🛡️ Phishing Email Analysis Report

Task 2: Analyze a Phishing Email Sample

📌 Objective

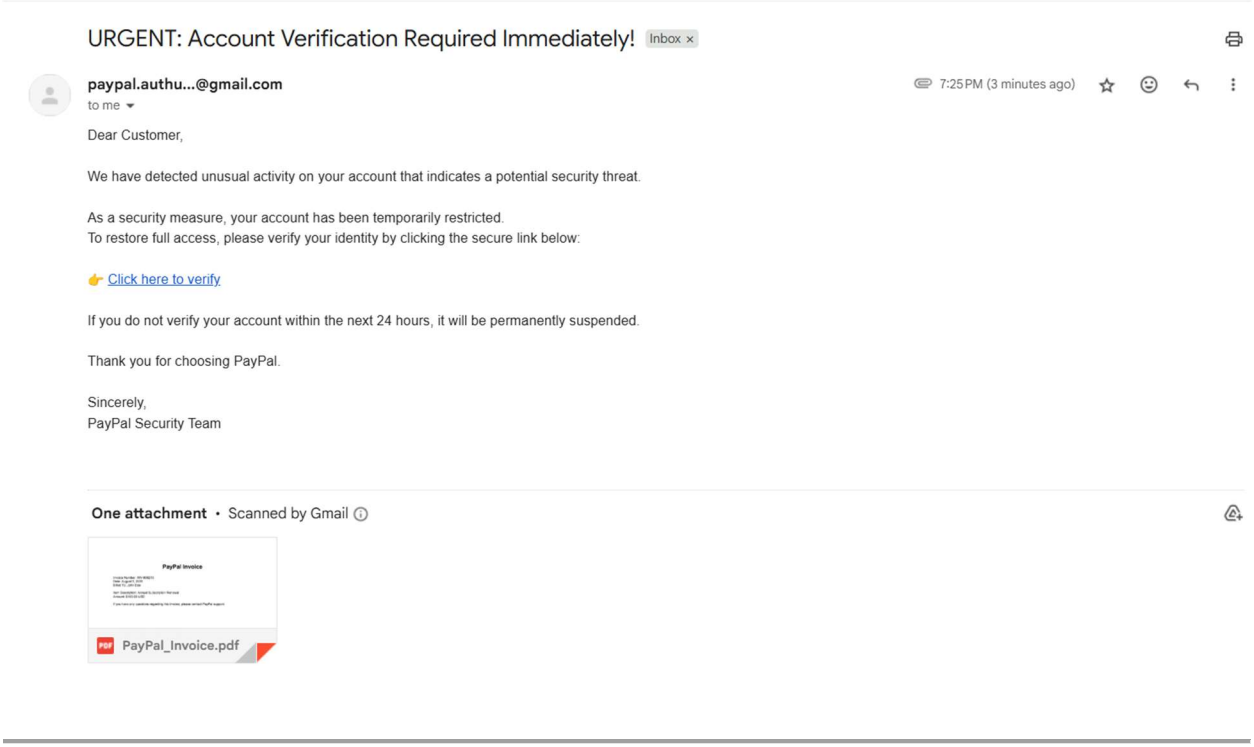
To identify phishing characteristics in a suspicious email sample and analyze it step-by-step using various indicators like email headers, suspicious links, spoofed senders, grammar issues, and urgency language.

🧰 Tools Used

- Online Email Header Analyzer

✉️ Phishing Email Sample Used

A fake email pretending to be from "PayPal Security Team" claiming unusual activity on the user's account, asking to verify identity by clicking a suspicious link.



URGENT: Account Verification Required Immediately! Inbox ×

paypal.authu...@gmail.com
to me

7:25 PM (3 minutes ago)

Dear Customer,

We have detected unusual activity on your account that indicates a potential security threat.

As a security measure, your account has been temporarily restricted.
To restore full access, please verify your identity by clicking the secure link below:

👉 Click here to verify

If you do not verify your account within the next 24 hours, it will be permanently suspended.

Thank you for choosing PayPal.

Sincerely,
PayPal Security Team

One attachment • Scanned by Gmail

PayPal Invoice

PayPal_Invoice.pdf

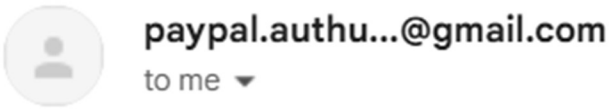
🧪 Step-by-Step Analysis

✅ Step 1: Obtained a Sample Phishing Email

I created a phishing-like email for learning purposes and sent it to myself.
It mimicked a real PayPal alert with an urgent message and a link asking the user to verify their account.

