FUTURE
INTERNS

Phishing Email Detection & Awareness Report

Phishing Detection & Awareness

Prepared by:

NAGULAPALLI SRIVIDYA NARASIMHA

Cybersecurity Task 2

INTRODUCTION

Phishing Email Detection & Awareness System:

Phishing is one of the most common and dangerous cyber threats targeting individuals and organizations worldwide. Attackers use deceptive emails to trick users into revealing sensitive information such as passwords, banking details, and personal data.

This project focuses on identifying phishing indicators, analyzing suspicious emails, and building awareness to prevent cyber fraud.

Objective

The objective of this task is to analyze a phishing email sample, identify malicious indicators, classify associated risks, and provide awareness guidelines to help users recognize and prevent phishing attacks

Phishing Email Sample

Email Sample Evidence:

A Suspicious email pretending to be form Amazon was analyzed. The email requests the user to verify account information through a provided link, Which is a common phishing technique used to steal user credentials.

Email Header Analysis

The email header was analyzed using an online header analysis tool. The analysis showed authentication and domain inconsistencies, indicating that the email was not sent from an official Amazon server and may be malicious.

Domain and Link Inspection

The email contains a hyperlink directing users to a suspicious domain that imitates Amazon but does not belong to the official Amazon website .
Further investigation using kali linux tools revealed suspicious domain details, confirming phishing activity.

Phishing Indicators Identified

Phishing Indicators

Several Phishing indicators were identified in the email::

- Fake sender domain
- Urgent action request
- Suspicious verification link
- Generic greeting message
- Account suspension warning

These signs indicate phishing behavior.

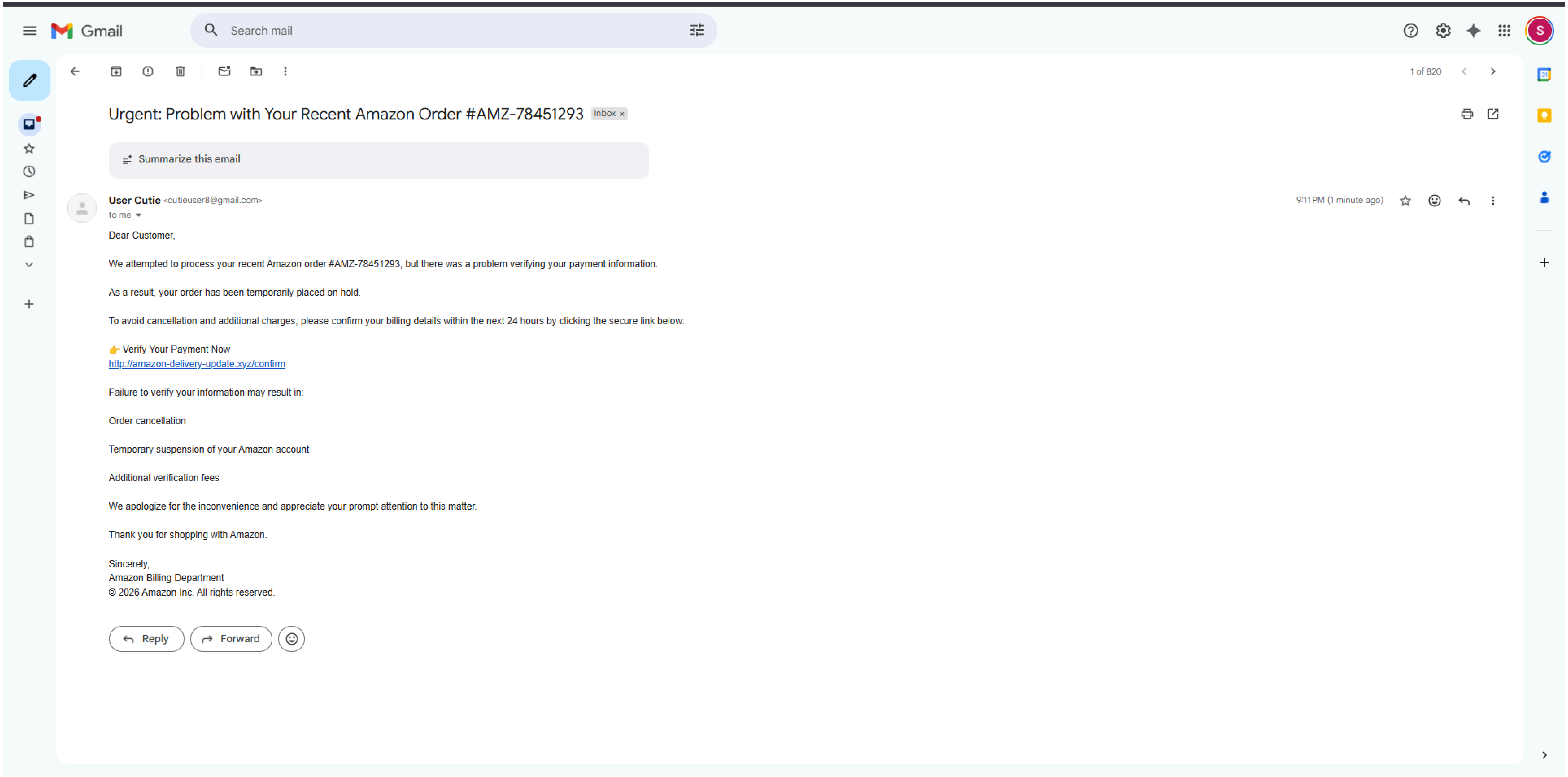
Risk Classification

The analyzed email is classified as Phishing(High Risk) because it attempts to deceive users into providing sensitive account information through a malicious link.

