TASK 2: ANALYZE A PHISHING EMAIL SAMPLE.

Objective:

To analyze a suspicious phishing email and identify characteristics that confirm it is a phishing attempt.

Tools Used:

Phish Tank	To verify a suspicious URL.
Domain Tools	WHOIS lookup and gather domain registration details.
MxToolbox	Email header analyzer.
VirusTotal	To scan suspicious URLs and attachments.

Procedure:

Step 1. Obtain a sample phishing

Sample Phishing Email:

Subject: Urgent: Account Suspension Notice

From: support@amaz0n-security.com

Body:

Dear Customer,

We've detected unusual activity in Amazon account. For your security, your account has been temporarily suspended.

Please verify your identity by logging in using the secre link below:

http://amazn-security-check.com/login

Failure to respond within 24 hours will result in permanent suspension.

Thank you,

Amazon Security Team

Attachment: verify_account.zip

Step 2. Examine sender's email address for spoofing.

- “Amazon” is misspelled.
- The word “Body” is not used in an email.

The domain name may look legitimate but it’s a fake website.

Step 3. Check email headers for discrepancies.

- Extract full email headers from your email client.
- Subject should come below the sender’s address.

Look for:

- IP address origin
- SPF/DKIM/DMARC failures
- Return-Path mismatches

Step 4. Identify suspicious links or attachments.

- http://amazn-security-check.com/login
- Attachment: verify_account.zip

Step 5. Look for urgent or threatening language in the email body.

- "Failure to respond within 24 hours will result in permanent suspension."

Step 6. Note any mismatched URLs.

- Do not click links—hover over them to see real URL.
- Scanning with tools like VirusTotal would likely flag it as malicious.

Check for:

- Mismatched or suspicious domains (`login-amaz0n.com`)
- Shortened URLs (e.g., bit.ly)

Step 7. Verify presence of spelling or grammar errors.

- Wrong spelling: “using the secre link below:”
- Grammar error: “activity in Amazon account”

Phishing Report:

Subject: Urgent: Account Suspension Notice

From: support@amaz0n-security.com

Email Header:

```
Return-Path: <support@amaz0n-security.com>

Received: from mail.amazn-security-check.com ([192.0.2.10]) by mx.google.com with ESMTP id x10si12345678qke.123.2025.06.25.11.00.00

        for <victim@example.com>;

        Wed, 25 Jun 2025 11:00:00 -0700 (PDT)

Received-SPF: softfail (google.com: domain of transitioning support@amaz0n-security.com does not designate 192.0.2.10 as permitted sender)

Authentication-Results: mx.google.com;

       spf=softfail (google.com: domain of transitioning support@amaz0n-security.com does not designate 192.0.2.10 as permitted sender) smtp.mailfrom=support@amaz0n-security.com;

       dkim=none;

       dmarc=fail (p=REJECT sp=REJECT dis=NONE) header.from=amaz0n-security.com

Message-ID: <x09876a1234@amaz0n-security.com>

Subject: Urgent: Account Suspension Notice

From: Amazon Security Team <support@amaz0n-security.com>

To: <victim@example.com>

Date: Wed, 25 Jun 2025 11:00:00 -0700

Content-Type: multipart/mixed; boundary="XYZBoundary"

MIME-Version: 1.0
```

Header Analysis:

- Dkim Signature Error:

