PHISHING EMAIL ANALYSIS

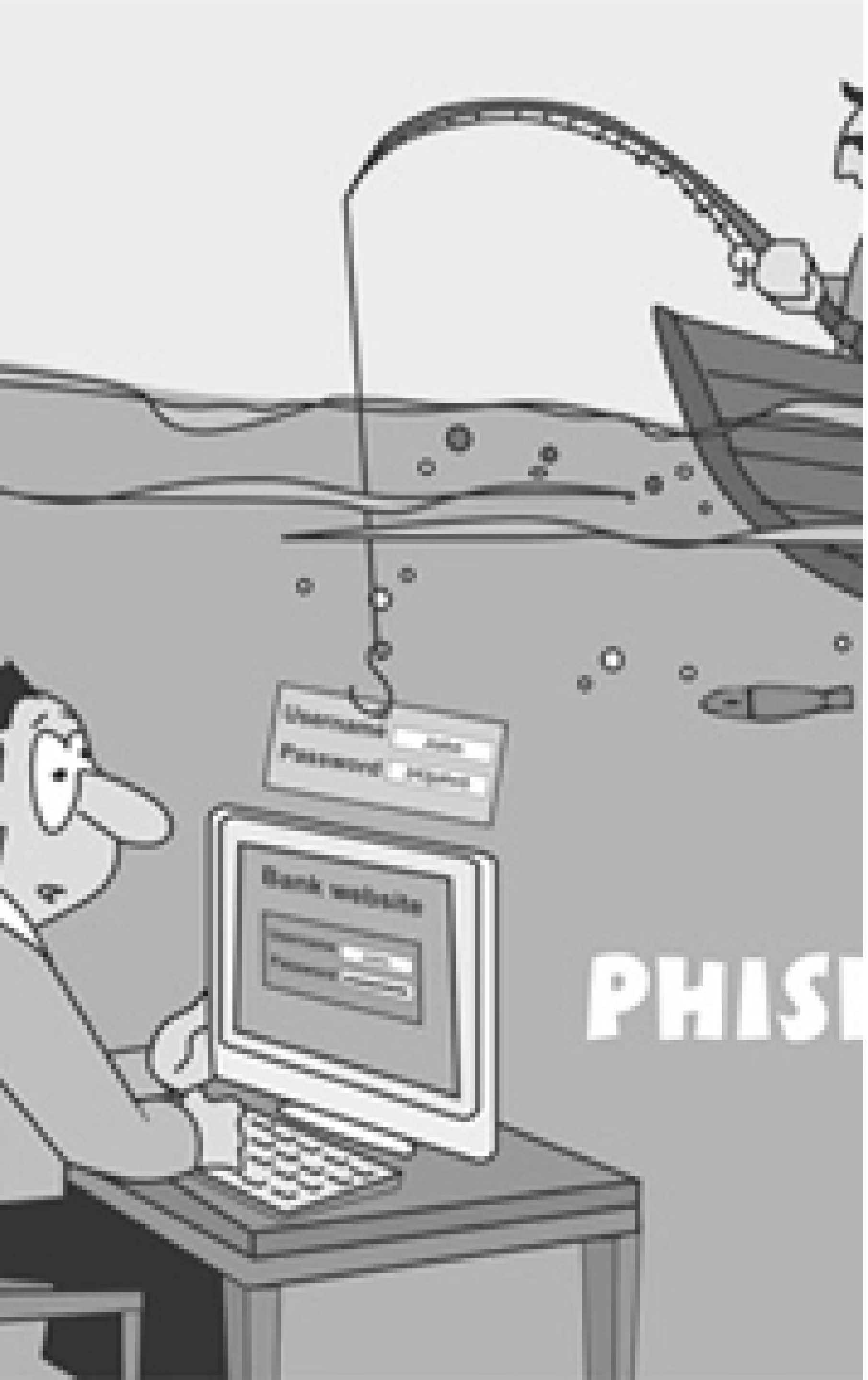
CASE STUDY:

MALICIOUS EMAIL RECEIVED DIRECTLY IN MY PERSONAL GMAIL

BY: ELIZABETH SESEBOR
DATE: 4TH DEC. 2025

CONTENT

- Understanding phishing in organizations
- Spotting a spoofed email
- Analyzing suspicious urlS
- Investigating email headers
- Leveraging email security/filtering tools
- Remediation strategies
- conclusion



WHAT IS PHISHING?

Phishing is a type of social engineering attack in which an attacker impersonates a trusted entity to trick recipients into revealing sensitive information, clicking malicious links, or executing harmful attachments.

Why it matters to organizations:

- Can lead to credential theft, financial loss, data breach, and malware infection.
- Often targets employees via email, chat, or other communication platforms.

COMMON TYPES OF PHISHING IN ORGANIZATIONS

Spear Phishing: Targeted emails crafted for specific individuals or roles (uses personal details).

Whaling: High-value target attacks (CEO/CFO) — often financially motivated.

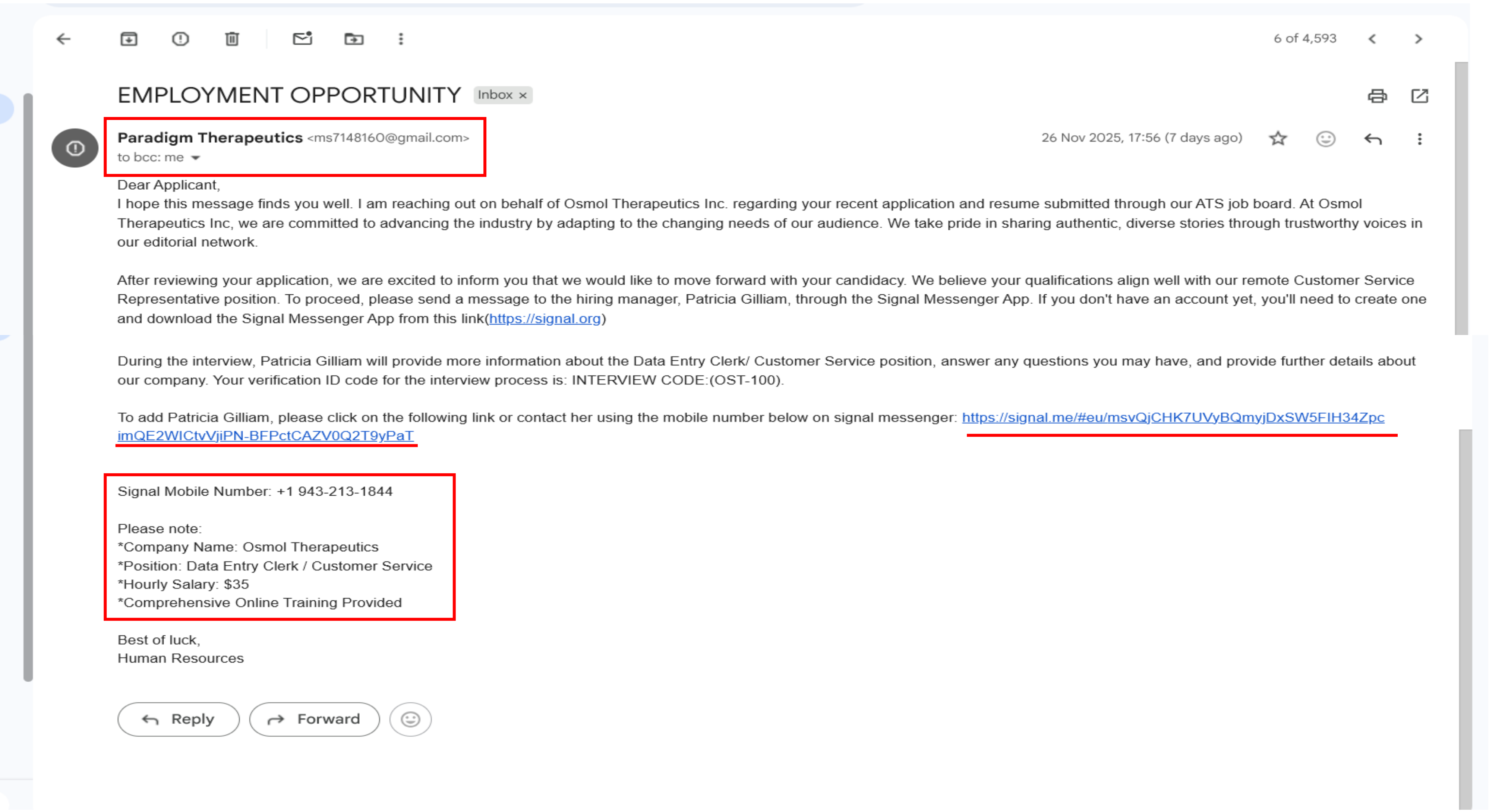
Business Email Compromise (BEC): Fraudulent requests that appear to come from executives or vendors asking for fund transfers or confidential info.