Attack Explanation

In this phishing attack, the attacker impersonates a trusted organization and sends fake emails to users. Victims are tricked into clicking malicious links and entering login credentials, which are then stolen by attackers.

Phishing Email Sample



Urgent: Problem with Your Recent Amazon Order #AMZ-78451293

User Cutie <cutieuser8@gmail.com>
to me

Dear Customer,

We attempted to process your recent Amazon order #AMZ-78451293, but there was a problem verifying your payment information.

As a result, your order has been temporarily placed on hold.

To avoid cancellation and additional charges, please confirm your billing details within the next 24 hours by clicking the secure link below:

👉 Verify Your Payment Now
http://amazon-delivery-update.xyz/confirm

Failure to verify your information may result in:

Order cancellation

Temporary suspension of your Amazon account

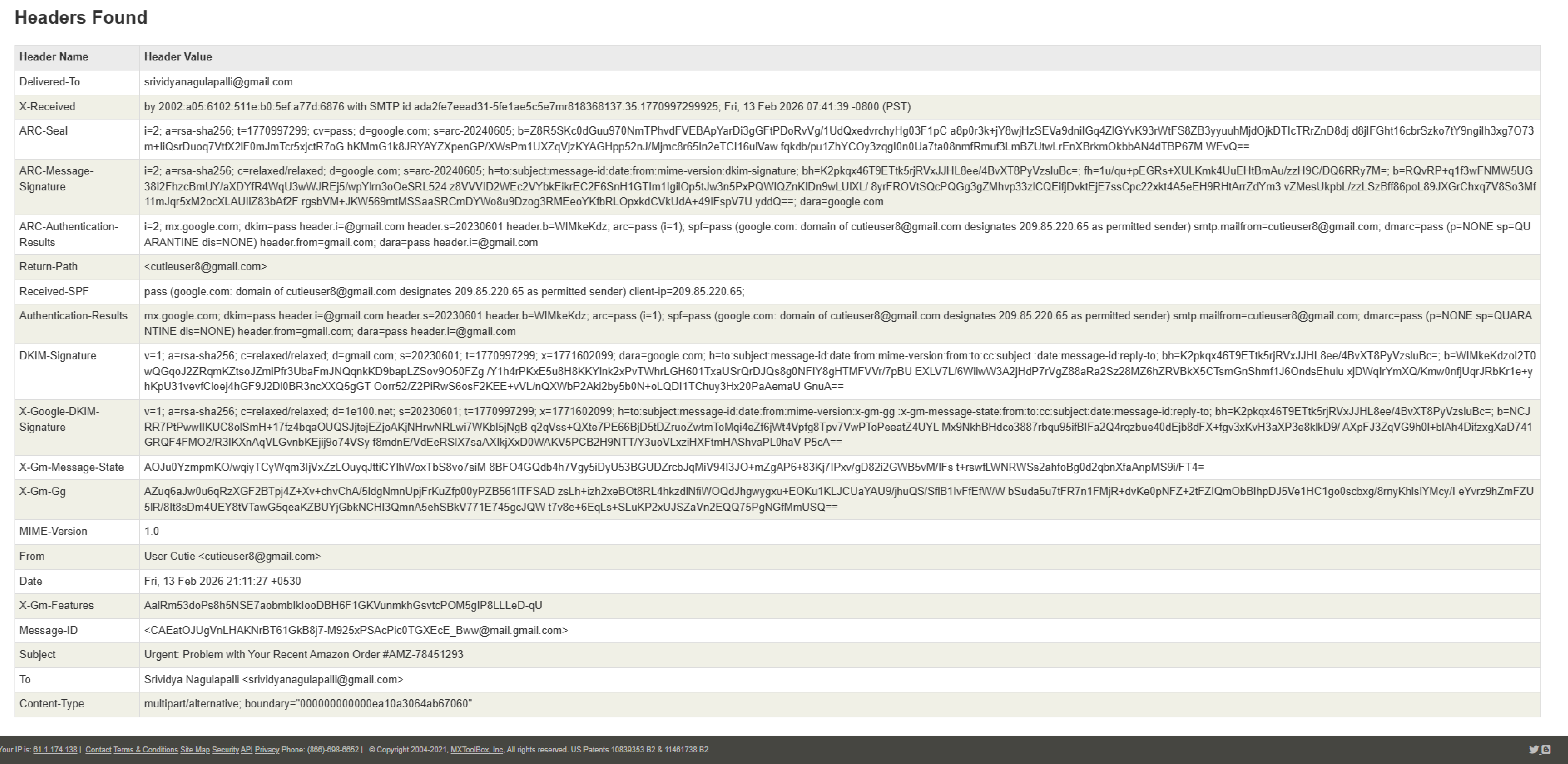
Additional verification fees

We apologize for the inconvenience and appreciate your prompt attention to this matter.

