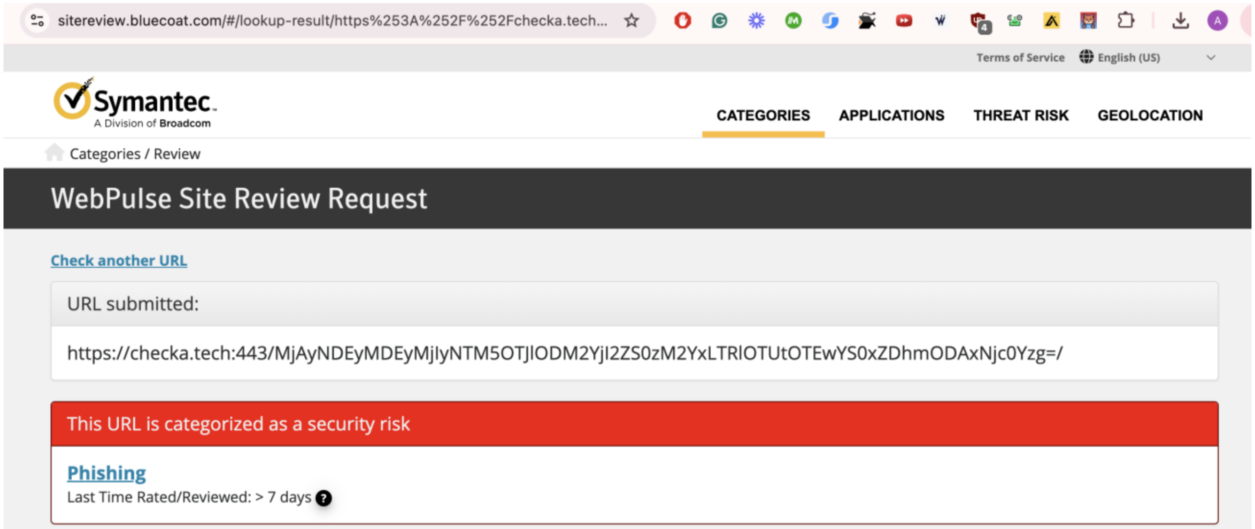
Now's the perfect time to get your shopping done early and avoid the fuss later on. With amazing deals of up to 40% off, you get more cha-cheer for less cha-ching.

https://checka.tech/MjAyNDEyMDEyMjlyNTM5OTJlODM2Yjl2ZS0zM2YxLTRlOTUtOTEwYS0xZDhmODAxNjc0Yzg=

We hope you enjoyed receiving this message. However, if you'd rather not receive future e-mails of this sort from Amazon please opt-out here.

Terms and conditions apply. Click on the offer for details of applicable products and terms and conditions. Offers are for a limited time only and subject to availability. Discounts and savings on offers on products sold by Amazon (excluding MP3s) refer to savings against Recommended Retail Price ("RRP") or our previous selling price, as indicated. Discounts and savings on digital music refer to savings against our previous selling price, or as otherwise indicated. Offers on products sold by a Marketplace seller are subject to that

/checka.tech/MjAyNDEyMDEyMjlyNTM5OTJlODM2Yjl2ZS0zM2YxLTRlOTUtOTEwYS0xZDhmODAxNjc0Yzg= . See www.amazon.com



sitereview.bluecoat.com/#/lookup-result/https%253A%252F%252Fchecka.tech...

WebPulse Site Review Request

Check another URL

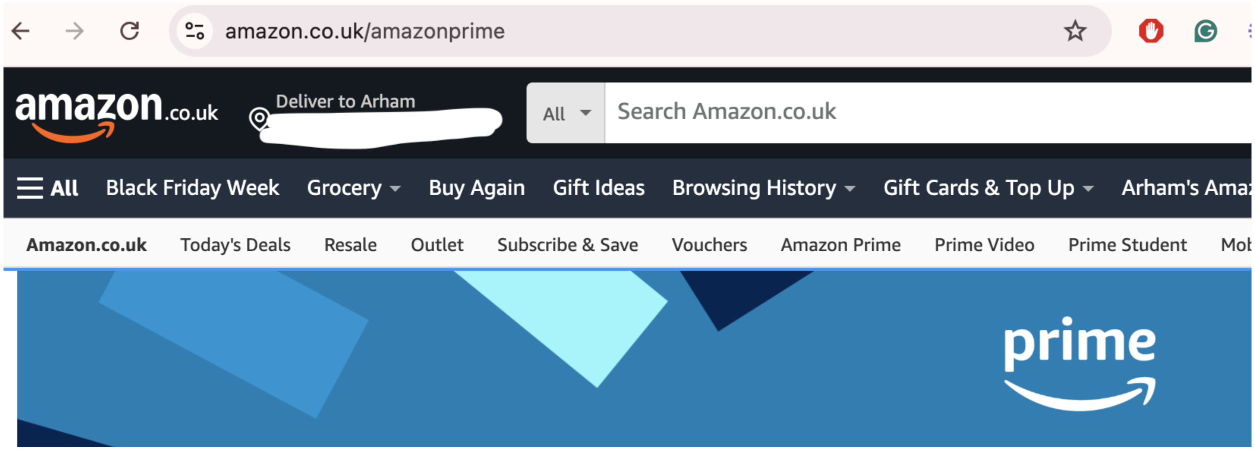
URL submitted:

https://checka.tech:443/MjAyNDEyMDEyMjlyNTM5OTJlODM2Yjl2ZS0zM2YxLTRlOTUtOTEwYS0xZDhmODAxNjc0Yzg=/

