📧 Task 2: Phishing Email Analysis (Simplified Report)

🎯 Objective

In this task, I reviewed a suspicious email to find signs of phishing. The goal was to learn how fake emails try to trick people and how to spot the warning signs.

□ Tools I Used

- A sample phishing email (included below)
- MXToolbox Email Header Analyzer
- A basic text editor to view the email

✉ Phishing Email Sample (Fake Email for Practice)

```
sql
CopyEdit
From: PayPal Security <support@paypa1-security-check.com>
To: youremail@example.com
Subject: Urgent: Your PayPal Account Will Be Suspended!
Date: 6 Aug 2025

Dear Customer,

We have detected suspicious activity on your PayPal account and need you to
verify your identity immediately. If you do not act within 24 hours, your
account will be permanently suspended.

Click the link below to confirm your details:
☞ https://paypal.com.secure-update.verify-portal.login-id873.com

You can also open the attached file "Account_Notice.pdf" to verify manually.

If you don't respond, your account may be closed.

Thank you,
PayPal Security Team
```

🔍 What I Did (Step-by-Step)

✅ 1. Checked the Sender’s Email

The email said it was from PayPal, but the address was:

```
pgsql
CopyEdit
support@paypa1-security-check.com
```

● **Warning Sign**: The domain name is fake — it uses “paypa1” (with a number) instead of “paypal”.

✅ 2. Analyzed the Email Headers

I used an online header analyzer to check where the email really came from.

● **Warning Sign**: The message was sent from a random server — not from PayPal.

✅ 3. Checked the Link

The email had a link that looked like it would go to PayPal, but when I hovered over it, the real link was:

```
pgsql
CopyEdit
https://paypal.com.secure-update.verify-portal.login-id873.com
```

● **Warning Sign**: The link is fake. It tries to look like PayPal but it’s a trick.

✅ 4. Looked at the Language

The message tried to scare the reader by saying:

"Your account will be suspended in 24 hours."

● **Warning Sign**: Phishing emails often try to create panic so people act without thinking.

✓ 5. Spelling and Grammar

The email didn’t have big grammar mistakes, but the way it was written felt off — like it wasn’t written by a professional.

□ **Small Clue**: Sometimes phishing emails have poor grammar or weird phrasing.

✓ 6. Attachment Mentioned

It said to open a file called:

```
CopyEdit
Account_Notice.pdf
```

In real phishing emails, such files are often harmful.

● **Warning Sign**: Unexpected attachments are risky and could contain malware.