Thank you for shopping with Amazon.

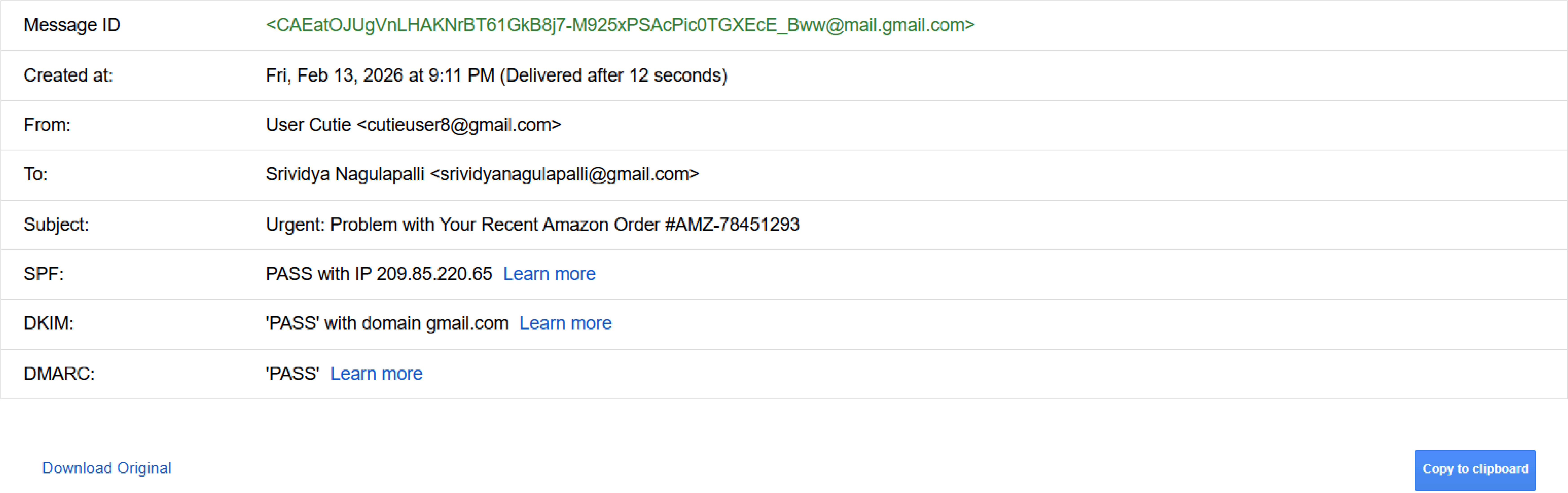
Sincerely,
Amazon Billing Department
© 2026 Amazon Inc. All rights reserved.