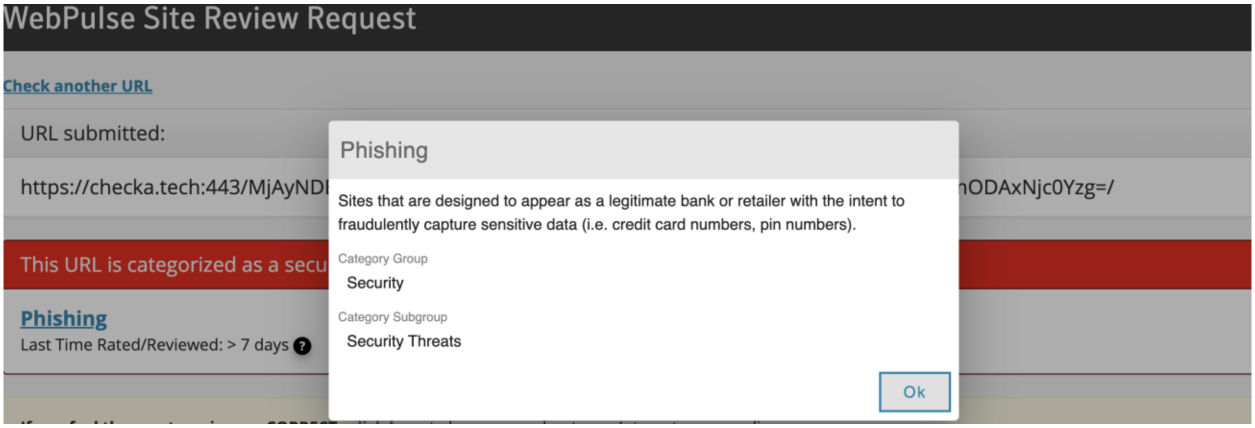
This URL is categorized as a security risk

Phishing

Last Time Rated/Reviewed: > 7 days ?



amazon.co.uk/amazonprime



WebPulse Site Review Request

Check another URL

URL submitted:

https://checka.tech:443/MjAyNDI

nODAxNjc0Yzg=/

This URL is categorized as a secu

Phishing

Last Time Rated/Reviewed: > 7 days ?

Phishing

Sites that are designed to appear as a legitimate bank or retailer with the intent to fraudulently capture sensitive data (i.e. credit card numbers, pin numbers).