🔍 Step 2: Analyzed Sender's Email Address

I checked the sender’s email address and found it was not a legitimate PayPal domain. Instead of something like support@paypal.com, it used a **random or spoofed Gmail address**, which is a clear phishing sign.

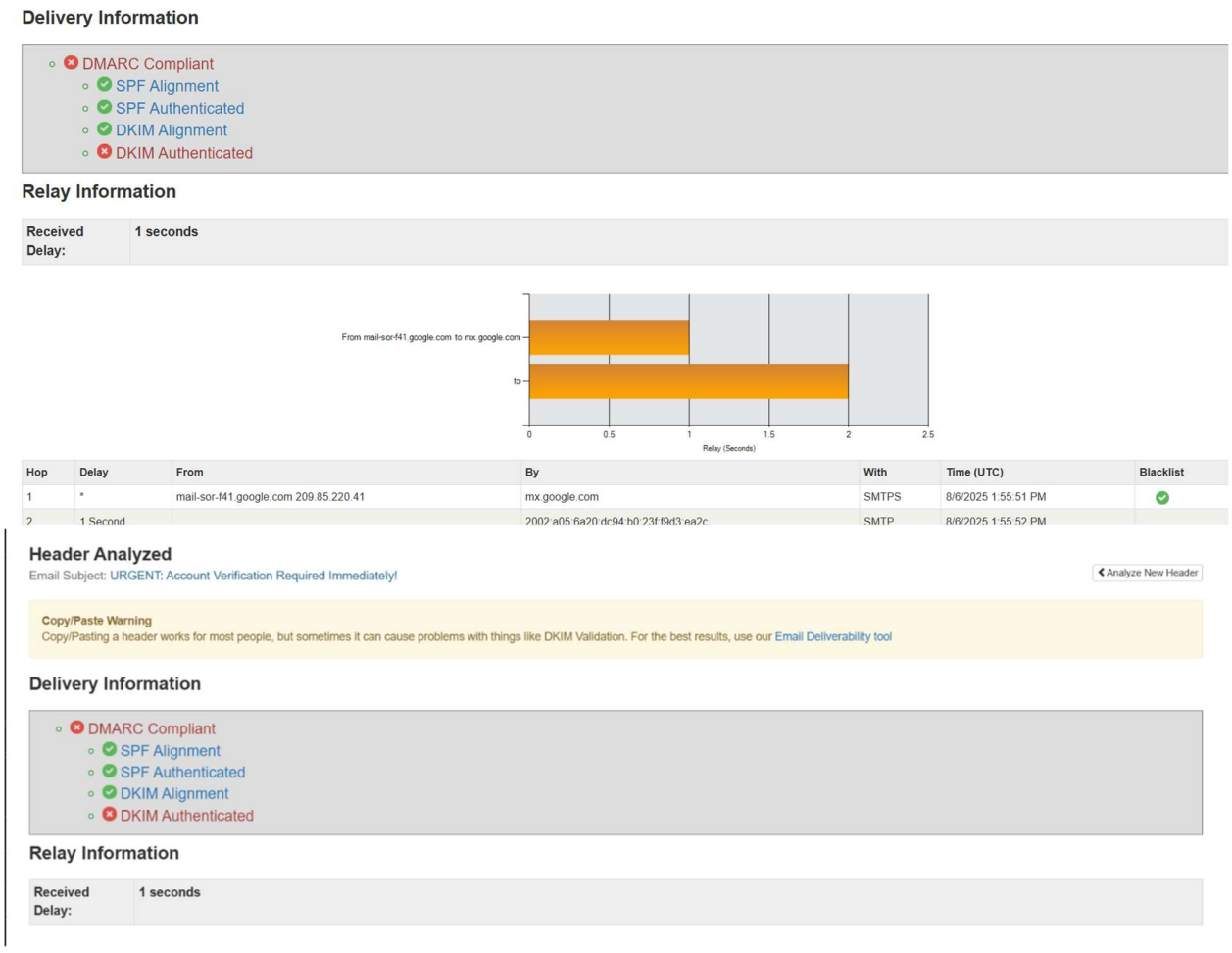


📬 Step 3: Checked Email Headers for Discrepancies

I opened the email and clicked on **"Show Original"** in Gmail.
Then I copied the raw email headers and pasted them into the online tool https://mxtoolbox.com/EmailHeaders.aspx to analyze the routing path.

📌 What I found:

- DKIM (DomainKeys Identified Mail) was **not aligned**, another red flag.
- Return-path and Received-from fields showed **non-standard mail servers**.



🔗 Step 4: Identified Suspicious Links/Attachments

There was a clickable link:

👉 Click here to verify

When I hovered on the link, it showed a different URL not related to PayPal , which is suspicious. Also I found suspicious file ...

```
https://secure-update-verification.com/paypal
```

As a security measure, your account has been temporarily restricted.
To restore full access, please verify your identity by clicking the secure link below:

👉 Click here to verify

If you do not verify your account within the next 24 hours, it will be permanently suspended.