Email Header Analysis

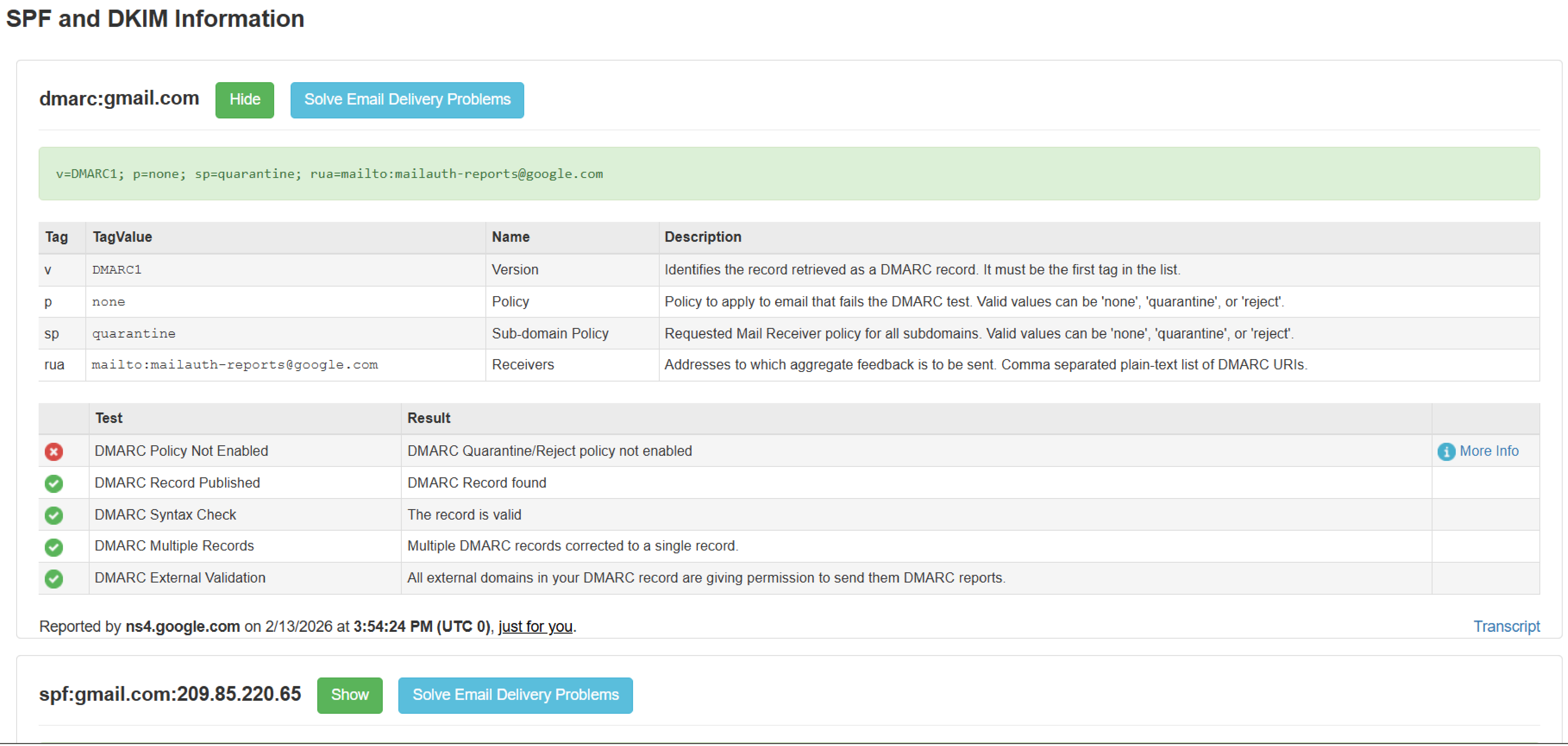


Headers Found

Header Name	Header Value
Delivered-To	srividyanagulapalli@gmail.com
X-Received	by 2002:a05:6102:511e:b0:5ef:a77d:6876 with SMTP id ada2fe7eead31-5fe1ae5c5e7mr818368137.35.1770997299925; Fri, 13 Feb 2026 07:41:39 -0800 (PST)
ARC-Seal	i=2; a=rsa-sha256; t=1770997299; cv=pass; d=google.com; s=arc-20240605; b=Z8R5SKc0dGuu970NmTPhvdFVEBApYarDi3gGFtPDoRvVg/1UdQxedvrchyHg03F1pC a8p0r3k+jY8wjHzSEVa9dnilGq4ZlGYvK93rWtFS8ZB3yyuuhMjdOjkDTIcTRrZnD8dj d8jIFGht16cbrSzko7tY9ngiIh3xg7O73m+liQsrDuoq7VtfX2lF0mJmTcr5xjctR7oG hKMmG1k8JRYAYZXpenGP/XWsPm1UXZqVjzKYAGHpp52nJ/Mjmc8r65In2eTCI16ulVaw fqkdb/pu1ZhYCOy3zqgI0n0Ua7ta08nmfRmuf3LmBZUtwLrEnXBrkmOkbbAN4dTBP67M WEvQ==
ARC-Message-Signature	i=2; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=to:subject:message-id:date:from:mime-version:dkim-signature; bh=K2pkqx46T9ETtk5rjRVxJJHL8ee/4BvXT8PyVzsluBc=; fh=1u/qu+pEGRs+XULKmk4UuEHtBmAu/zzH9C/DQ6RRy7M=; b=RQvRP+q1f3wFNMW5UG38l2FhzcBmUY/aXDYfR4WqU3wWJREj5/wpYIrn3oOeSRL524 z8VVVID2WEc2VYbkEikrEC2F6SnH1GTIm1IgilOp5tJw3n5PxPQWIQZnKIDn9wLUIXL/ 8yrFROVtSQcPQGg3gZMhvp33zICQEifjDvktEjE7ssCpc22xkt4A5eEH9RHtArrZdYm3 vZMesUkpbL/zzLSzBff86poL89JXGrChxq7V8So3Mf11mJqr5xM2ocXLAUIiZ83bAf2F rgsbVM+JKW569mtMSSaaSRCmDYWo8u9Dzog3RMEeoYKfbRLOpxkdCVkUdA+49IFspV7U yddQ==; dara=google.com
ARC-Authentication-Results	i=2; mx.google.com; dkim=pass header.i=@gmail.com header.s=20230601 header.b=WIMkeKdz; arc=pass (i=1); spf=pass (google.com: domain of cutieuser8@gmail.com designates 209.85.220.65 as permitted sender) smtp.mailfrom=cutieuser8@gmail.com; dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com; dara=pass header.i=@gmail.com
Return-Path	<cutieuser8@gmail.com>
Received-SPF	pass (google.com: domain of cutieuser8@gmail.com designates 209.85.220.65 as permitted sender) client-ip=209.85.220.65;
Authentication-Results	mx.google.com; dkim=pass header.i=@gmail.com header.s=20230601 header.b=WIMkeKdz; arc=pass (i=1); spf=pass (google.com: domain of cutieuser8@gmail.com designates 209.85.220.65 as permitted sender) smtp.mailfrom=cutieuser8@gmail.com; dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com; dara=pass header.i=@gmail.com