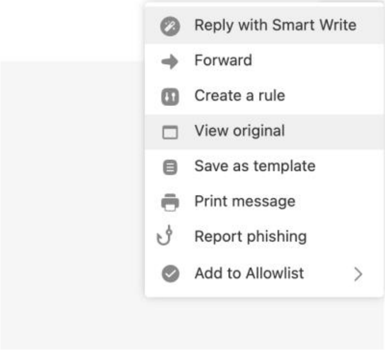
Category Group

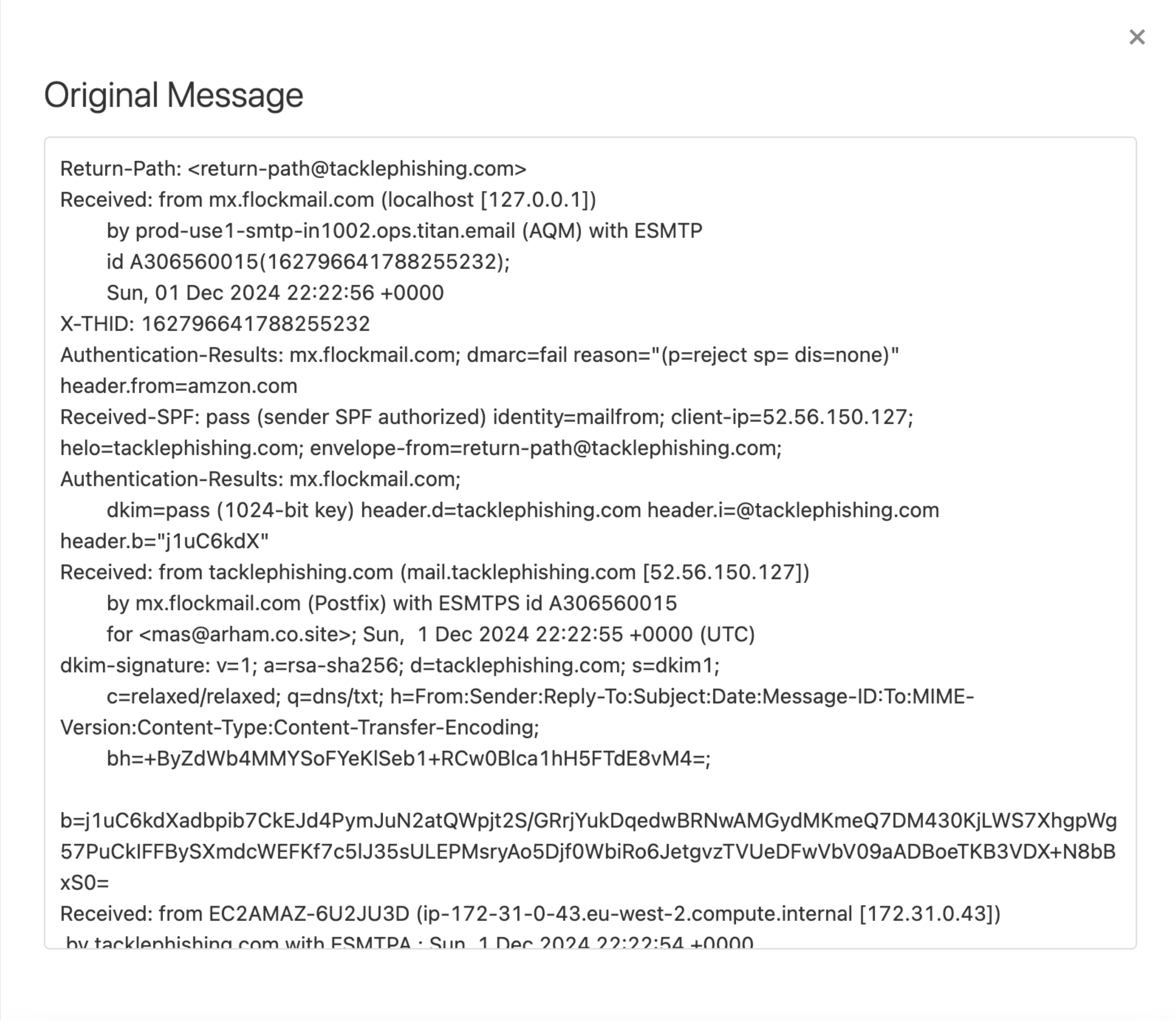
Security

Category Subgroup

Security Threats

Ok

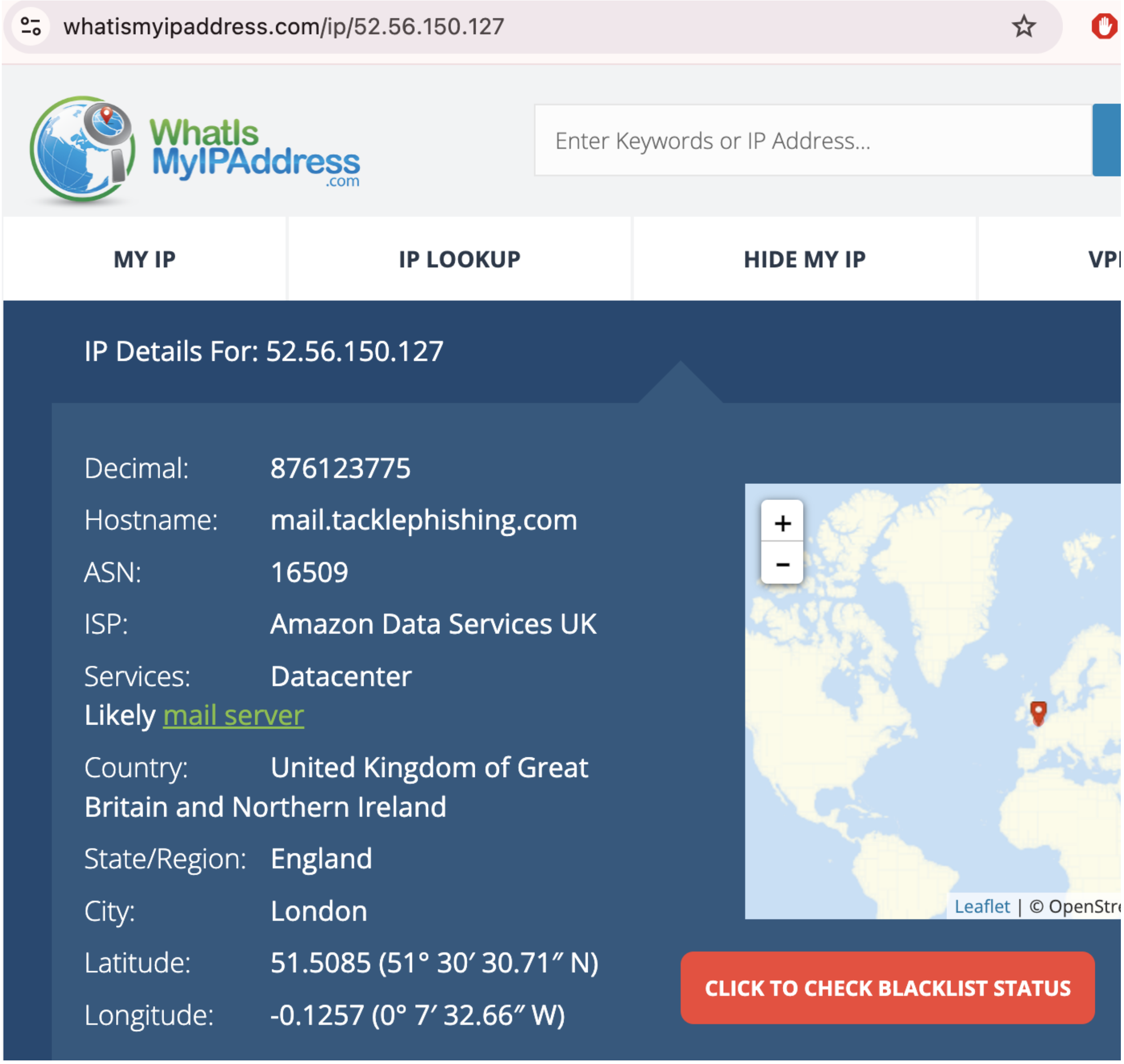




Original Message

```
Return-Path: <return-path@tacklephishing.com>
Received: from mx.flockmail.com (localhost [127.0.0.1])
        by prod-use1-smtp-in1002.ops.titan.email (AQM) with ESMTP
        id A306560015(162796641788255232);
        Sun, 01 Dec 2024 22:22:56 +0000
X-THID: 162796641788255232
Authentication-Results: mx.flockmail.com; dmarc=fail reason="(p=reject sp= dis=none)"
header.from=amzon.com
Received-SPF: pass (sender SPF authorized) identity=mailfrom; client-ip=52.56.150.127;
helo=tacklephishing.com; envelope-from=return-path@tacklephishing.com;
Authentication-Results: mx.flockmail.com;
        dkim=pass (1024-bit key) header.d=tacklephishing.com header.i=@tacklephishing.com