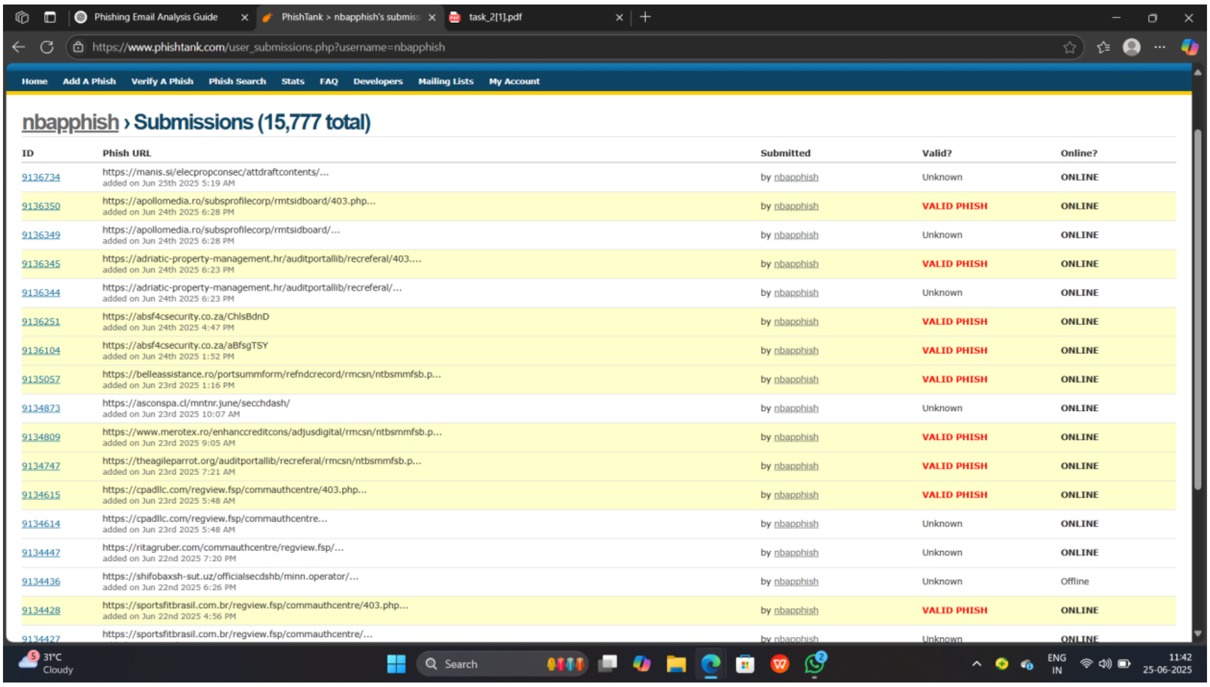
  No DKIM-Signature header found. There must be at least one aligned DKIM-Signature for the message to be considered aligned.

- SPF and DKIM Alignment is incorrect.
- No DMARC Record found.

Suspicious Indicators:

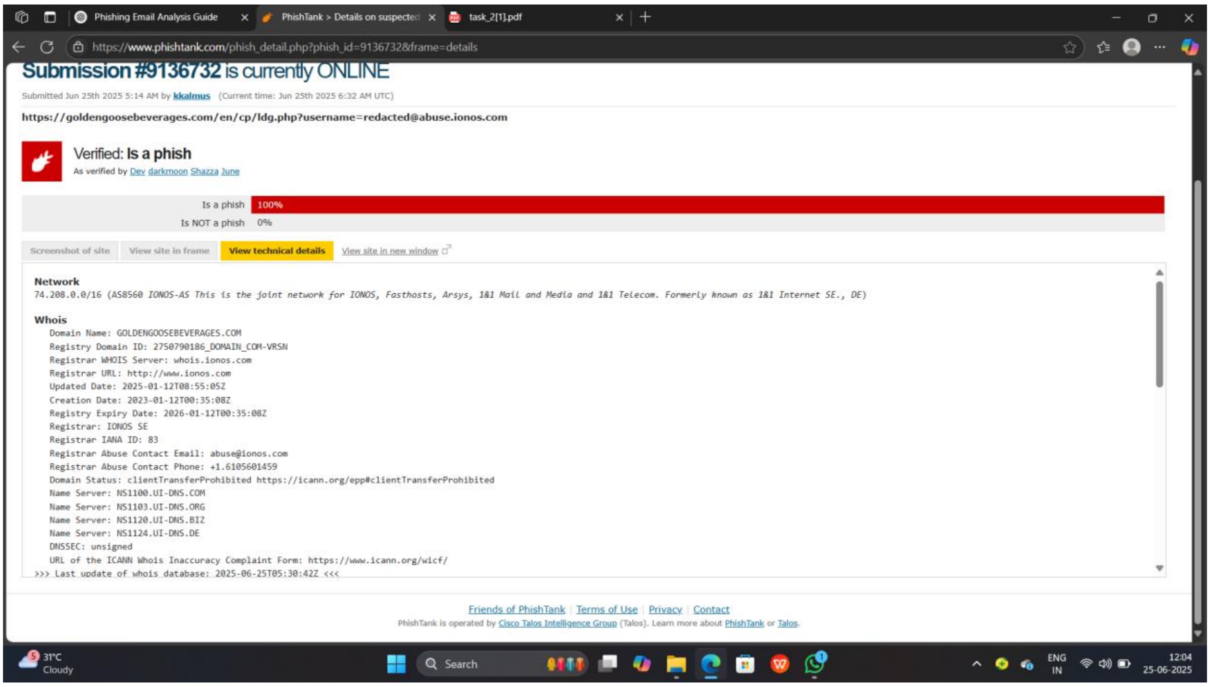
- Sender address: Amazon is misspelled.
- Link in the email: http://amazn-security-check.com/login
- Threatening language: ″Failure to respond within 24 hours will result in permanent suspension.″
- Attachment: verify_account.zip.