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=20230601; t=1770997299; x=1771602099; dara=google.com; h=to:subject:message-id:date:from:mime-version:from:to:cc:subject :date:message-id:reply-to; bh=K2pkqx46T9ETtk5rjRVxJJHL8ee/4BvXT8PyVzsluBc=; b=WIMkeKdzoI2T0wQGqoJ2ZRqmKZtsoJZmiPfr3UbaFmJNQqnkKD9bapLZSov9O50FZg /Y1h4rPKxE5u8H8KKYlnk2xPvTWhrLGH601TxaUSrQrDJQs8g0NFIY8gHTMFVVr/7pBU EXLV7L/6WiiwW3A2jHdP7rVgZ88aRa2Sz28MZ6hZRVBkX5CTsmGnShmf1J6OndsEhulu xjDWqIrYmXQ/Kmw0nfjUqrJRbKr1e+yhKpU31vevfCloej4hGF9J2DI0BR3ncXXQ5gGT Oorr52/Z2PiRwS6osF2KEE+vVL/nQXWbP2Aki2by5b0N+oLQDI1TChuy3Hx20PaAemaU GnuA==
X-Google-DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20230601; t=1770997299; x=1771602099; h=to:subject:message-id:date:from:mime-version:x-gm-gg :x-gm-message-state:from:to:cc:subject:date:message-id:reply-to; bh=K2pkqx46T9ETtk5rjRVxJJHL8ee/4BvXT8PyVzsluBc=; b=NCJRR7PtPwwIIKUC8olSmH+17fz4bqaOUQSJjtejEZjoAKjNHrwNRLwi7WKbI5jNgB q2qVss+QXte7PE66BjD5tDZruoZwtmToMqi4eZf6jWt4Vpfg8Tpv7VwPToPeeatZ4UYL Mx9NkhBHdco3887rbqu95ifBIFa2Q4rqzbue40dEjb8dFX+fgv3xKvH3aXP3e8klkD9/ AXpFJ3ZqVG9h0I+blAh4DifzxgXaD741GRQF4FMO2/R3IKXnAqVLGvnbKEjij9o74VSy f8mdnE/VdEeRSIX7saAXIkjXxD0WAKV5PCB2H9NTT/Y3uoVLxziHXFtmHAShvaPL0haV P5cA==
X-Gm-Message-State	AOJu0YzmpmKO/wqiyTCyWqm3IjVxZzLOuyqJttiCYlhWoxTbS8vo7siM 8BFO4GQdb4h7Vgy5iDyU53BGUDZrcbJqMiV94I3JO+mZgAP6+83Kj7IPxv/gD82i2GWB5vM/IFs t+rswfLWNRWSs2ahfoBg0d2qbnXfaAnpMS9i/FT4=
X-Gm-Gg	AZuq6aJw0u6qRzXGF2BTpj4Z+Xv+chvChA/5ldgNmnUpjFrKuZfp00yPZB561ITFSAD zsLh+izh2xeBOt8RL4hkzdlNfiWOQdJhgwygxu+EOKu1KLJCUaYAU9/jhuQS/SflB1IvFfEfW/W bSuda5u7tFR7n1FMjR+dvKe0pNFZ+2tFZIQmObBlhpDJ5Ve1HC1go0scbxg/8rnyKhlslYMcy/l eYvrz9hZmFZU5lR/8It8sDm4UEY8tVTawG5qeaKZBUYjGbkNCHI3QmnA5ehSBkV771E745gcJQW t7v8e+6EqLs+SLuKP2xUJSZaVn2EQQ75PgNGfMmUSQ==
MIME-Version	1.0
From	User Cutie <cutieuser8@gmail.com>
Date	Fri, 13 Feb 2026 21:11:27 +0530
X-Gm-Features	AaiRm53doPs8h5NSE7aobmblklooDBH6F1GKVunmkhGsvtcPOM5gIP8LLLeD-qU
Message-ID	<CAEatOJUgVnLHAKNrBT61GkB8j7-M925xPSAcPic0TGXEcE_Bww@mail.gmail.com>
Subject	Urgent: Problem with Your Recent Amazon Order #AMZ-78451293
To	Srividya Nagulapalli <srividyanagulapalli@gmail.com>
Content-Type	multipart/alternative; boundary="000000000000ea10a3064ab67060"