header.b="j1uC6kdX"
Received: from tacklephishing.com (mail.tacklephishing.com [52.56.150.127])
        by mx.flockmail.com (Postfix) with ESMTPS id A306560015
        for <mas@arham.co.site>; Sun,  1 Dec 2024 22:22:55 +0000 (UTC)
dkim-signature: v=1; a=rsa-sha256; d=tacklephishing.com; s=dkim1;
        c=relaxed/relaxed; q=dns/txt; h=From:Sender:Reply-To:Subject:Date:Message-ID:To:MIME-
Version:Content-Type:Content-Transfer-Encoding;
        bh=+ByZdWb4MMYSoFYeKlSeb1+RCw0Blca1hH5FTdE8vM4=;

b=j1uC6kdXadbpib7CkEJd4PymJuN2atQWpjt2S/GRrjYukDqedwBRNwAMGydMKmeQ7DM430KjLWS7XhgpWg
57PuCklFFBySXmdcWEFKf7c5lJ35sULEPMsryAo5Djf0WbiRo6JetgvzTVUeDFwVbV09aADBoeTKB3VDX+N8bB
xS0=
Received: from EC2AMAZ-6U2JU3D (ip-172-31-0-43.eu-west-2.compute.internal [172.31.0.43])
 by tacklephishing.com with ESMTPA ; Sun, 1 Dec 2024 22:22:54 +0000
```