Clone Phishing: A legitimate email is copied, modified with malicious links/attachments, then resent.

Credential Harvesting: Fake login pages used to capture usernames/passwords.

Malicious Attachments: Emails carrying weaponized docs or executables.

SPOTTING A SPOOFED EMAIL



EMPLOYMENT OPPORTUNITY

Paradigm Therapeutics <ms7148160@gmail.com>
to bcc: me

26 Nov 2025, 17:56 (7 days ago)

Dear Applicant,
I hope this message finds you well. I am reaching out on behalf of Osmol Therapeutics Inc. regarding your recent application and resume submitted through our ATS job board. At Osmol Therapeutics Inc, we are committed to advancing the industry by adapting to the changing needs of our audience. We take pride in sharing authentic, diverse stories through trustworthy voices in our editorial network.

After reviewing your application, we are excited to inform you that we would like to move forward with your candidacy. We believe your qualifications align well with our remote Customer Service Representative position. To proceed, please send a message to the hiring manager, Patricia Gilliam, through the Signal Messenger App. If you don't have an account yet, you'll need to create one and download the Signal Messenger App from this link(https://signal.org)

During the interview, Patricia Gilliam will provide more information about the Data Entry Clerk/ Customer Service position, answer any questions you may have, and provide further details about our company. Your verification ID code for the interview process is: INTERVIEW CODE:(OST-100).

To add Patricia Gilliam, please click on the following link or contact her using the mobile number below on signal messenger: https://signal.me/#eu/msvQjCHK7UVyBQmyjDxSW5FIH34ZpcimQE2WICtvVjiPN-BFPctCAZV0Q2T9yPaT

Signal Mobile Number: +1 943-213-1844

Please note:
*Company Name: Osmol Therapeutics
*Position: Data Entry Clerk / Customer Service
*Hourly Salary: $35
*Comprehensive Online Training Provided

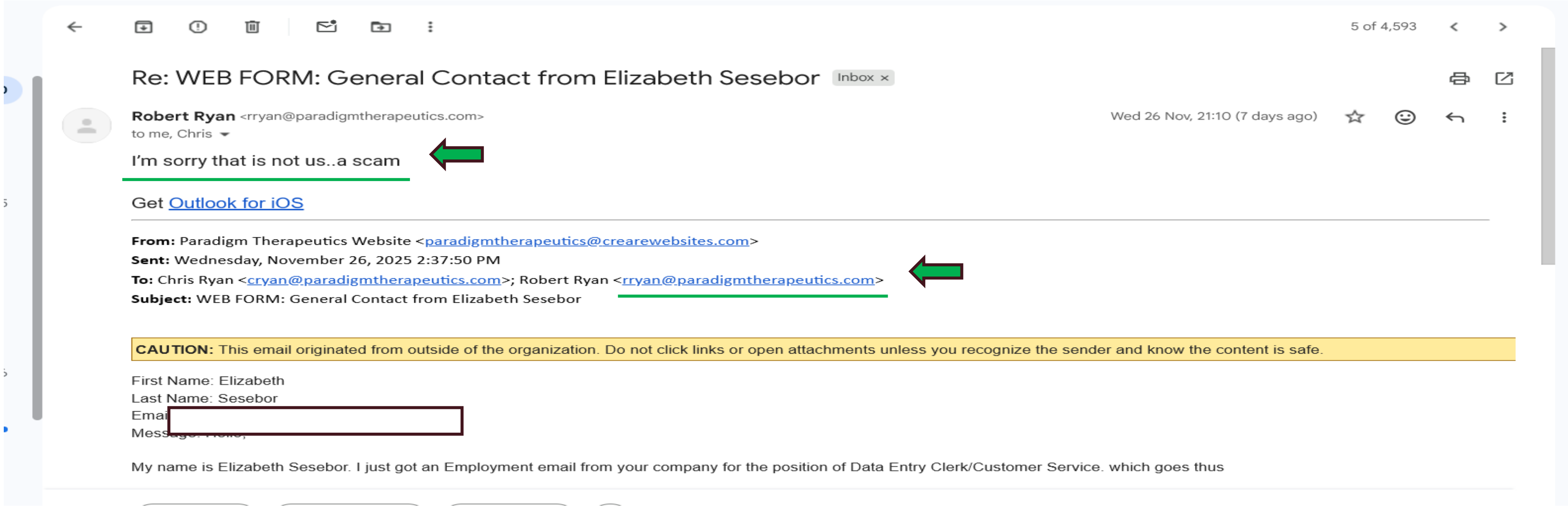
Best of luck,
Human Resources

The above screenshot shows a job-related email that was delivered to my personal inbox. The highlighted sections in red indicate several indicators that quickly identified the email as a **spoofed and potentially malicious message**.

The subject line was *“Employment Opportunity”*, and the sender claimed to represent a company named **Paradigm Therapeutics**. However, the sender's email address used a public domain (**gmail.com**) instead of an official corporate domain, which is a strong sign of impersonation. The message advertised an attractive pay rate of **$35 per hour** and listed an inconsistent job title (*Data Entry Clerk / Customer Service Representative*), which raised suspicion.
Using the **S.T.O.P phishing detection model**:

- **S – Suspicious:** The sender did not use an official company domain.
- **T – Tells you to click a link:** The email included a call-to-action link.
- **O – Offering something too good to be true:** A high hourly wage was offered for an unclear role.
- **P – Pressures you to act fast:** *(Not observed in this case)*

This email clearly triggered the first three indicators, making it highly suspicious.
To validate the legitimacy of the sender, I independently searched for Paradigm Therapeutics and contacted the company directly via their official website email address. The response received (shown below) confirmed that the email did **not** originate from them. The responder clearly used the legitimate domain (@paradigmtherapeutics.com), which verified that the email I received was **fraudulent** and that any link contained in the message was unsafe to click.