Message ID	<CAEatOJUgVnLHAKNrBT61GkB8j7-M925xPSAcPic0TGXEcE_Bww@mail.gmail.com>
Created at:	Fri, Feb 13, 2026 at 9:11 PM (Delivered after 12 seconds)
From:	User Cutie <cutieuser8@gmail.com>
To:	Srividya Nagulapalli <srividyanagulapalli@gmail.com>
Subject:	Urgent: Problem with Your Recent Amazon Order #AMZ-78451293
SPF:	PASS with IP 209.85.220.65 Learn more
DKIM:	'PASS' with domain gmail.com Learn more
DMARC:	'PASS' Learn more



SPF and DKIM Information

dmarc:gmail.com

```
v=DMARC1; p=none; sp=quarantine; rua=mailto:mailauth-reports@google.com
```

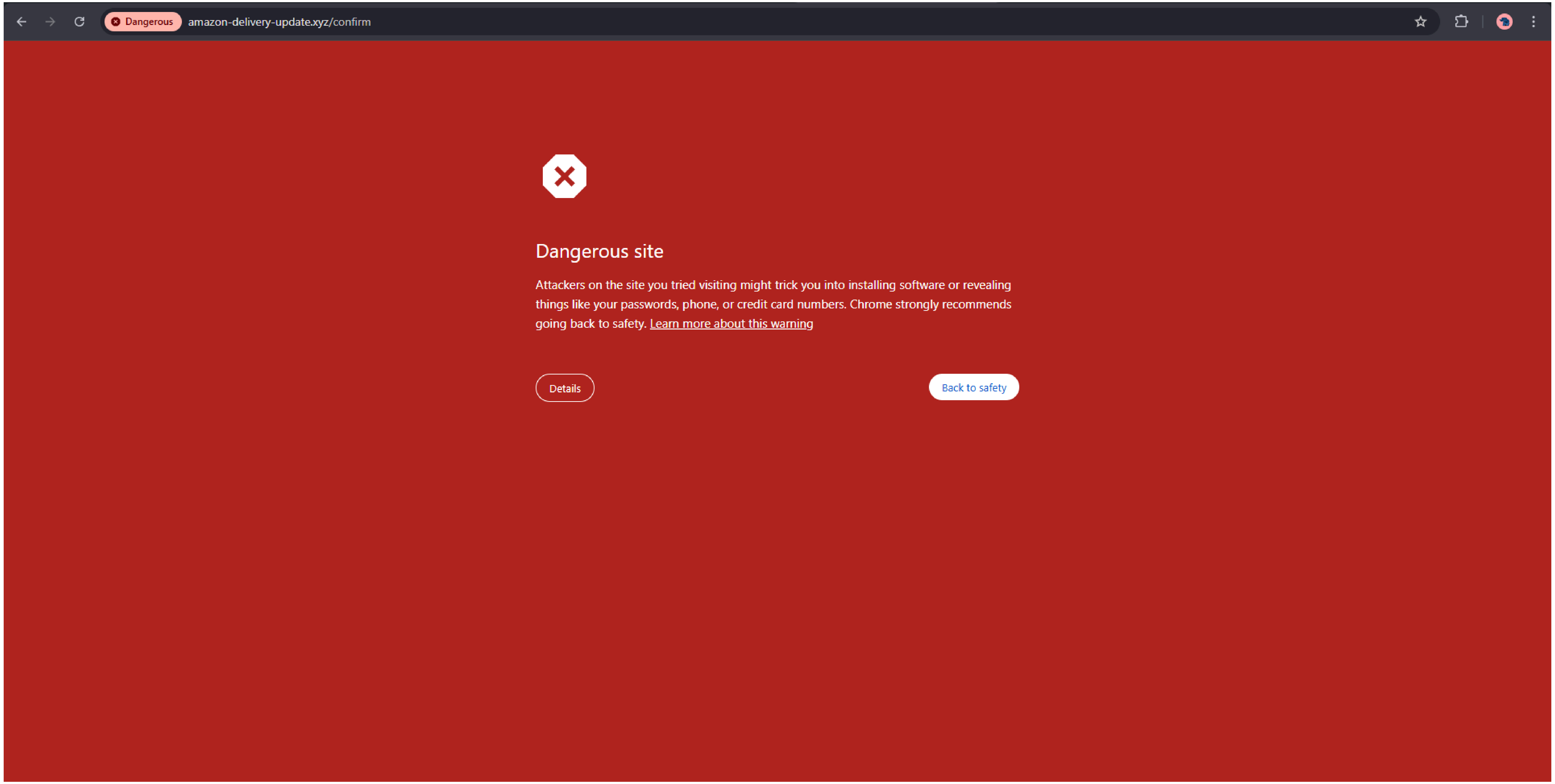
Tag	TagValue	Name	Description
v	`DMARC1`	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	`none`	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
sp	`quarantine`	Sub-domain Policy	Requested Mail Receiver policy for all subdomains. Valid values can be 'none', 'quarantine', or 'reject'.
rua	`mailto:mailauth-reports@google.com`	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.

	Test	Result	
✗	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	ℹ More Info
✓	DMARC Record Published	DMARC Record found	
✓	DMARC Syntax Check	The record is valid	
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.	
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.	