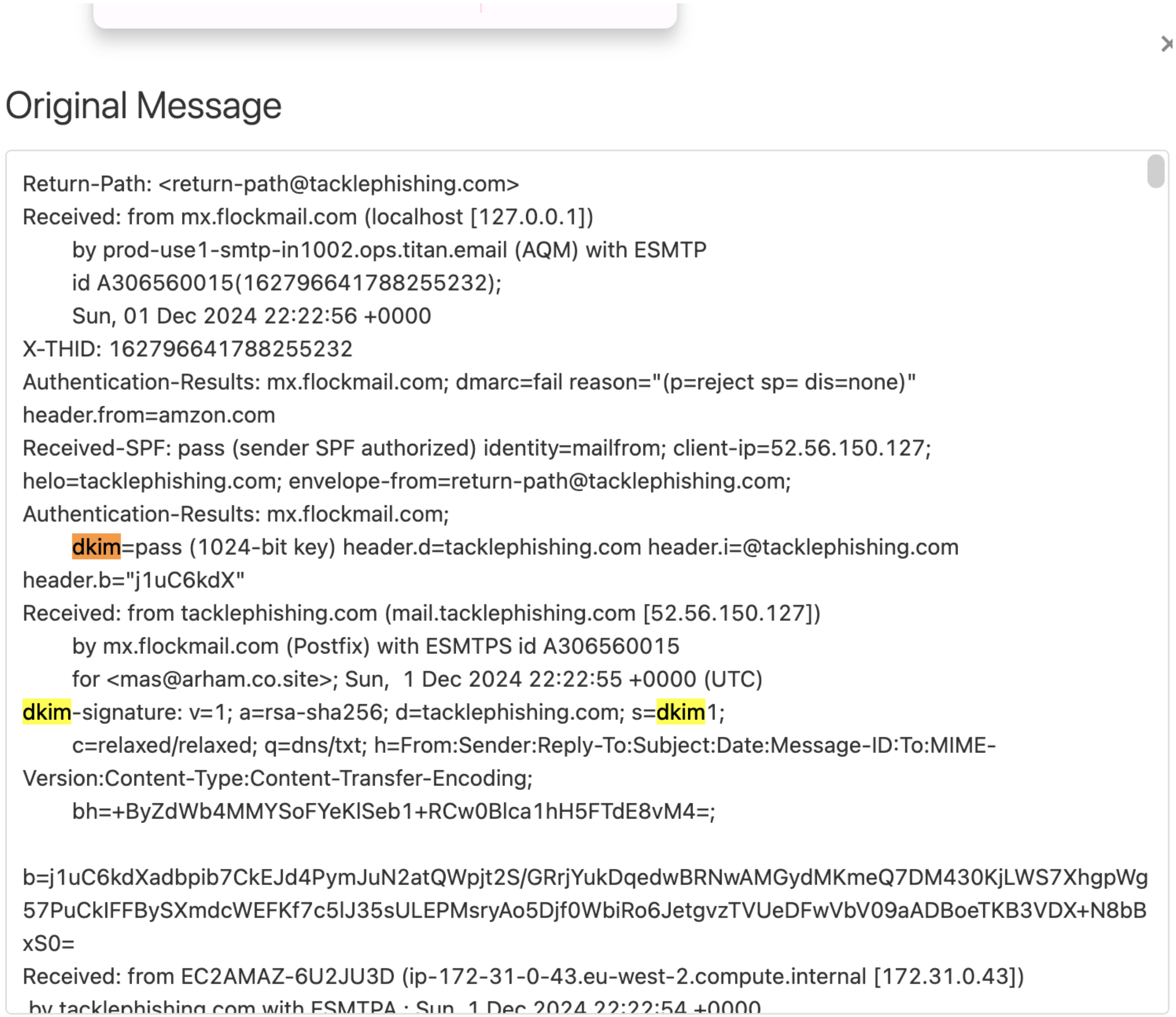

whatismyipaddress.com/ip/52.56.150.127
WhatIs MyIPAddress .com
Enter Keywords or IP Address...
MY IP
IP LOOKUP
HIDE MY IP
VP
+
-
Leaflet | © OpenStr
CLICK TO CHECK BLACKLIST STATUS

IP Details For: 52.56.150.127

Decimal:	876123775
Hostname:	mail.tacklephishing.com
ASN:	16509
ISP:	Amazon Data Services UK
Services:	Datacenter

Likely mail server

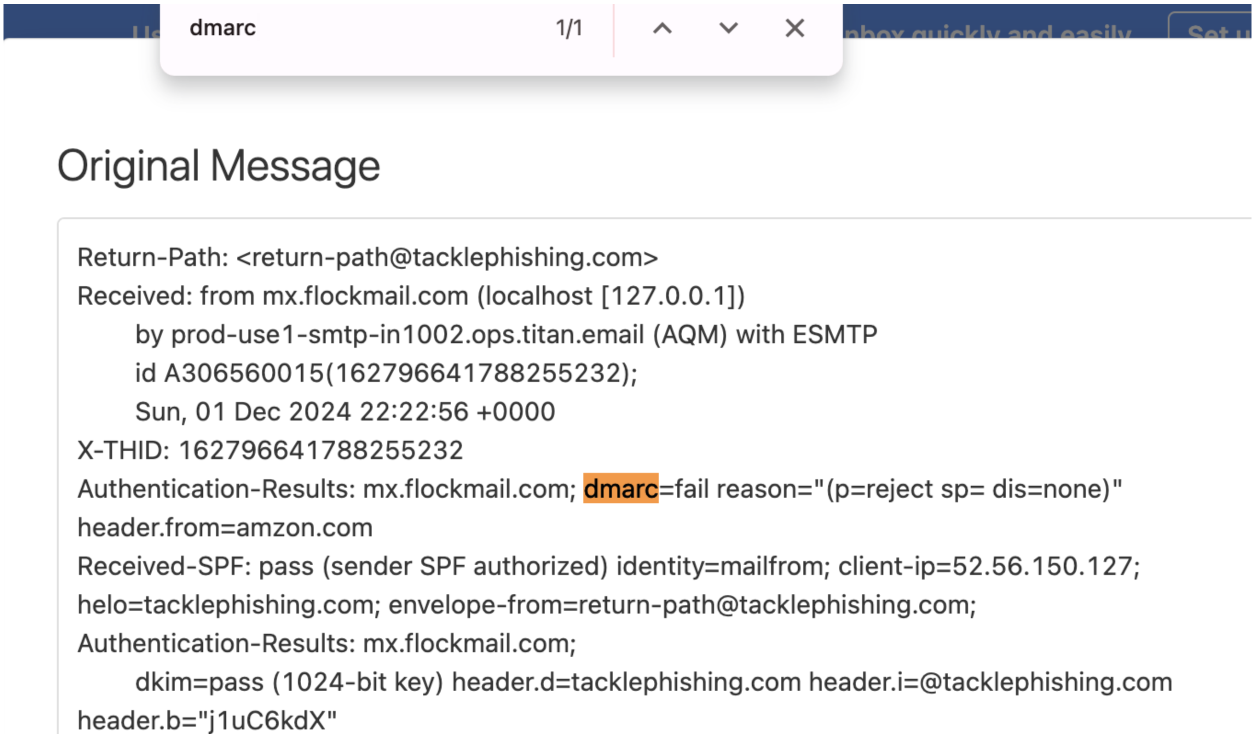
Country:	United Kingdom of Great Britain and Northern Ireland
State/Region:	England
City:	London
Latitude:	51.5085 (51° 30′ 30.71″ N)
Longitude:	-0.1257 (0° 7′ 32.66″ W)