Re: WEB FORM: General Contact from Elizabeth Sesebor

Robert Ryan <rryan@paradigmtherapeutics.com>
to me, Chris
Wed 26 Nov, 21:10 (7 days ago)

I'm sorry that is not us..a scam

Get Outlook for iOS

From: Paradigm Therapeutics Website <paradigmtherapeutics@crearewebsites.com>
Sent: Wednesday, November 26, 2025 2:37:50 PM
To: Chris Ryan <cryan@paradigmtherapeutics.com>; Robert Ryan <rryan@paradigmtherapeutics.com>
Subject: WEB FORM: General Contact from Elizabeth Sesebor

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

First Name: Elizabeth
Last Name: Sesebor
Emai[redacted]
Mess

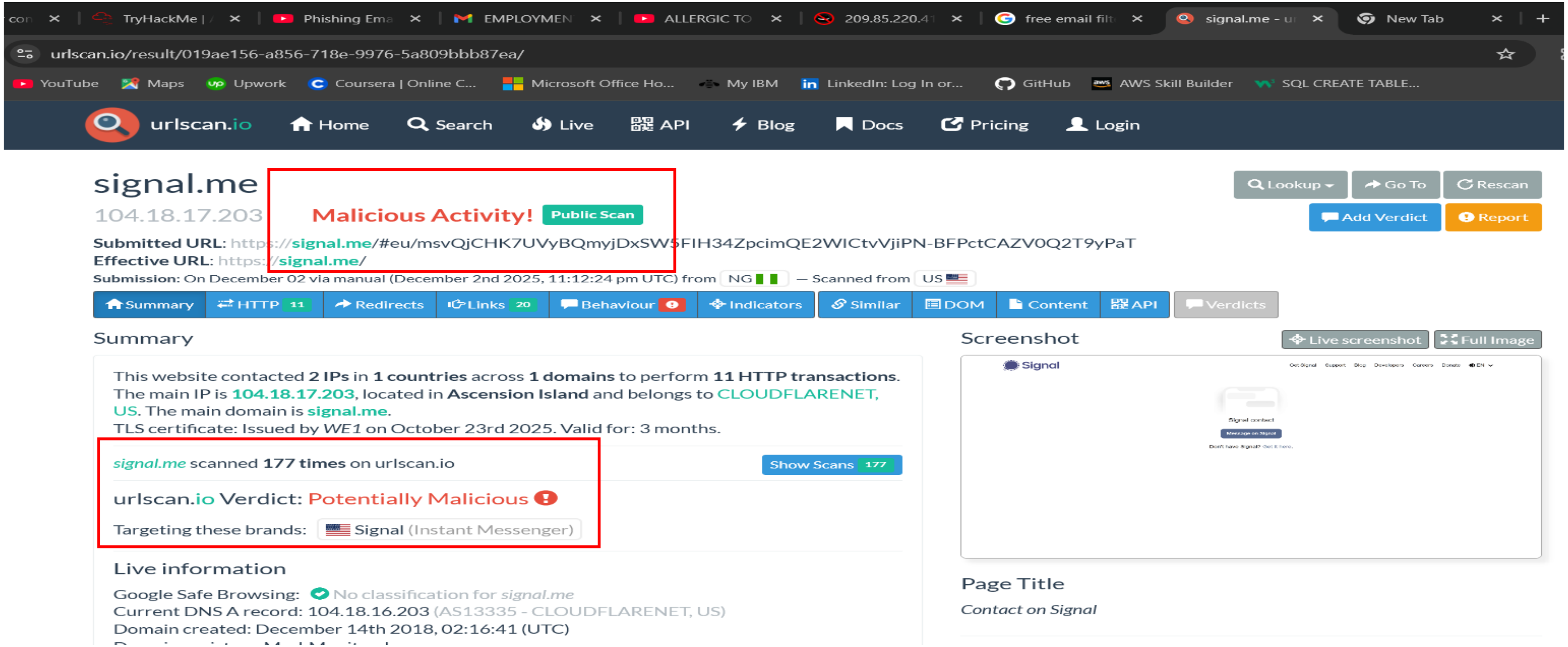
My name is Elizabeth Sesebor. I just got an Employment email from your company for the position of Data Entry Clerk/Customer Service. which goes thus

To further confirm the malicious nature of the email, I conducted a deeper investigation of the embedded link using the tool **urlscan.io**.

This analysis resolved the destination of the link, identified redirections, and revealed indicators commonly associated with phishing websites. The results provided further confirmation that the link was unsafe and associated with suspicious hosting behavior.

The screenshot below displays the output of the URL analysis.

ANALYZING SUSPICIOUS URLs



signal.me
104.18.17.203

Malicious Activity! Public Scan

Submitted URL: https://signal.me/#eu/msvQjCHK7UVyBQmyjDxSW5FIH34ZpcimQE2WICtvVjiPN-BFPctCAZV0Q2T9yPaT
Effective URL: https://signal.me/
Submission: On December 02 via manual (December 2nd 2025, 11:12:24 pm UTC) from NG — Scanned from US

Summary

This website contacted **2 IPs** in **1 countries** across **1 domains** to perform **11 HTTP transactions**. The main IP is **104.18.17.203**, located in **Ascension Island** and belongs to **CLOUDFLARENET, US**. The main domain is **signal.me**.
TLS certificate: Issued by *WE1* on October 23rd 2025. Valid for: 3 months.

signal.me scanned **177 times** on urlscan.io Show Scans 177

urlscan.io Verdict: Potentially Malicious

Targeting these brands: Signal (Instant Messenger)

Live information

Google Safe Browsing: No classification for *signal.me*
Current DNS A record: 104.18.16.203 (AS13335 - CLOUDFLARENET, US)
Domain created: December 14th 2018, 02:16:41 (UTC)

Screenshot

Page Title

Contact on Signal

INESTIGATING EMAIL HEADERS

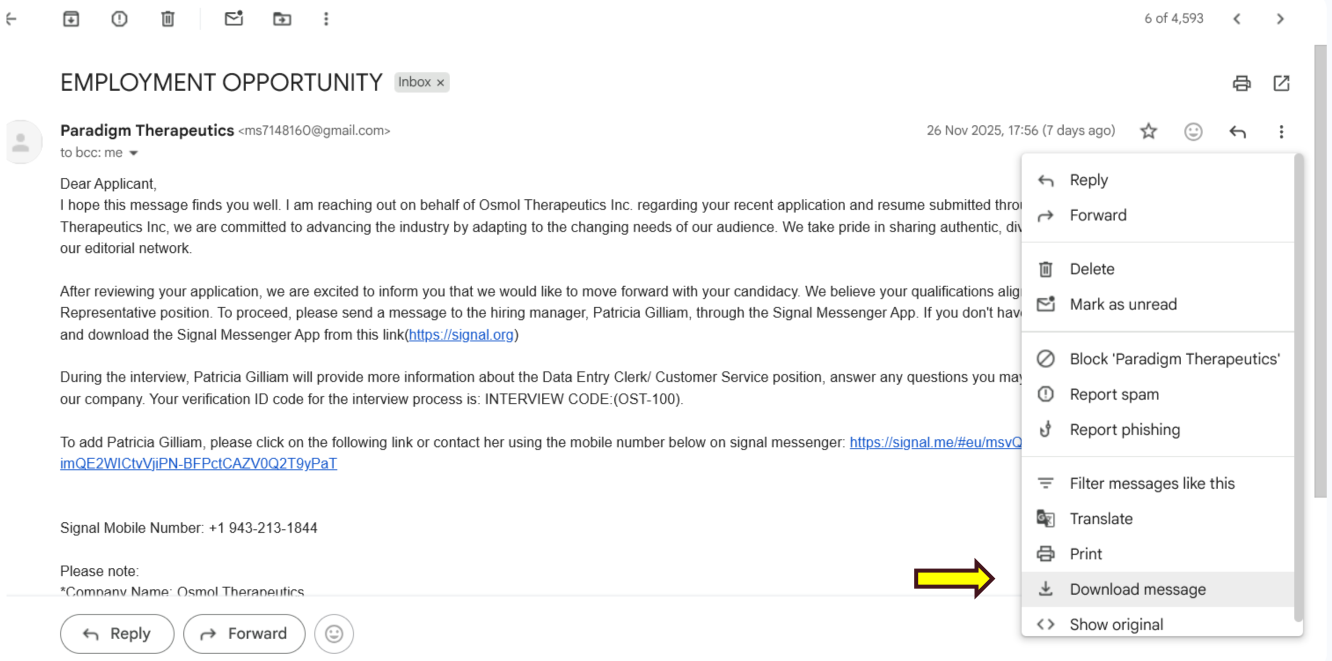
The next phase of the investigation was **email header analysis**, which helps determine the true source of an email.

