Intern Name: S. Sai Amrutha
Mail: 240160226211.sunkavalli@gdgu.org

Task 2 – Analyze Phishing Email Sample

Tools used: EML Analyzer, ChatGPT.

INTRODUCTION:

Email is one of the most widely used communication tools, but it is also a common vector for cyberattacks. Among these, phishing emails are one of the most frequent and dangerous threats. Phishing attempts aim to trick recipients into revealing sensitive information such as usernames, passwords, or financial details by impersonating trusted organizations.

The objective of this task, *"Analyse a Phishing Email Sample"*, is to study the characteristics of a suspicious email and identify indicators of phishing. The analysis involves examining email headers for spoofing, checking the body content for suspicious links, grammatical errors, or threatening language, and utilizing online tools to validate the findings.

PHISHING:

Phishing is a type of cybercrime and social engineering attack where criminals impersonate a legitimate person or entity to trick victims into revealing sensitive information, such as passwords, bank details, or credit card numbers. Attackers use fraudulent communications through email, text messages, or fake websites to manipulate victims into revealing personal data, installing malware, or making financial payments.

Phishing often uses:

- Urgency or fear in the content
- Fake links that look similar to the real ones.
- Poor grammar and spelling mistakes.
- Imitating logos and brand names to look authentic

EMAIL SPOOFING:

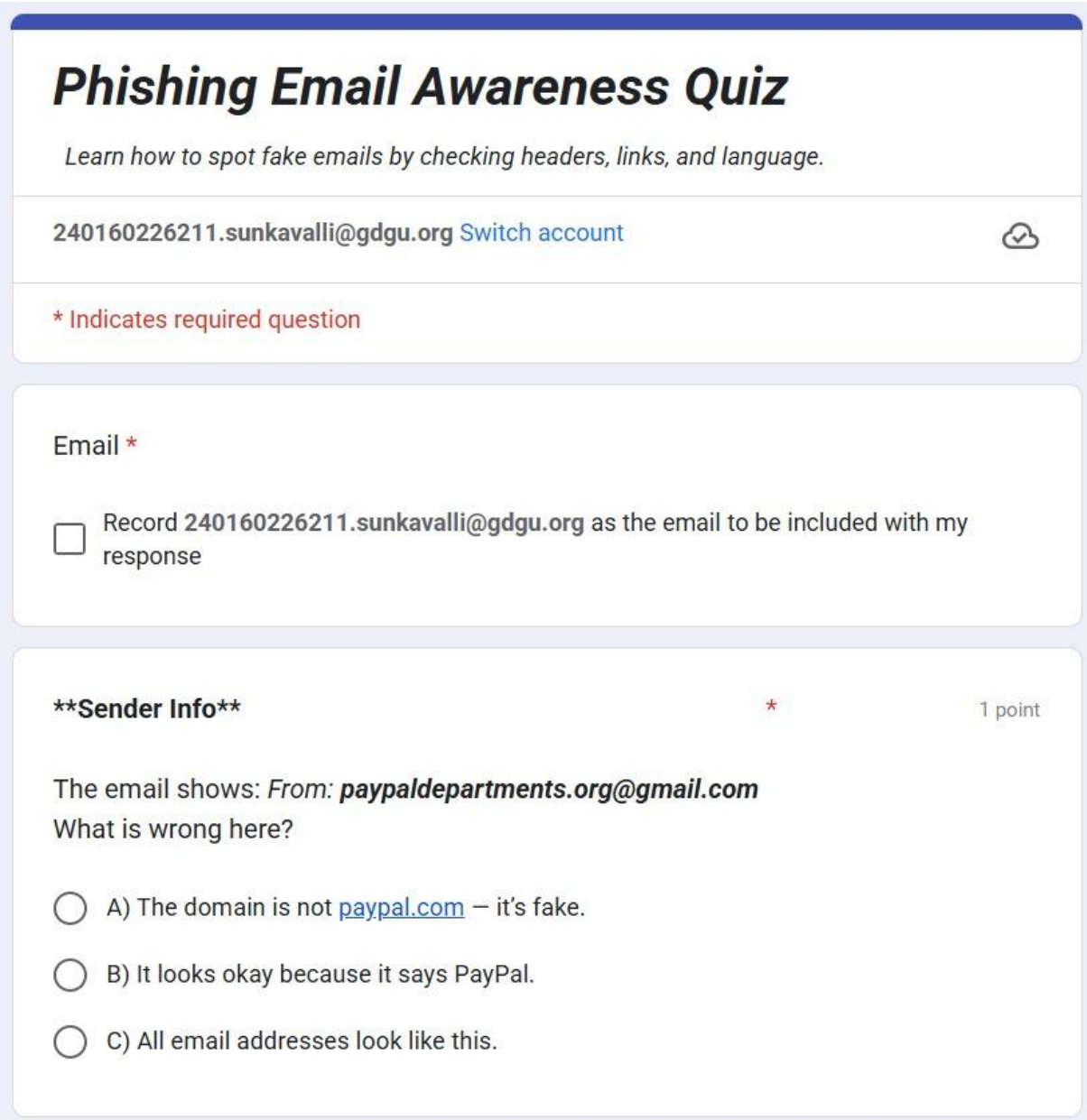
Email spoofing in cybersecurity is a malicious tactic where an attacker sends an email with a forged sender address, making it appear to come from a trusted source, to trick recipients into divulging sensitive information, downloading malware, or sending money.