Reported by **ns4.google.com** on 2/13/2026 at **3:54:24 PM (UTC 0)**, just for you.

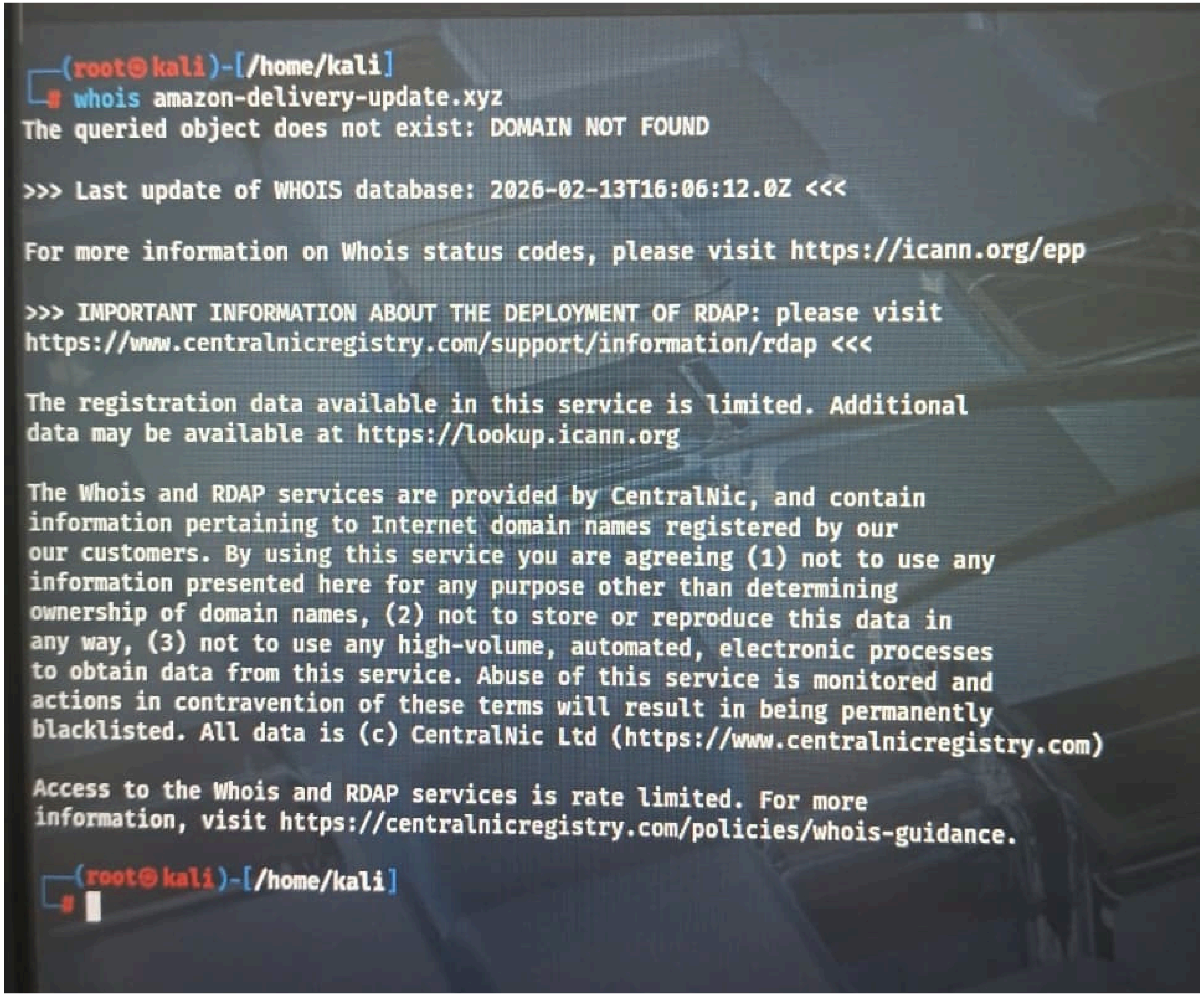
Transcript

spf:gmail.com:209.85.220.65

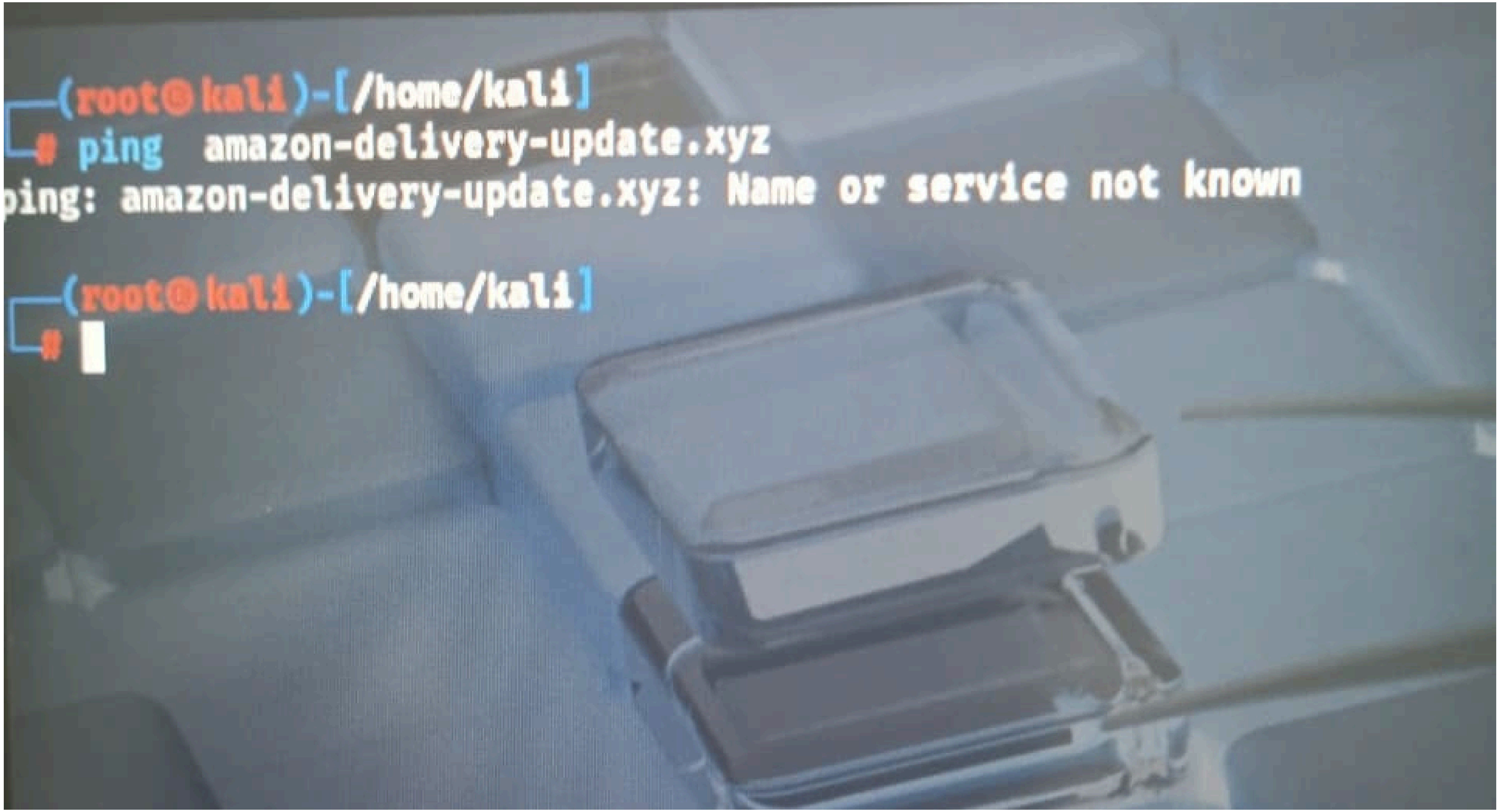


Dangerous site

Attackers on the site you tried visiting might trick you into installing software or revealing things like your passwords, phone, or credit card numbers. Chrome strongly recommends going back to safety. Learn more about this warning



```
┌──(root㉿kali)-[/home/kali]
└─# whois amazon-delivery-update.xyz
The queried object does not exist: DOMAIN NOT FOUND

>>> Last update of WHOIS database: 2026-02-13T16:06:12.0Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

>>> IMPORTANT INFORMATION ABOUT THE DEPLOYMENT OF RDAP: please visit
https://www.centralnicregistry.com/support/information/rdap <<<

The registration data available in this service is limited. Additional
data may be available at https://lookup.icann.org

The Whois and RDAP services are provided by CentralNic, and contain
information pertaining to Internet domain names registered by our
our customers. By using this service you are agreeing (1) not to use any
information presented here for any purpose other than determining
ownership of domain names, (2) not to store or reproduce this data in
any way, (3) not to use any high-volume, automated, electronic processes
to obtain data from this service. Abuse of this service is monitored and
actions in contravention of these terms will result in being permanently
blacklisted. All data is (c) CentralNic Ltd (https://www.centralnicregistry.com)

Access to the Whois and RDAP services is rate limited. For more
information, visit https://centralnicregistry.com/policies/whois-guidance.

┌──(root㉿kali)-[/home/kali]
└─# █
```



```
┌──(root㉿kali)-[/home/kali]
└─# ping  amazon-delivery-update.xyz
ping: amazon-delivery-update.xyz: Name or service not known

┌──(root㉿kali)-[/home/kali]
└─# 
```

Prevention Guidelines

Users can protect themselves from phishing attacks by following these practices:

- Do not click links from unknown or suspicious emails .
- Verify sender email domains carefully.
- Enable two-factor authentication(2FA).
- Report suspicious emails immediately.
- Never share passwords or OTP with anyone.

Conclusion

This analysis demonstrates how phishing emails operate and highlights the importance of user awareness and cautious behavior to protect personal and organizational data from cyber threats.