I exported the message as a file and opened it using **Notepad** to view the raw header data. A second tool, **MxToolBox**, was also used to assist with header parsing and interpretation.

The header analysis revealed details about:

- Sending mail servers
- Origin IP address
- SPF, DKIM, and DMARC authentication results
- Message routing path
- Domain used
- Mail transfer agents involved

All these elements are critical for forensically reviewing phishing emails and tracing their origin.



EMPLOYMENT OPPORTUNITY

Paradigm Therapeutics <ms7148160@gmail.com>
to bcc: me

26 Nov 2025, 17:56 (7 days ago)

Dear Applicant,
I hope this message finds you well. I am reaching out on behalf of Osmol Therapeutics Inc. regarding your recent application and resume submitted thro
Therapeutics Inc, we are committed to advancing the industry by adapting to the changing needs of our audience. We take pride in sharing authentic, div
our editorial network.

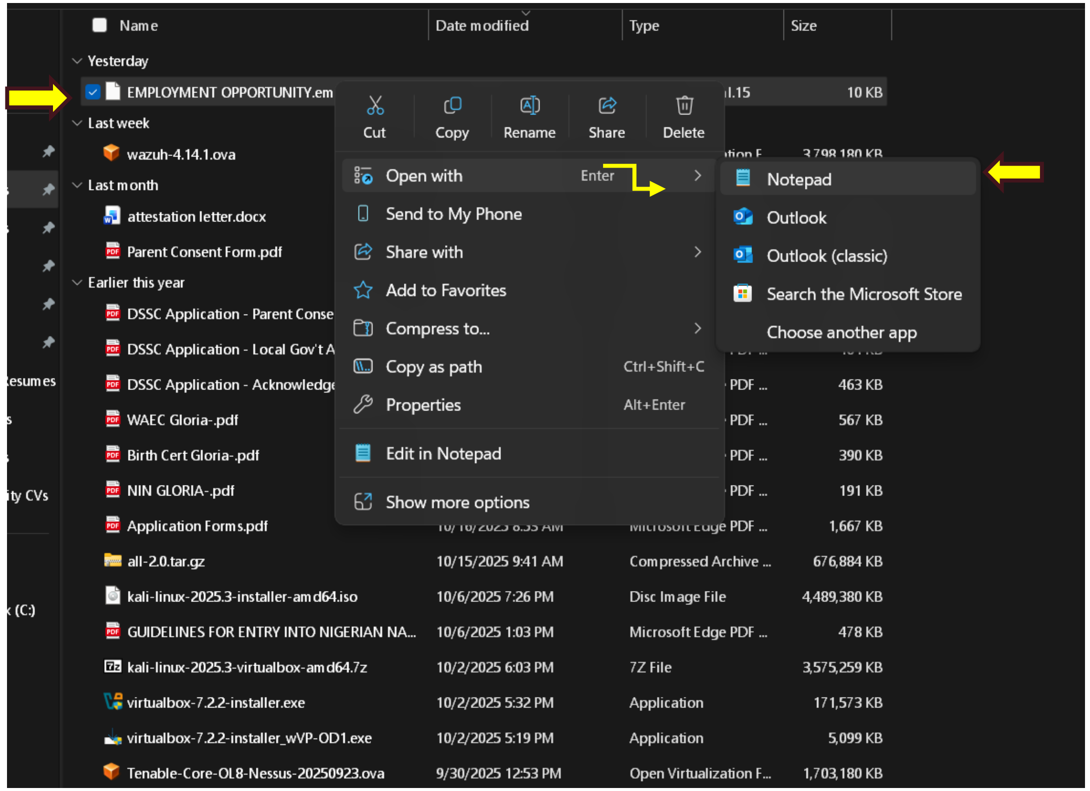
After reviewing your application, we are excited to inform you that we would like to move forward with your candidacy. We believe your qualifications alig
Representative position. To proceed, please send a message to the hiring manager, Patricia Gilliam, through the Signal Messenger App. If you don't hav
and download the Signal Messenger App from this link(https://signal.org)

During the interview, Patricia Gilliam will provide more information about the Data Entry Clerk/ Customer Service position, answer any questions you ma
our company. Your verification ID code for the interview process is: INTERVIEW CODE:(OST-100).

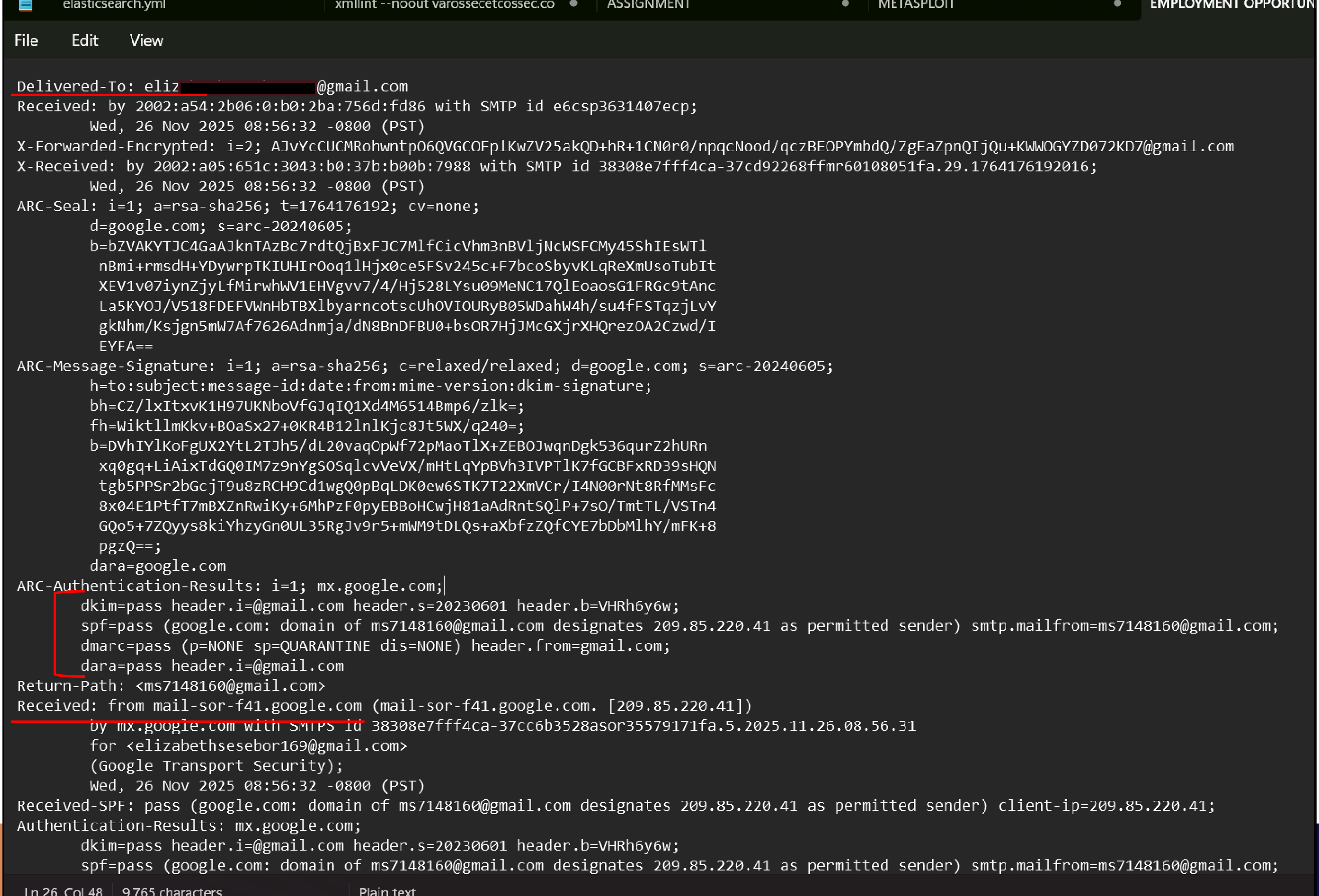
To add Patricia Gilliam, please click on the following link or contact her using the mobile number below on signal messenger: https://signal.me/#eu/msvQ
imQE2WICtvVjiPN-BFPctCAZV0Q2T9yPaT