Intern Name: S. Sai Amrutha
Mail: 240160226211.sunkavalli@gdgu.org

Here, I used a sample phishing email "*paypaldepartments.org@gmail.com*" which I created. In the email body, I have created a Google Form, which is an awareness quiz for people to find phishing emails.

The Google Form:
https://docs.google.com/forms/d/e/1FAIpQLSdTOsyXxQKWED__cBjfSiJQoQ06Cgbie3ZUtR4p3KGfzh0WSw/viewform?usp=header

The following pictures show the questions included in the form:



Phishing Email Awareness Quiz

Learn how to spot fake emails by checking headers, links, and language.

240160226211.sunkavalli@gdgu.org Switch account

* Indicates required question

Email *

Record 240160226211.sunkavalli@gdgu.org as the email to be included with my response

Sender Info * 1 point

The email shows: *From:* ***paypaldepartments.org@gmail.com***
What is wrong here?

A) The domain is not paypal.com – it's fake.

B) It looks okay because it says PayPal.

C) All email addresses look like this.

Intern Name: S. Sai Amrutha
Mail: 240160226211.sunkavalli@gdgu.org

****Grammar/Spelling**** * 1 point

The email says: *"**For any issueses or not opening of link, go to the form that was provide below.**"*
What makes this suspicious?

- ◯ A) It uses bad grammar and spelling mistakes
- ◯ B) PayPal sometimes makes grammar mistakes.
- ◯ C) Nothing is wrong.

****Urgency**** * 1 point

The email says: ***"Confirm within 24 hours or your account will be blocked"***
Why is this suspicious?

- ◯ A) Real companies don't use threats/pressure in emails
- ◯ B) PayPal limits accounts for fun.
- ◯ C) It is completely normal.

****Hover to see real link**** * 1 point

http://paypal-secure-verify[.]com/login

What happens when you hover to this link provided?