Original Message

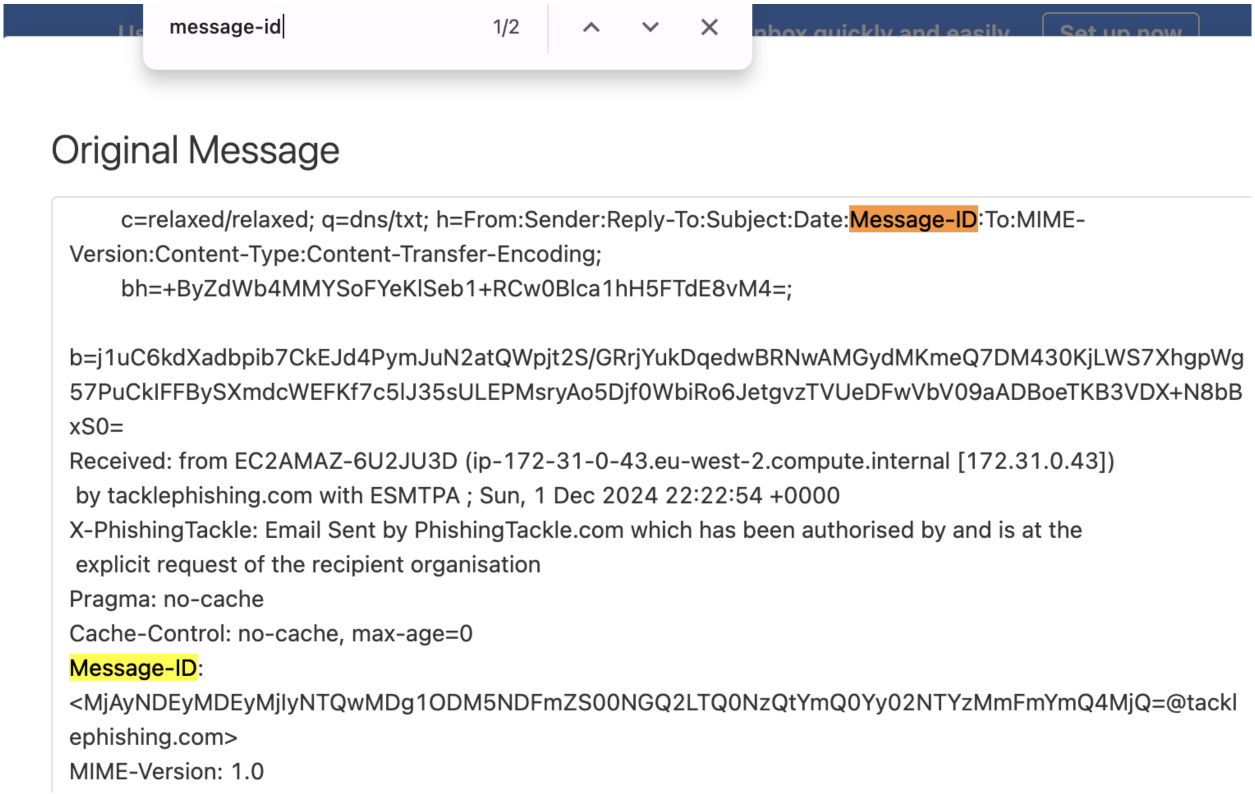
```
Return-Path: <return-path@tacklephishing.com>
Received: from mx.flockmail.com (localhost [127.0.0.1])
        by prod-use1-smtp-in1002.ops.titan.email (AQM) with ESMTP
        id A306560015(1627966417882552З2);
        Sun, 01 Dec 2024 22:22:56 +0000
X-THID: 1627966417882552З2
Authentication-Results: mx.flockmail.com; dmarc=fail reason="(p=reject sp= dis=none)"
header.from=amzon.com
Received-SPF: pass (sender SPF authorized) identity=mailfrom; client-ip=52.56.150.127;
helo=tacklephishing.com; envelope-from=return-path@tacklephishing.com;
Authentication-Results: mx.flockmail.com;
        dkim=pass (1024-bit key) header.d=tacklephishing.com header.i=@tacklephishing.com
header.b="j1uC6kdX"
Received: from tacklephishing.com (mail.tacklephishing.com [52.56.150.127])
        by mx.flockmail.com (Postfix) with ESMTPS id A306560015
        for <mas@arham.co.site>; Sun,  1 Dec 2024 22:22:55 +0000 (UTC)
dkim-signature: v=1; a=rsa-sha256; d=tacklephishing.com; s=dkim1;
        c=relaxed/relaxed; q=dns/txt; h=From:Sender:Reply-To:Subject:Date:Message-ID:To:MIME-
Version:Content-Type:Content-Transfer-Encoding;
        bh=+ByZdWb4MMYSoFYeKlSeb1+RCw0Blca1hH5FTdE8vM4=;

b=j1uC6kdXadbpib7CkEJd4PymJuN2atQWpjt2S/GRrjYukDqedwBRNwAMGydMKmeQ7DM430KjLWS7XhgpWg
57PuCkIFFBySXmdcWEFKf7c5lJ35sULEPMsryAo5Djf0WbiRo6JetgvzTVUeDFwVbV09aADBoeTKB3VDX+N8bB
xS0=
Received: from EC2AMAZ-6U2JU3D (ip-172-31-0-43.eu-west-2.compute.internal [172.31.0.43])
 by tacklephishing.com with ESMTPA ; Sun, 1 Dec 2024 22:22:54 +0000
```