Signal Mobile Number: +1 943-213-1844

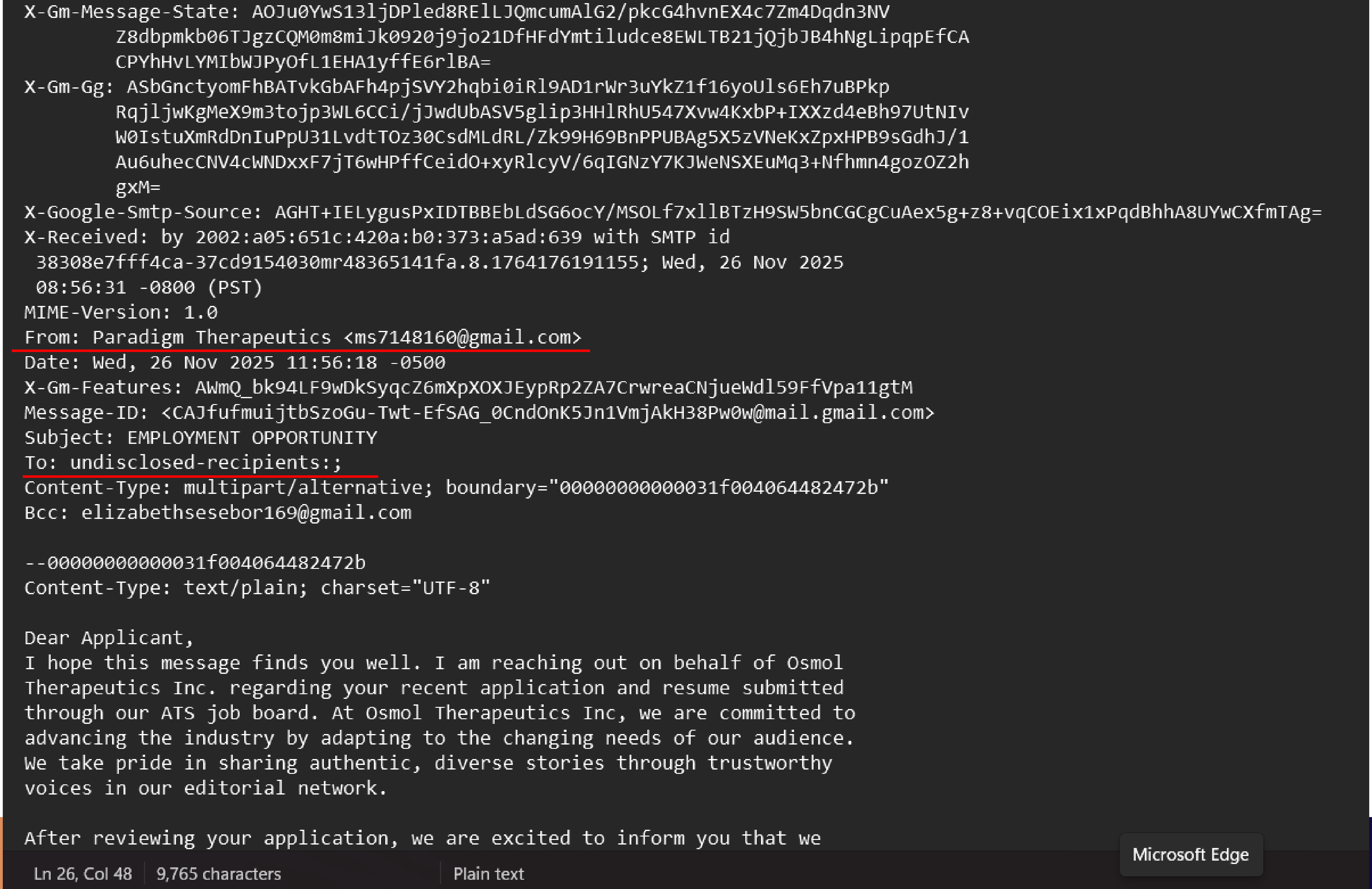
Please note:
*Company Name: Osmol Therapeutics