Screenshots:



nbapphish › Submissions (15,777 total)

ID	Phish URL	Submitted	Valid?	Online?
9136734	https://manis.si/elecpropconsec/attdraftcontents/... added on Jun 25th 2025 5:19 AM	by nbapphish	Unknown	ONLINE
9136350	https://apollomedia.ro/subsprofilecorp/rmtsidboard/403.php... added on Jun 24th 2025 6:28 PM	by nbapphish	VALID PHISH	ONLINE
9136349	https://apollomedia.ro/subsprofilecorp/rmtsidboard/... added on Jun 24th 2025 6:28 PM	by nbapphish	Unknown	ONLINE
9136345	https://adriatic-property-management.hr/auditportallib/recreferal/403.... added on Jun 24th 2025 6:23 PM	by nbapphish	VALID PHISH	ONLINE
9136344	https://adriatic-property-management.hr/auditportallib/recreferal/... added on Jun 24th 2025 6:23 PM	by nbapphish	Unknown	ONLINE
9136251	https://absf4csecurity.co.za/ChlsBdnD added on Jun 24th 2025 4:47 PM	by nbapphish	VALID PHISH	ONLINE
9136104	https://absf4csecurity.co.za/aBfsgTSY added on Jun 24th 2025 1:52 PM	by nbapphish	VALID PHISH	ONLINE
9135057	https://belleassistance.ro/portsummform/refndcrecord/rmcsn/ntbsmmfsb.p... added on Jun 23rd 2025 1:16 PM	by nbapphish	VALID PHISH	ONLINE
9134873	https://asconspa.cl/mntnr.june/secchdash/ added on Jun 23rd 2025 10:07 AM	by nbapphish	Unknown	ONLINE
9134809	https://www.merotex.ro/enhanccreditcons/adjusdigital/rmcsn/ntbsmmfsb.p... added on Jun 23rd 2025 9:05 AM	by nbapphish	VALID PHISH	ONLINE
9134747	https://theagileparrot.org/auditportallib/recreferal/rmcsn/ntbsmmfsb.p... added on Jun 23rd 2025 7:21 AM	by nbapphish	VALID PHISH	ONLINE
9134615	https://cpadllc.com/regview.fsp/commauthcentre/403.php... added on Jun 23rd 2025 5:48 AM	by nbapphish	VALID PHISH	ONLINE
9134614	https://cpadllc.com/regview.fsp/commauthcentre... added on Jun 23rd 2025 5:48 AM	by nbapphish	Unknown	ONLINE
9134447	https://ritagruber.com/commauthcentre/regview.fsp/... added on Jun 22nd 2025 7:20 PM	by nbapphish	Unknown	ONLINE
9134436	https://shifobaxsh-sut.uz/officialsecdshb/minn.operator/... added on Jun 22nd 2025 6:26 PM	by nbapphish	Unknown	Offline
9134428	https://sportsfitbrasil.com.br/regview.fsp/commauthcentre/403.php... added on Jun 22nd 2025 4:56 PM	by nbapphish	VALID PHISH	ONLINE
9134427	https://sportsfitbrasil.com.br/regview.fsp/commauthcentre/...	by nbapphish	Unknown	ONLINE



Phishing Email Analysis Guide
PhishTank > Details on suspected
task_2[1].pdf
https://www.phishtank.com/phish_detail.php?phish_id=9136732&frame=details
Screenshot of site
View site in frame
View technical details
View site in new window
31°C
Cloudy
Search
ENG
IN
12:04
25-06-2025

Submission #9136732 is currently ONLINE

Submitted Jun 25th 2025 5:14 AM by kkalmus (Current time: Jun 25th 2025 6:32 AM UTC)