Original Message

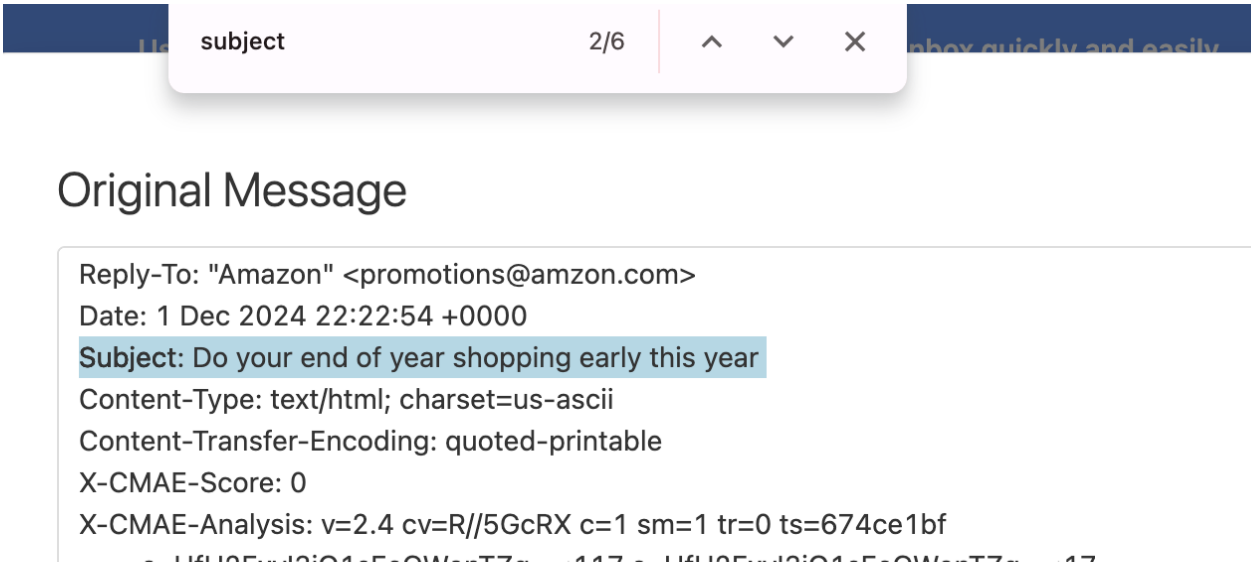
```
Return-Path: <return-path@tacklephishing.com>
Received: from mx.flockmail.com (localhost [127.0.0.1])
	by prod-use1-smtp-in1002.ops.titan.email (AQM) with ESMTP
	id A306560015(162796641788255232);
	Sun, 01 Dec 2024 22:22:56 +0000
X-THID: 162796641788255232
Authentication-Results: mx.flockmail.com; dmarc=fail reason="(p=reject sp= dis=none)"
header.from=amzon.com
Received-SPF: pass (sender SPF authorized) identity=mailfrom; client-ip=52.56.150.127;
helo=tacklephishing.com; envelope-from=return-path@tacklephishing.com;
Authentication-Results: mx.flockmail.com;
	dkim=pass (1024-bit key) header.d=tacklephishing.com header.i=@tacklephishing.com
header.b="j1uC6kdX"
```