Name	Date modified	Type	Size
Yesterday			
EMPLOYMENT OPPORTUNITY.em		l.15	10 KB
Last week			
wazuh-4.14.1.ova		tion F	3,798,180 KB
Last month			
attestation letter.docx			
Parent Consent Form.pdf			
Earlier this year			
DSSC Application - Parent Conse			
DSSC Application - Local Gov't A		PDF ...	
DSSC Application - Acknowledge		PDF ...	463 KB
WAEC Gloria-.pdf		PDF ...	567 KB
Birth Cert Gloria-.pdf		PDF ...	390 KB
NIN GLORIA-.pdf		PDF ...	191 KB
Application Forms.pdf	10/16/2025 8:35 AM	Microsoft Edge PDF ...	1,667 KB
all-2.0.tar.gz	10/15/2025 9:41 AM	Compressed Archive ...	676,884 KB
kali-linux-2025.3-installer-amd64.iso	10/6/2025 7:26 PM	Disc Image File	4,489,380 KB
GUIDELINES FOR ENTRY INTO NIGERIAN NA...	10/6/2025 1:03 PM	Microsoft Edge PDF ...	478 KB
kali-linux-2025.3-virtualbox-amd64.7z	10/2/2025 6:03 PM	7Z File	3,575,259 KB
virtualbox-7.2.2-installer.exe	10/2/2025 5:32 PM	Application	171,573 KB
virtualbox-7.2.2-installer_wVP-OD1.exe	10/2/2025 5:19 PM	Application	5,099 KB
Tenable-Core-OL8-Nessus-20250923.ova	9/30/2025 12:53 PM	Open Virtualization F...	1,703,180 KB



```
Delivered-To: eliz[redacted]@gmail.com
Received: by 2002:a54:2b06:0:b0:2ba:756d:fd86 with SMTP id e6csp3631407ecp;
        Wed, 26 Nov 2025 08:56:32 -0800 (PST)
X-Forwarded-Encrypted: i=2; AJvYcCUCMRohwntpO6QVGCOFplKwZV25akQD+hR+1CN0r0/npqcNood/qczBEOPYmbdQ/ZgEaZpnQIjQu+KWWOGYZD072KD7@gmail.com
X-Received: by 2002:a05:651c:3043:b0:37b:b00b:7988 with SMTP id 38308e7fff4ca-37cd92268ffmr60108051fa.29.1764176192016;
        Wed, 26 Nov 2025 08:56:32 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1764176192; cv=none;
        d=google.com; s=arc-20240605;
        b=bZVAKYTJC4GaAJknTAzBc7rdtQjBxFJC7MlfCicVhm3nBVljNcWSFCMy45ShIEsWTl
         nBmi+rmsdH+YDywrpTKIUHIrOoq1lHjx0ce5FSv245c+F7bcoSbyvKLqReXmUsoTubIt
         XEV1v07iynZjyLfMirwhWV1EHVgvv7/4/Hj528LYsu09MeNC17QlEoaosG1FRGc9tAnc
         La5KYOJ/V518FDEFVWnHbTBXlbyarncotscUhOVIOURyB05WDahW4h/su4fFSTqzjLvY
         gkNhm/Ksjgn5mW7Af7626Adnmja/dN8BnDFBU0+bsOR7HjJMcGXjrXHQrezOA2Czwd/I
         EYFA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
        h=to:subject:message-id:date:from:mime-version:dkim-signature;
        bh=CZ/lxItxvK1H97UKNboVfGJqIQ1Xd4M6514Bmp6/zlk=;
        fh=WiktllmKkv+BOaSx27+0KR4B12lnlKjc8Jt5WX/q240=;
        b=DVhIYlKoFgUX2YtL2TJh5/dL20vaqOpWf72pMaoTlX+ZEBOJwqnDgk536qurZ2hURn
         xq0gq+LiAixTdGQ0IM7z9nYgSOSqlcvVeVX/mHtLqYpBVh3IVPTlK7fGCBFxRD39sHQN
         tgb5PPSr2bGcjT9u8zRCH9Cd1wgQ0pBqLDK0ew6STK7T22XmVCr/I4N00rNt8RfMMsFc
         8x04E1PtfT7mBXZnRwiKy+6MhPzF0pyEBBoHCwjH81aAdRntSQlP+7sO/TmtTL/VSTn4
         GQo5+7ZQyys8kiYhzyGn0UL35RgJv9r5+mWM9tDLQs+aXbfzZQfCYE7bDbMlhY/mFK+8
         pgzQ==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20230601 header.b=VHRh6y6w;
       spf=pass (google.com: domain of ms7148160@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=ms7148160@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com;
       dara=pass header.i=@gmail.com
Return-Path: <ms7148160@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id 38308e7fff4ca-37cc6b3528asor35579171fa.5.2025.11.26.08.56.31
        for <elizabethsesebor169@gmail.com>
        (Google Transport Security);
        Wed, 26 Nov 2025 08:56:32 -0800 (PST)
Received-SPF: pass (google.com: domain of ms7148160@gmail.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20230601 header.b=VHRh6y6w;
       spf=pass (google.com: domain of ms7148160@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=ms7148160@gmail.com;
```



```
X-Gm-Message-State: AOJu0YwS13ljDPled8RElLJQmcumAlG2/pkcG4hvnEX4c7Zm4Dqdn3NV
        Z8dbpmkb06TJgzCQM0m8miJk0920j9jo21DfHFdYmtiludce8EWLTB21jQjbJB4hNgLipqpEfCA
        CPYhHvLYMIbWJPyOfL1EHA1yffE6rlBA=
X-Gm-Gg: ASbGnctyomFhBATvkGbAFh4pjSVY2hqbi0iRl9AD1rWr3uYkZ1f16yoUls6Eh7uBPkp
        RqjljwKgMeX9m3tojp3WL6CCi/jJwdUbASV5glip3HHlRhU547Xvw4KxbP+IXXzd4eBh97UtNIv
        W0IstuXmRdDnIuPpU31LvdtTOz30CsdMLdRL/Zk99H69BnPPUBAg5X5zVNeKxZpxHPB9sGdhJ/1
        Au6uhecCNV4cWNDxxF7jT6wHPffCeidO+xyRlcyV/6qIGNzY7KJWeNSXEuMq3+Nfhmn4gozOZ2h
        gxM=
X-Google-Smtp-Source: AGHT+IELygusPxIDTBBEbLdSG6ocY/MSOLf7xllBTzH9SW5bnCGCgCuAex5g+z8+vqCOEix1xPqdBhhA8UYwCXfmTAg=
X-Received: by 2002:a05:651c:420a:b0:373:a5ad:639 with SMTP id
 38308e7fff4ca-37cd9154030mr48365141fa.8.1764176191155; Wed, 26 Nov 2025
 08:56:31 -0800 (PST)
MIME-Version: 1.0
From: Paradigm Therapeutics <ms7148160@gmail.com>
Date: Wed, 26 Nov 2025 11:56:18 -0500
X-Gm-Features: AWmQ_bk94LF9wDkSyqcZ6mXpXOXJEypRp2ZA7CrwreaCNjueWdl59FfVpa11gtM
Message-ID: <CAJfufmuijtbSzoGu-Twt-EfSAG_0CndOnK5Jn1VmjAkH38Pw0w@mail.gmail.com>
Subject: EMPLOYMENT OPPORTUNITY
To: undisclosed-recipients:;
Content-Type: multipart/alternative; boundary="00000000000031f004064482472b"
Bcc: elizabethsesebor169@gmail.com

--00000000000031f004064482472b
Content-Type: text/plain; charset="UTF-8"

Dear Applicant,
I hope this message finds you well. I am reaching out on behalf of Osmol
Therapeutics Inc. regarding your recent application and resume submitted
through our ATS job board. At Osmol Therapeutics Inc, we are committed to
advancing the industry by adapting to the changing needs of our audience.
We take pride in sharing authentic, diverse stories through trustworthy
voices in our editorial network.

After reviewing your application, we are excited to inform you that we
```

Under the **Authentication Results**, SPF, DKIM, and DMARC all passed, and the sending domain showed as **gmail.com**, which is a legitimate and trusted domain. However, deeper inspection revealed a major discrepancy:

- **From:** “Paradigm Therapeutics” ms7148160@gmail.com
- **Return-Path:** ms7148160@gmail.com

This indicates that although the message passed authentication checks, the sender **did not** originate from Paradigm Therapeutics but from a personal Gmail account—confirming impersonation.