https://goldengoosebeverages.com/en/cp/ldg.php?username=redacted@abuse.ionos.com

Verified: **Is a phish**

As verified by Dev darkmoon Shazza June

Is a phish	100%
Is NOT a phish	0%

Network

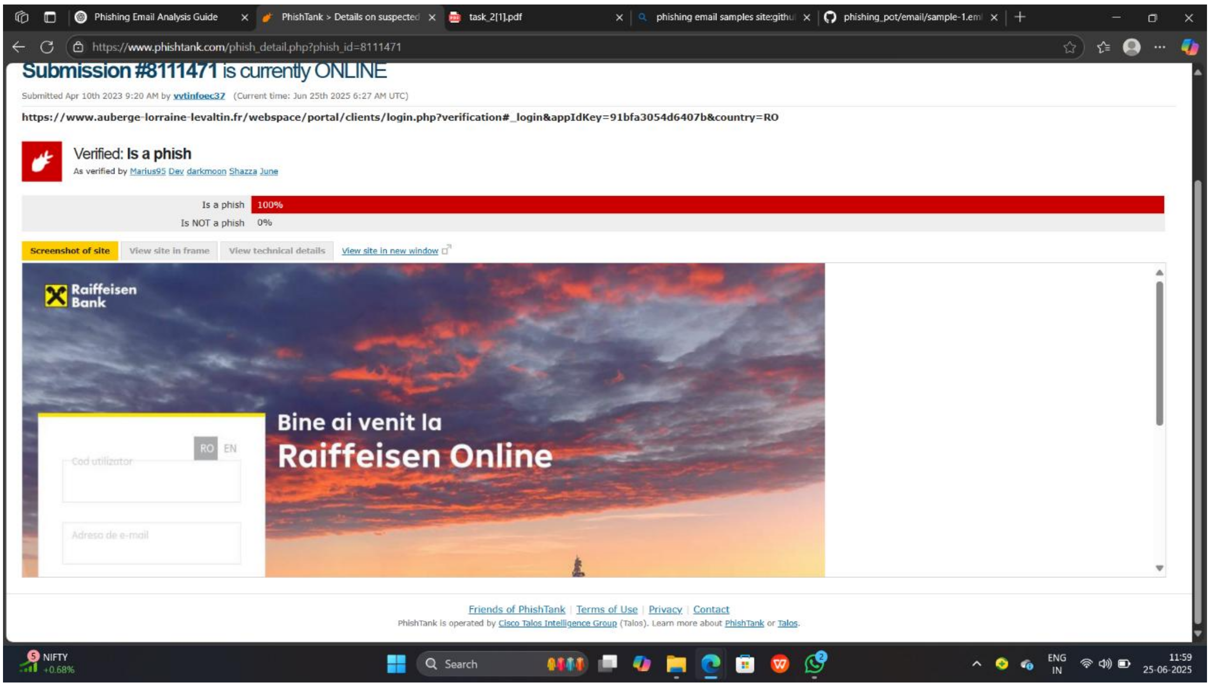
```
74.208.0.0/16 (AS8560 IONOS-AS This is the joint network for IONOS, Fasthosts, Arsys, 1&1 Mail and Media and 1&1 Telecom. Formerly known as 1&1 Internet SE., DE)
```

Whois

```
   Domain Name: GOLDENGOOSEBEVERAGES.COM
   Registry Domain ID: 2750790186_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.ionos.com
   Registrar URL: http://www.ionos.com
   Updated Date: 2025-01-12T08:55:05Z
   Creation Date: 2023-01-12T00:35:08Z
   Registry Expiry Date: 2026-01-12T00:35:08Z
   Registrar: IONOS SE
   Registrar IANA ID: 83
   Registrar Abuse Contact Email: abuse@ionos.com
   Registrar Abuse Contact Phone: +1.6105601459
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1100.UI-DNS.COM
   Name Server: NS1103.UI-DNS.ORG
   Name Server: NS1120.UI-DNS.BIZ
   Name Server: NS1124.UI-DNS.DE
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-06-25T05:30:42Z <<<
```

Friends of PhishTank | Terms of Use | Privacy | Contact

PhishTank is operated by Cisco Talos Intelligence Group (Talos). Learn more about PhishTank or Talos.


Phishing Email Analysis Guide
PhishTank > Details on suspected
task_2[1].pdf
phishing email samples site:githu
phishing_pot/email/sample-1.eml
https://www.phishtank.com/phish_detail.php?phish_id=8111471

Submission #8111471 is currently ONLINE

Submitted Apr 10th 2023 9:20 AM by vvtinfoec37 (Current time: Jun 25th 2025 6:27 AM UTC)

https://www.auberge-lorraine-levaltin.fr/webspace/portal/clients/login.php?verification#_login&appIdKey=91bfa3054d6407b&country=RO