Original Message

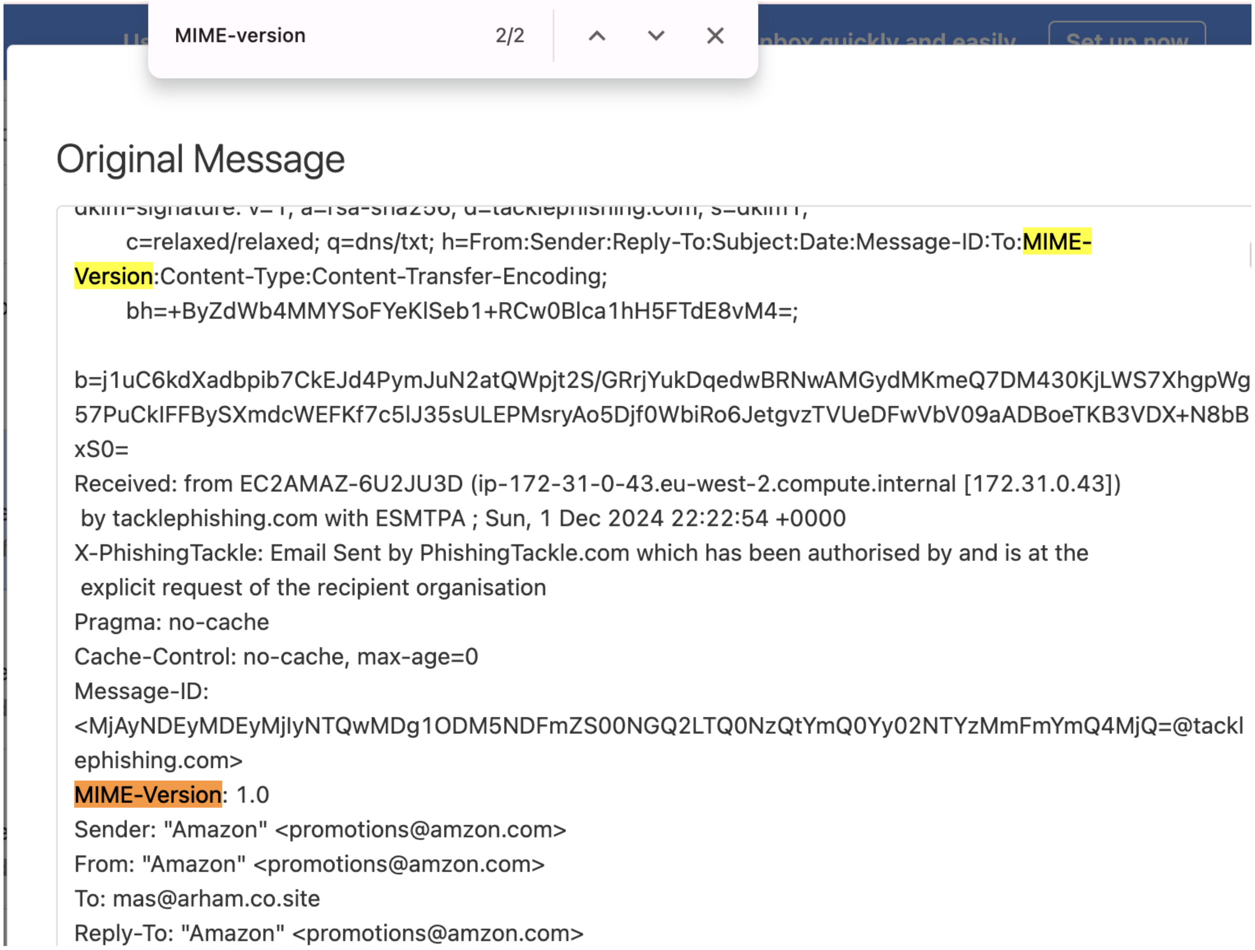
```
	c=relaxed/relaxed; q=dns/txt; h=From:Sender:Reply-To:Subject:Date:Message-ID:To:MIME-
Version:Content-Type:Content-Transfer-Encoding;
	bh=+ByZdWb4MMYSoFYeKlSeb1+RCw0Blca1hH5FTdE8vM4=;

b=j1uC6kdXadbpib7CkEJd4PymJuN2atQWpjt2S/GRrjYukDqedwBRNwAMGydMKmeQ7DM430KjLWS7XhgpWg
57PuCklFFBySXmdcWEFKf7c5lJ35sULEPMsryAo5Djf0WbiRo6JetgvzTVUeDFwVbV09aADBoeTKB3VDX+N8bB
xS0=
Received: from EC2AMAZ-6U2JU3D (ip-172-31-0-43.eu-west-2.compute.internal [172.31.0.43])
 by tacklephishing.com with ESMTPA ; Sun, 1 Dec 2024 22:22:54 +0000
X-PhishingTackle: Email Sent by PhishingTackle.com which has been authorised by and is at the
 explicit request of the recipient organisation
Pragma: no-cache
Cache-Control: no-cache, max-age=0
Message-ID:
<MjAyNDEyMDEyMjIyNTQwMDg1ODM5NDFmZS00NGQ2LTQ0NzQtYmQ0Yy02NTYzMmFmYmQ4MjQ=@tackl
ephishing.com>
MIME-Version: 1.0
```



Original Message

```
Reply-To: "Amazon" <promotions@amzon.com>
Date: 1 Dec 2024 22:22:54 +0000
Subject: Do your end of year shopping early this year
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable
X-CMAE-Score: 0
X-CMAE-Analysis: v=2.4 cv=R//5GcRX c=1 sm=1 tr=0 ts=674ce1bf
```



Original Message

```
dkim-signature: v=1; a=rsa-sha256; d=tacklephishing.com; s=dkim1;
        c=relaxed/relaxed; q=dns/txt; h=From:Sender:Reply-To:Subject:Date:Message-ID:To:MIME-
Version:Content-Type:Content-Transfer-Encoding;
        bh=+ByZdWb4MMYSoFYeKlSeb1+RCw0Blca1hH5FTdE8vM4=;

b=j1uC6kdXadbpib7CkEJd4PymJuN2atQWpjt2S/GRrjYukDqedwBRNwAMGydMKmeQ7DM430KjLWS7XhgpWg
57PuCkIFFBySXmdcWEFKf7c5lJ35sULEPMsryAo5Djf0WbiRo6JetgvzTVUeDFwVbV09aADBoeTKB3VDX+N8bB
xS0=
Received: from EC2AMAZ-6U2JU3D (ip-172-31-0-43.eu-west-2.compute.internal [172.31.0.43])
 by tacklephishing.com with ESMTPA ; Sun, 1 Dec 2024 22:22:54 +0000
X-PhishingTackle: Email Sent by PhishingTackle.com which has been authorised by and is at the
 explicit request of the recipient organisation
Pragma: no-cache
Cache-Control: no-cache, max-age=0
Message-ID:
<MjAyNDEyMDEyMjIyNTQwMDg1ODM5NDFmZS00NGQ2LTQ0NzQtYmQ0Yy02NTYzMmFmYmQ4MjQ=@tackl
ephishing.com>
MIME-Version: 1.0
Sender: "Amazon" <promotions@amzon.com>
From: "Amazon" <promotions@amzon.com>
To: mas@arham.co.site
Reply-To: "Amazon" <promotions@amzon.com>
```