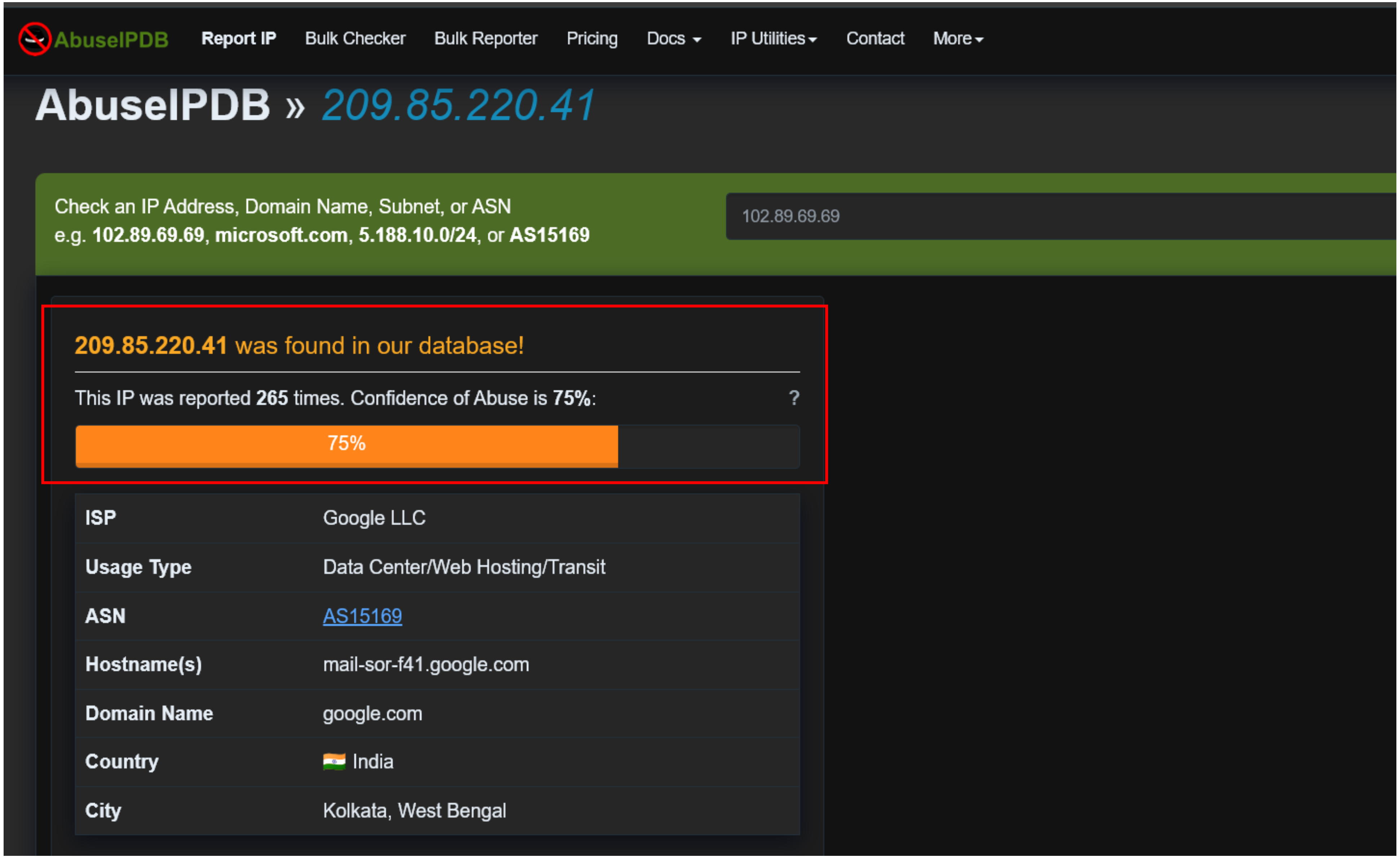
The sending server was identified as **mail-sor-f41**, a legitimate Google mail server. Attackers frequently exploit trusted email service providers like Google to send phishing emails, allowing them to bypass initial filtering mechanisms and appear legitimate.

I also ran the sender IP address through **AbuseIPDB**,(diagram shown below) which showed:

- The IP had been reported **265 times**
- Geographic location: India (ISP location, not necessarily the attacker)
- This suggests historical abuse or suspicious activity associated with the IP.

Another red flag identified was:

- The email was sent using **“To: undisclosed recipients”**, which is often used during bulk phishing campaigns to prevent recipients from seeing each other.



AbuseIPDB » 209.85.220.41

Check an IP Address, Domain Name, Subnet, or ASN
e.g. **102.89.69.69**, **microsoft.com**, **5.188.10.0/24**, or **AS15169**

209.85.220.41 was found in our database!

This IP was reported **265** times. Confidence of Abuse is **75%**:

ISP	Google LLC
Usage Type	Data Center/Web Hosting/Transit
ASN	AS15169
Hostname(s)	mail-sor-f41.google.com
Domain Name	google.com
Country	🇮🇳 India
City	Kolkata, West Bengal

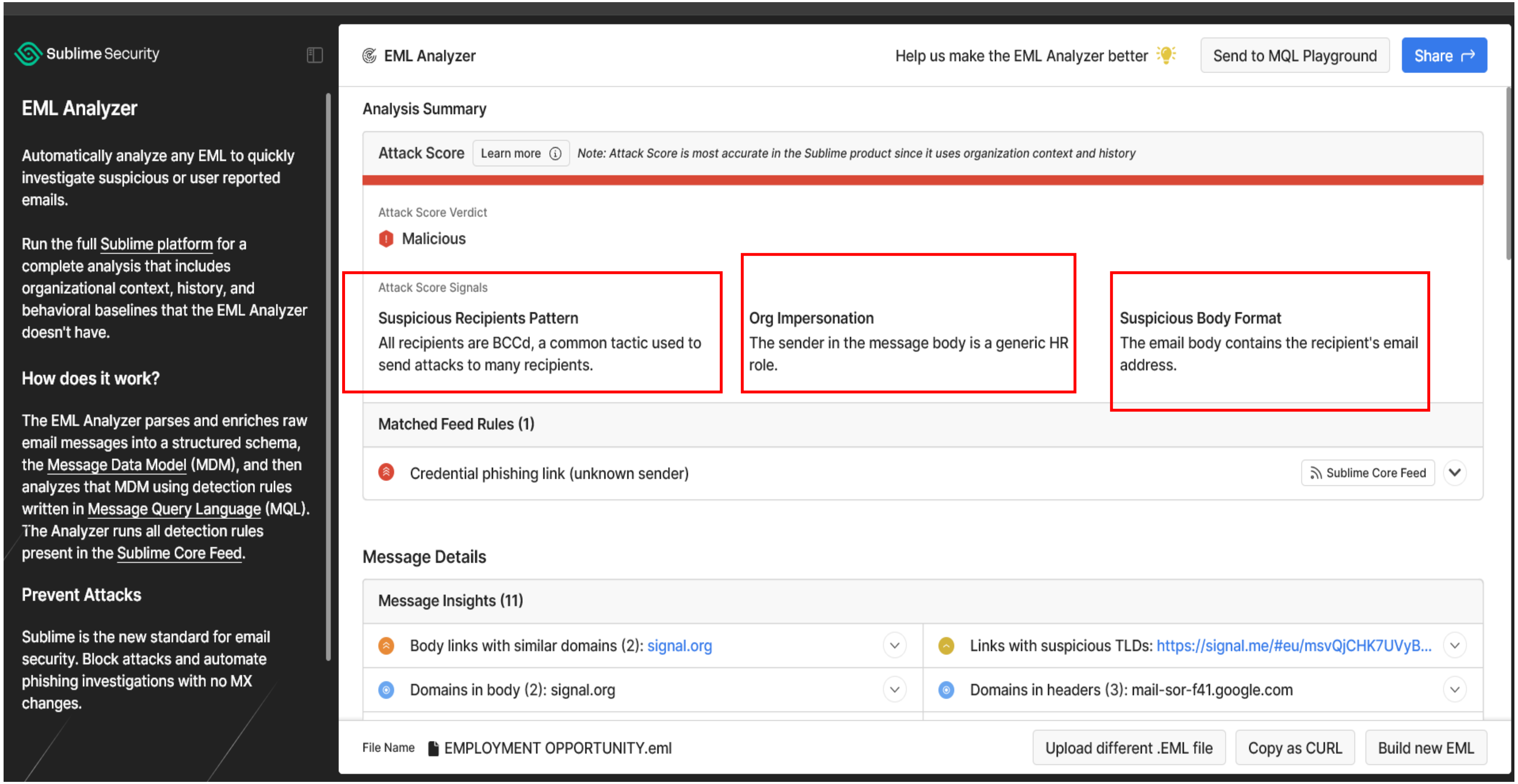
LEVERAGING EMAIL SECURITY/FILTERING TOOLS

I used a free automated phishing detection tool called **Sublime Security** to analyze the email.