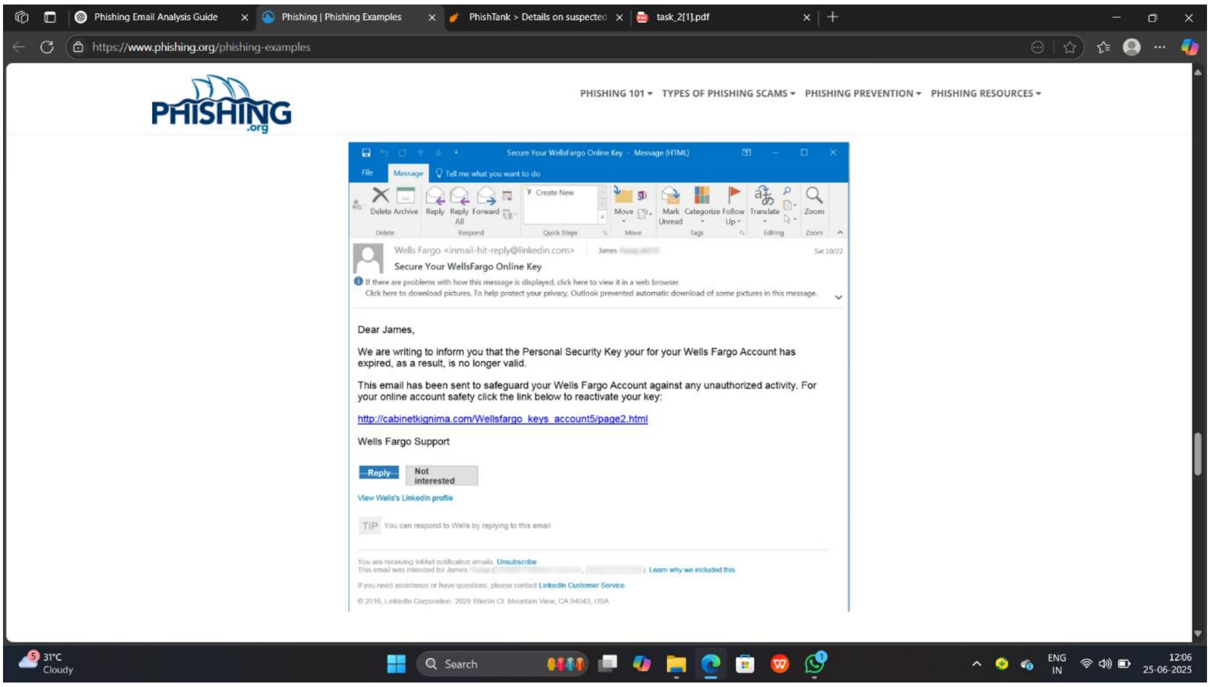
Verified: **Is a phish**

As verified by Marius95 Dev darkmoon Shazza June

Is a phish	100%
Is NOT a phish	0%

Screenshot of site
View site in frame
View technical details
View site in new window
Raiffeisen Bank
RO EN
Cod utilizator
Adresa de e-mail
Bine ai venit la
Raiffeisen Online
Friends of PhishTank | Terms of Use | Privacy | Contact

PhishTank is operated by Cisco Talos Intelligence Group (Talos). Learn more about PhishTank or Talos.


Phishing Email Analysis Guide
Phishing | Phishing Examples
PhishTank > Details on suspected
task_2[1].pdf
https://www.phishing.org/phishing-examples
PHISHING .org
PHISHING 101 ▾
TYPES OF PHISHING SCAMS ▾
PHISHING PREVENTION ▾
PHISHING RESOURCES ▾
Secure Your WellsFargo Online Key - Message (HTML)
File
Message
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
Create New
Move
Mark Unread
Categorize
Follow Up
Translate
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom

Wells Fargo <inmail-hit-reply@linkedin.com> James [redacted] Sat 10/22

Secure Your WellsFargo Online Key

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear James,

We are writing to inform you that the Personal Security Key your for your Wells Fargo Account has expired, as a result, is no longer valid.

This email has been sent to safeguard your Wells Fargo Account against any unauthorized activity. For your online account safety click the link below to reactivate your key:

http://cabinetkignima.com/Wellsfargo_keys_account5/page2.html

Wells Fargo Support

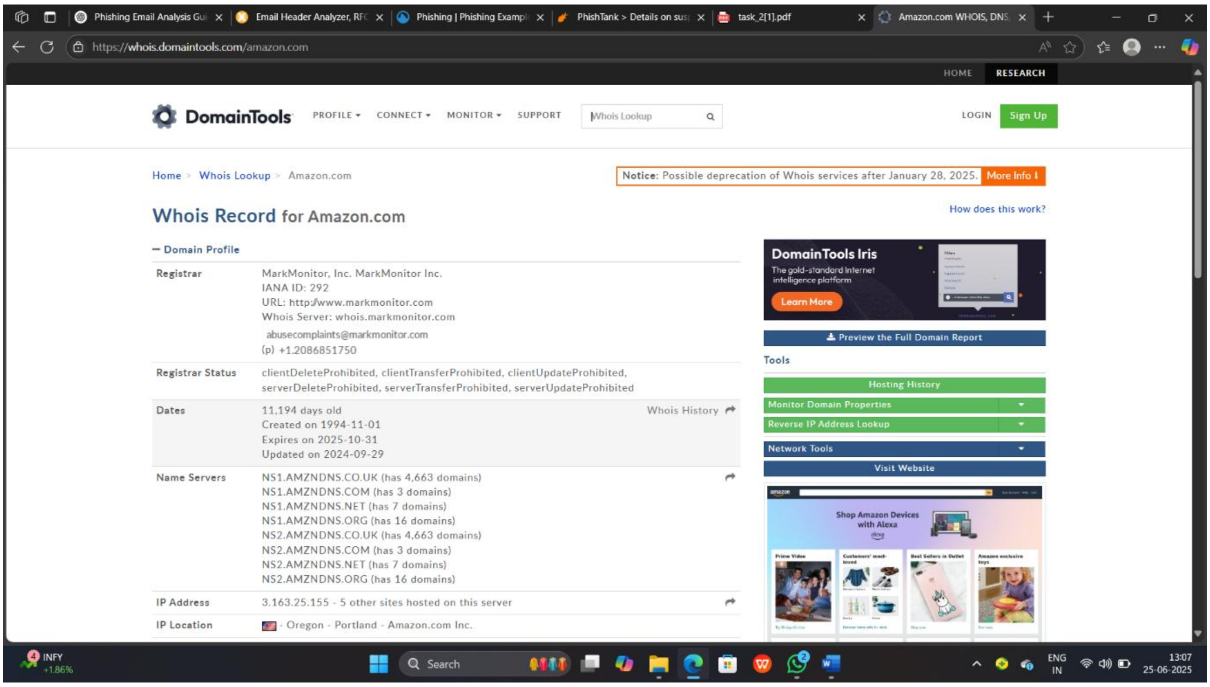
View Wells's LinkedIn profile

TIP You can respond to Wells by replying to this email

You are receiving InMail notification emails. Unsubscribe
This email was intended for James [redacted] ([redacted], [redacted]). Learn why we included this.

If you need assistance or have questions, please contact LinkedIn Customer Service

© 2016, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA


Phishing Email Analysis Gui
Email Header Analyzer, RFC
Phishing | Phishing Exampl
PhishTank > Details on sus
task_2[1].pdf
Amazon.com WHOIS, DNS
https://whois.domaintools.com/amazon.com
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
DomainTools Iris
The gold-standard Internet intelligence platform
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Visit Website
Shop Amazon Devices with Alexa
INFY
+1.86%
Search
ENG
IN
13:07
25-06-2025

Home > Whois Lookup > Amazon.com

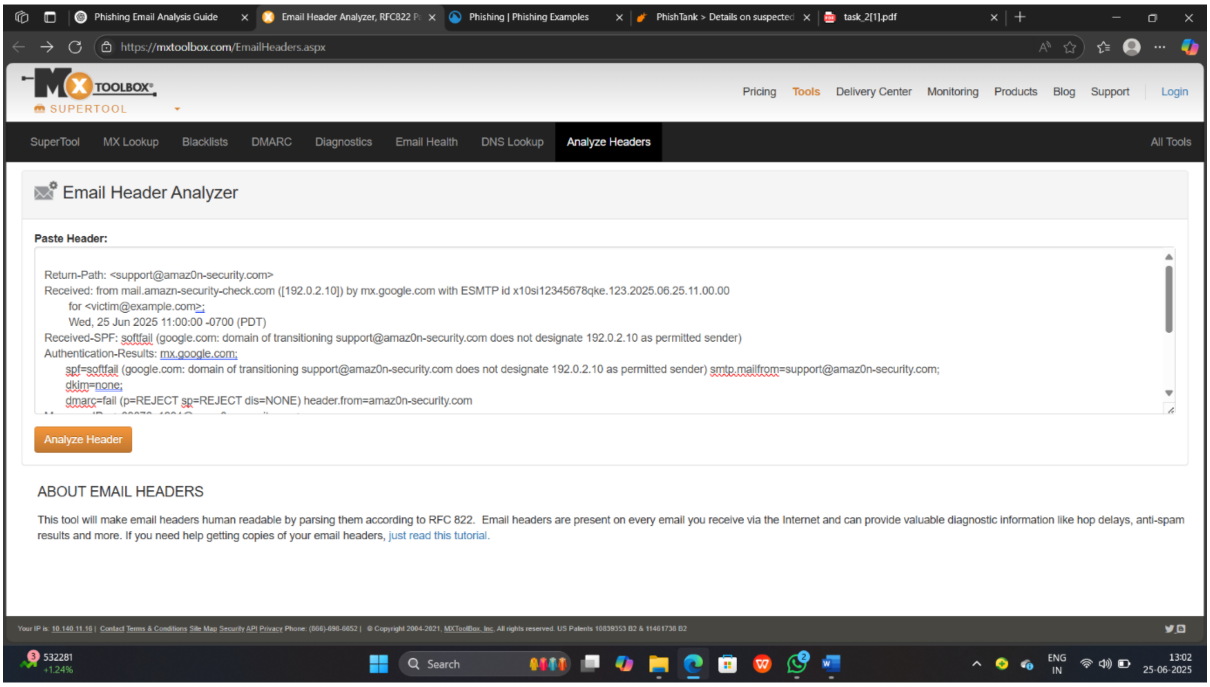
Notice: Possible deprecation of Whois services after January 28, 2025. More Info

How does this work?