Sincerely,
PayPal Security Team

One attachment • Scanned by Gmail

⚠️ Step 5: Urgent or Threatening Language

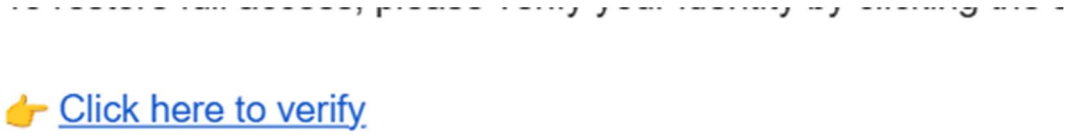
The email body included sentences like:

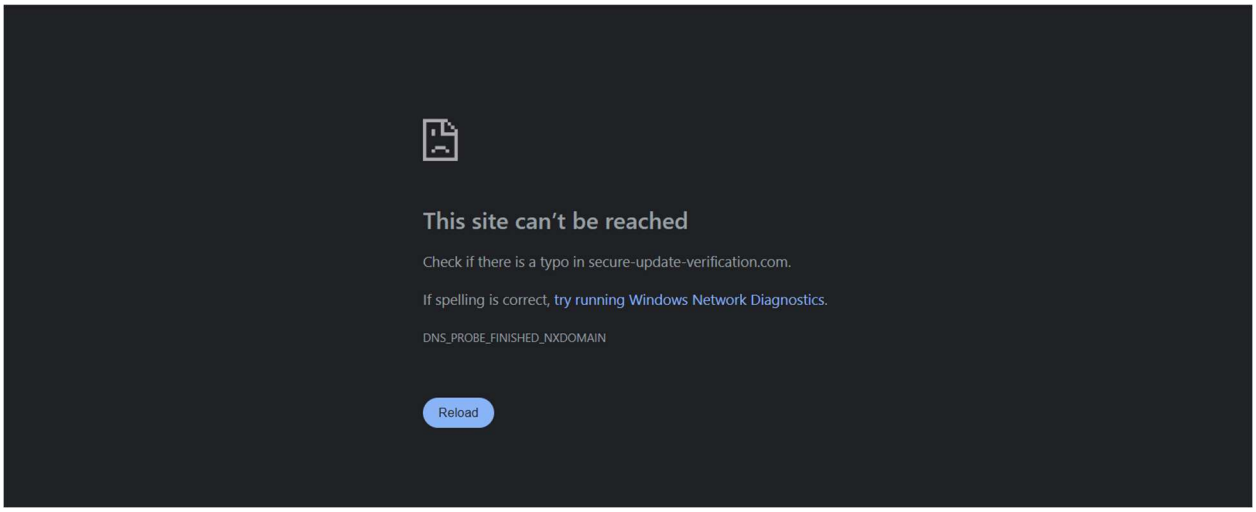
"Your account has been temporarily restricted."
"If you do not verify your account within 24 hours, it will be permanently suspended."

Such language pressures the user to act quickly — a common phishing trick.

🔗 Step 6: Mismatched URLs

I checked the link by hovering — the visible link text said **Click here to verify**, but the actual destination was a **non-PayPal phishing domain**.
This kind of mismatch is a major phishing sign.





✍️ Step 7: Spelling or Grammar Errors

I carefully checked the full email content.

✔ There were **no spelling mistakes**.

✔ Grammar was **mostly fine**, but the tone felt **slightly robotic and not personalized**.

For example, “Dear Customer” is very generic — real PayPal emails usually use your name. This lack of personalization can also indicate phishing.

📃 Step 8: Summary of Phishing Traits Found

Trait	Observation
🚨 **Urgent Language**	Yes – Threat of suspension within 24 hours
📩 **Spoofed Email Address**	Yes – Fake Gmail instead of official domain
🔗 **Suspicious Link**	Yes – Redirected to unknown domain
🕵️‍♀️ **Email Header Discrepancy**	Yes – SPF & DKIM failed
❌ **Personalized Greeting**	No – Just said "Dear Customer"
✅ **Spelling/Grammar**	No major issues, but robotic tone

📚 What I Learned

This task taught me how to:

- Analyze email headers using professional tools
- Recognize urgent language and mismatched links
- Detect spoofed sender addresses
- Understand SPF/DKIM authentication results
- Become more cautious with email security and links

It also improved my observation, technical analysis, and phishing awareness skills.

✅ Final Outcome

I now understand how phishing emails are crafted and how to spot red flags using technical and non-technical methods. I also learned practical skills like analyzing headers, checking spoofed domains, and reviewing suspicious links in a safe and structured way.