The tool immediately flagged multiple anomalies including:

- Sender impersonation
- Header inconsistencies
- Domain reputation issues
- Suspicious message patterns

The results aligned with my manual analysis and confirmed that the email was malicious. The screenshots below show how the tool automatically detected these indicators.



EML Analyzer

Automatically analyze any EML to quickly investigate suspicious or user reported emails.

Run the full Sublime platform for a complete analysis that includes organizational context, history, and behavioral baselines that the EML Analyzer doesn't have.

How does it work?

The EML Analyzer parses and enriches raw email messages into a structured schema, the Message Data Model (MDM), and then analyzes that MDM using detection rules written in Message Query Language (MQL). The Analyzer runs all detection rules present in the Sublime Core Feed.

Prevent Attacks

Sublime is the new standard for email security. Block attacks and automate phishing investigations with no MX changes.

Analysis Summary

Attack Score Learn more *Note: Attack Score is most accurate in the Sublime product since it uses organization context and history*

Attack Score Verdict

Malicious

Attack Score Signals

Suspicious Recipients Pattern
All recipients are BCCd, a common tactic used to send attacks to many recipients.

Org Impersonation
The sender in the message body is a generic HR role.

Suspicious Body Format
The email body contains the recipient's email address.

Matched Feed Rules (1)

Credential phishing link (unknown sender) — Sublime Core Feed

Message Details

Message Insights (11)

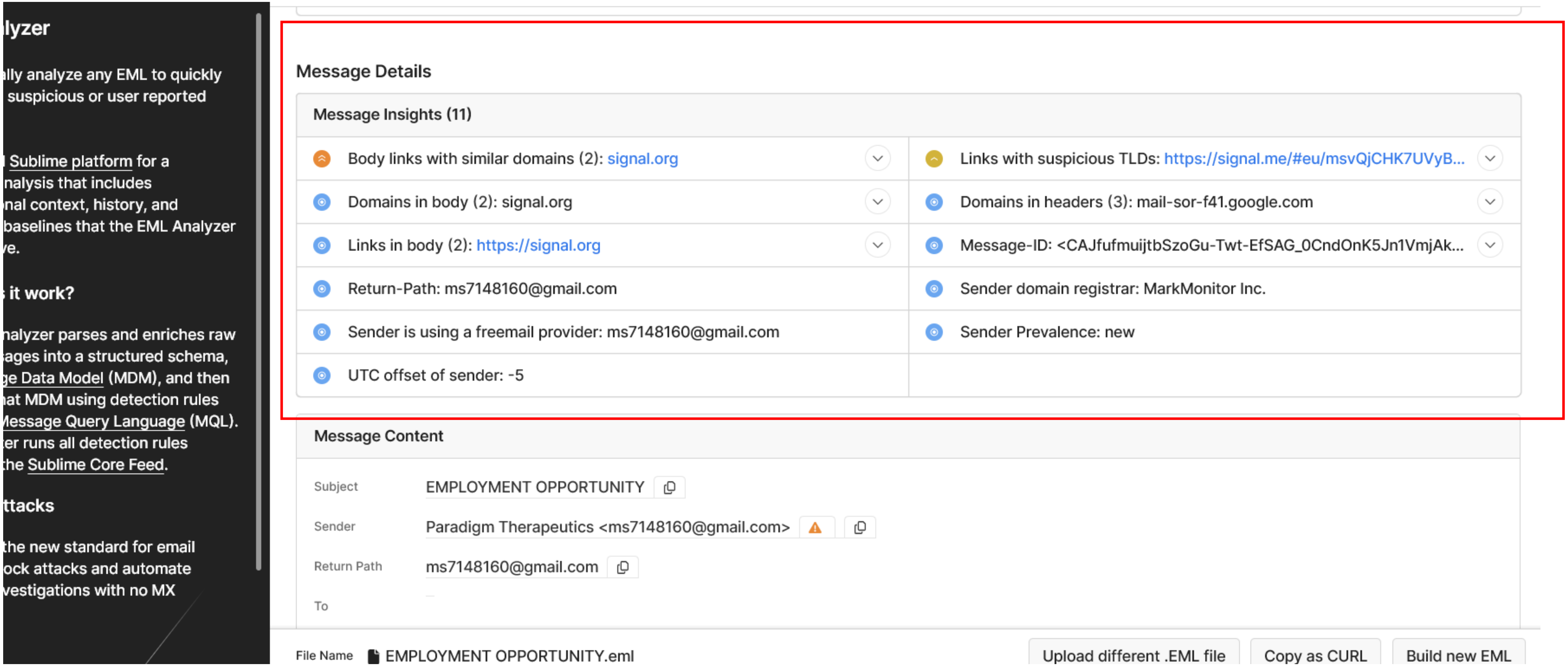
Body links with similar domains (2): signal.org

Links with suspicious TLDs: https://signal.me/#eu/msvQjCHK7UVyB...

Domains in body (2): signal.org

Domains in headers (3): mail-sor-f41.google.com

File Name EMPLOYMENT OPPORTUNITY.eml



lyzer

lly analyze any EML to quickly suspicious or user reported

l Sublime platform for a nalysis that includes nal context, history, and baselines that the EML Analyzer e.

it work?

nalyzer parses and enriches raw ages into a structured schema, ge Data Model (MDM), and then at MDM using detection rules Message Query Language (MQL). er runs all detection rules he Sublime Core Feed.

ttacks

the new standard for email ock attacks and automate vestigations with no MX

Message Details

Message Insights (11)

Body links with similar domains (2): signal.org	Links with suspicious TLDs: https://signal.me/#eu/msvQjCHK7UVyB...
Domains in body (2): signal.org	Domains in headers (3): mail-sor-f41.google.com
Links in body (2): https://signal.org	Message-ID: <CAJfufmuijtbSzoGu-Twt-EfSAG_0CndOnK5Jn1VmjAk...
Return-Path: ms7148160@gmail.com	Sender domain registrar: MarkMonitor Inc.
Sender is using a freemail provider: ms7148160@gmail.com	Sender Prevalence: new
UTC offset of sender: -5	

Message Content

Subject EMPLOYMENT OPPORTUNITY

Sender Paradigm Therapeutics <ms7148160@gmail.com> ⚠

Return Path ms7148160@gmail.com

To

File Name EMPLOYMENT OPPORTUNITY.eml

REMEDIATION STRATEGIES

Since this incident involved my personal email account, the immediate actions I took included:

- Blocking the sender
- Reporting the message as phishing/spam
- Reviewing and tightening security settings

If this incident had occurred within an organization, the recommended actions would include:

1. Isolate the affected account(s) — force logout and revoke active sessions.
2. Reset credentials and enable MFA for compromised accounts.
3. Block malicious domains/IPs at the gateway and in web filters.
4. Quarantine or delete similar emails across mailboxes (search by Message-ID / subject / sender).
5. Scan affected endpoints for malware and indicators of compromise.

Follow-up actions:

- Notify stakeholders and legal/compliance if PII was exposed.
- Update blocklists and filtering rules.
- Run a company-wide password reset if multiple accounts compromised.
- Deliver a targeted awareness message to users about the specific phishing technique used.

CONCLUSION

This analysis confirms that phishing attacks today are sophisticated and often designed to appear legitimate. Although the email passed SPF, DKIM, and DMARC checks, deeper investigation exposed impersonation, suspicious routing, and malicious URLs. The attacker exploited a trusted email platform to bypass filters and increase delivery success. This case emphasizes that authentication alone does not guarantee legitimacy and highlights the importance of layered security controls, user awareness, and forensic analysis. Effective defense against phishing requires a combination of human vigilance, technical verification, and automated detection tools.