Whois Record for Amazon.com

– Domain Profile

Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) +1.2086851750
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	11,194 days old Created on 1994-11-01 Expires on 2025-10-31 Updated on 2024-09-29 Whois History
Name Servers	NS1.AMZNDNS.CO.UK (has 4,663 domains) NS1.AMZNDNS.COM (has 3 domains) NS1.AMZNDNS.NET (has 7 domains) NS1.AMZNDNS.ORG (has 16 domains) NS2.AMZNDNS.CO.UK (has 4,663 domains) NS2.AMZNDNS.COM (has 3 domains) NS2.AMZNDNS.NET (has 7 domains) NS2.AMZNDNS.ORG (has 16 domains)
IP Address	3.163.25.155 - 5 other sites hosted on this server
IP Location	- Oregon - Portland - Amazon.com Inc.



Email Header Analyzer

Paste Header:

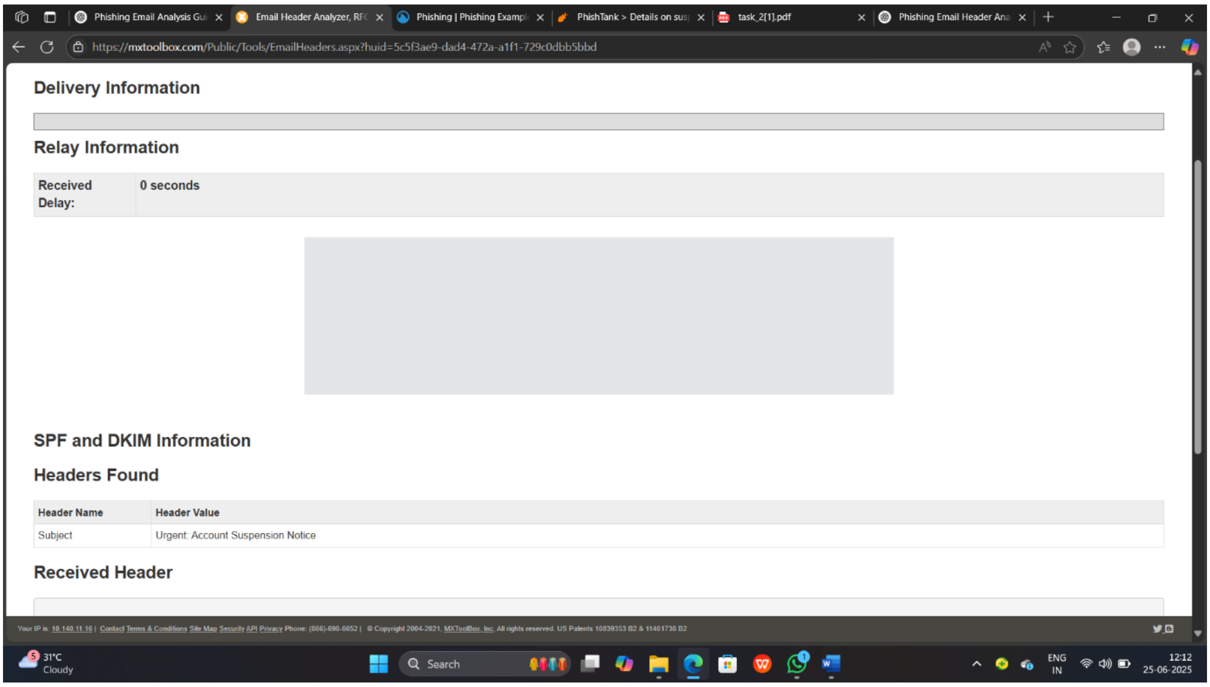
```
Return-Path: <support@amaz0n-security.com>
Received: from mail.amazn-security-check.com ([192.0.2.10]) by mx.google.com with ESMTP id x10si12345678qke.123.2025.06.25.11.00.00
        for <victim@example.com>;
        Wed, 25 Jun 2025 11:00:00 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning support@amaz0n-security.com does not designate 192.0.2.10 as permitted sender)
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning support@amaz0n-security.com does not designate 192.0.2.10 as permitted sender) smtp.mailfrom=support@amaz0n-security.com;
       dkim=none;
       dmarc=fail (p=REJECT sp=REJECT dis=NONE) header.from=amaz0n-security.com
```

Analyze Header

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.

Your IP is: 10.140.11.16 | 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


Phishing Email Analysis Gui
Email Header Analyzer, RFC
Phishing | Phishing Example
PhishTank > Details on susp
task_2[1].pdf
Phishing Email Header Ana
https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=5c5f3ae9-dad4-472a-a1f1-729c0dbb5bbd

Delivery Information

Relay Information

Received Delay:	**0 seconds**

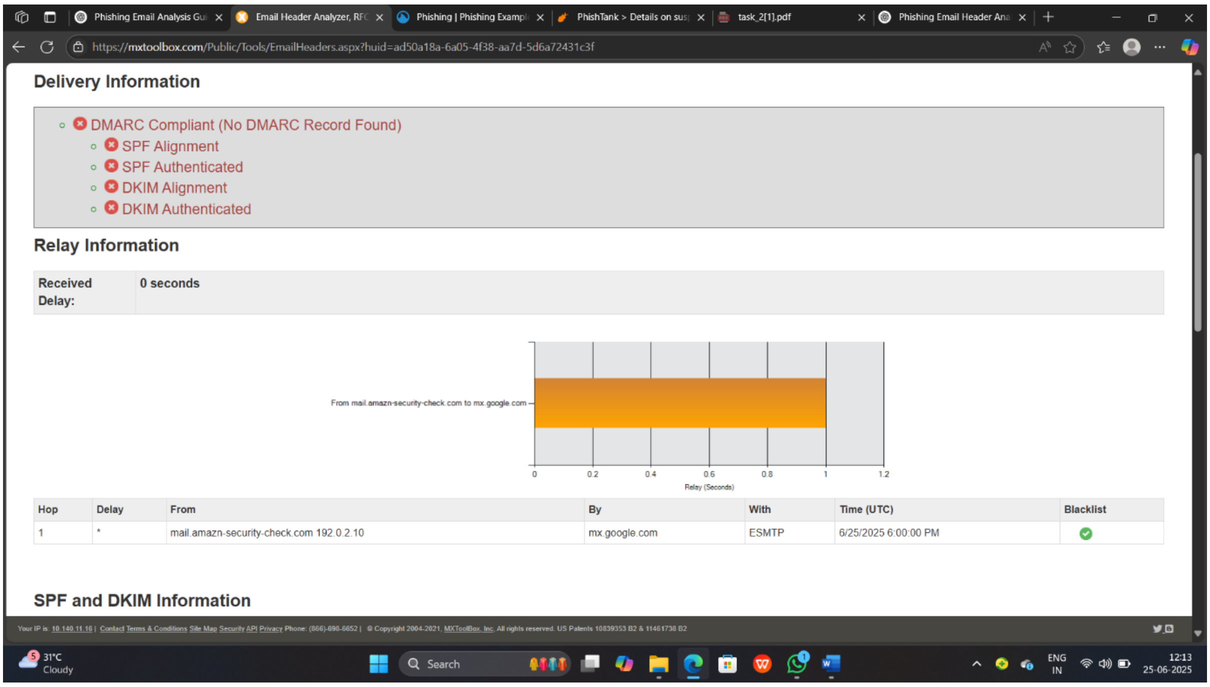
SPF and DKIM Information

Headers Found

Header Name	Header Value
Subject	Urgent: Account Suspension Notice

Received Header

Your IP is: 10.140.11.16 | 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
31°C
Cloudy
Search
ENG
IN
12:12
25-06-2025


Phishing Email Analysis Gui
Email Header Analyzer, RFC
Phishing | Phishing Example
PhishTank > Details on susp
task_2[1].pdf
Phishing Email Header Ana
https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=ad50a18a-6a05-4f38-aa7d-5d6a72431c3f

Delivery Information

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

Relay Information

Received Delay:	**0 seconds**

From mail.amazn-security-check.com to mx.google.com
0
0.2
0.4
0.6
0.8
1
1.2
Relay (Seconds)

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	mail.amazn-security-check.com 192.0.2.10	mx.google.com	ESMTP	6/25/2025 6:00:00 PM	✓

SPF and DKIM Information

Your IP is: 10.140.11.16 | 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
31°C
Cloudy
Search
ENG
IN
12:13
25-06-2025

Conclusion:

This email is a clear example of a phishing attempt. It uses a fake sender address, suspicious links, and urgent language to trick the user into clicking on a harmful website. The mismatched URL, possible spelling mistakes, and lack of proper security checks also show that it is not from a trusted source. Such emails should be reported and deleted to stay safe.

References:

- https://mxtoolbox.com
- https://www.phishing.org
- https://www.phishtank.com
- https://whois.domaintools.com
- https://chatgpt.com