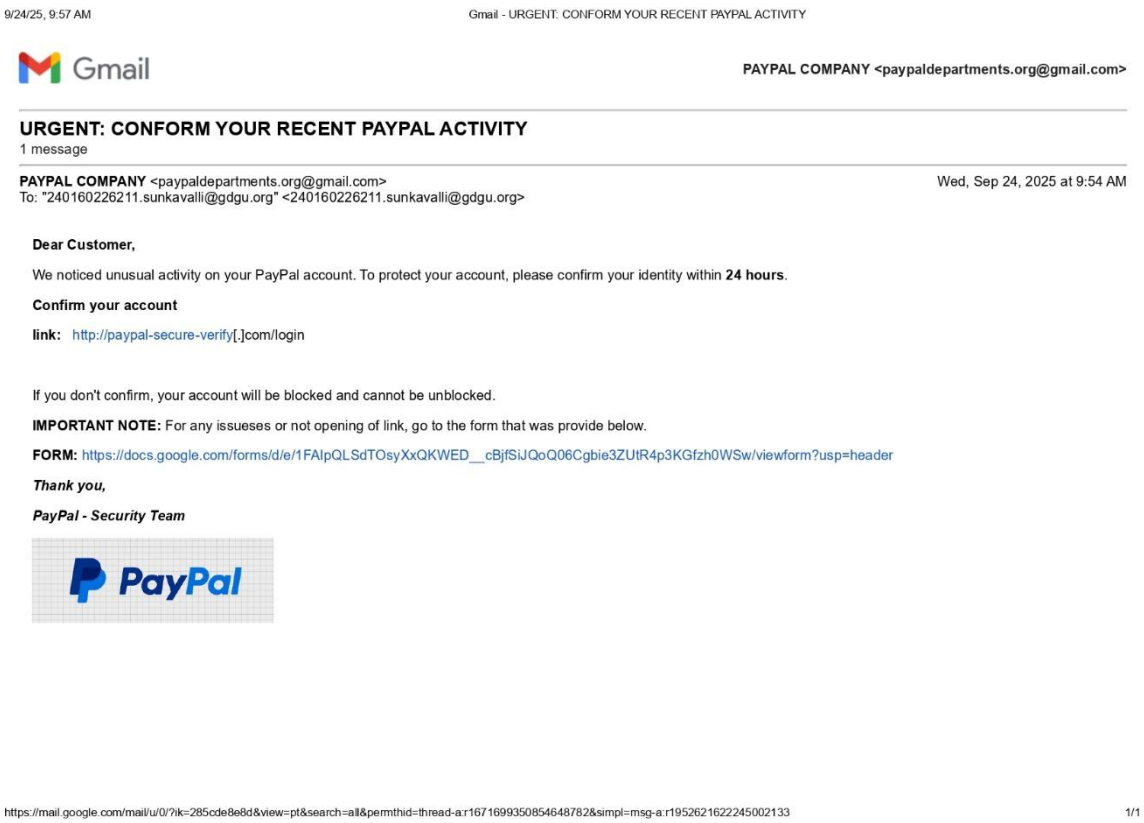
- ◯ A) The email is safe because it mentions PayPal.
- ◯ B) The real link is different from the display — this is a phishing sign.
- ◯ C) Hovering doesn't matter; all links are safe.

Submit Clear form

This form was created inside of G D Goenka University. - Contact form owner

Google Forms

Intern Name: S. Sai Amrutha
Mail: 240160226211.sunkavalli@gdgu.org



9/24/25, 9:57 AM Gmail - URGENT: CONFORM YOUR RECENT PAYPAL ACTIVITY

Gmail PAYPAL COMPANY <paypaldepartments.org@gmail.com>

URGENT: CONFORM YOUR RECENT PAYPAL ACTIVITY
1 message

PAYPAL COMPANY <paypaldepartments.org@gmail.com> Wed, Sep 24, 2025 at 9:54 AM
To: "240160226211.sunkavalli@gdgu.org" <240160226211.sunkavalli@gdgu.org>

Dear Customer,

We noticed unusual activity on your PayPal account. To protect your account, please confirm your identity within **24 hours**.

Confirm your account

link: http://paypal-secure-verify[.]com/login

If you don't confirm, your account will be blocked and cannot be unblocked.

IMPORTANT NOTE: For any issueses or not opening of link, go to the form that was provide below.

FORM: https://docs.google.com/forms/d/e/1FAIpQLSdTOsyXxQKWED__cBjfSiJQoQ06Cgbie3ZUtR4p3KGfzh0WSw/viewform?usp=header

Thank you,

PayPal - Security Team

PayPal

https://mail.google.com/mail/u/0/?ik=285cde8e8d&view=pt&search=all&permthid=thread-a:r1671699350854648782&simpl=msg-a:r1952621622245002133 1/1

HEADER ANALYSIS:

Header analysis is the process of examining the hidden header information within a digital message, most commonly an email, to understand its origin, routing path, and technical details. This analysis helps in verifying a sender's identity, tracking an email's journey, identifying spam or phishing attempts, and investigating security incidents. By using tools to parse this data, one can gain insights into the message's legitimacy and the servers it passed through.

When an email is sent, it carries two parts:

- **Header** → technical details about how and from where the email was sent.
- **Body** → the actual content/message the user reads.

WHY IS HEADER ANALYSIS IMPORTANT:

- Attackers often **spoof** (fake) the “From” address.

- The header reveals the **truth** about what servers actually handled the mail, and whether security checks passed.
- By analysing headers, we can detect **phishing** or spam emails even if the body looks real.

Original Message

Message ID	<CAP=yaJ3MFyV-dAqyGtzG1vXHFC+7DRHTqrgqyK1+FvMMnrjfoA@mail.gmail.com>
Created at:	Wed, Sep 24, 2025 at 9:54 AM (Delivered after 0 seconds)
From:	PAYPAL COMPANY <paypaldepartments.org@gmail.com>
To:	"240160226211.sunkavalli@gdgu.org" <240160226211.sunkavalli@gdgu.org>
Subject:	URGENT: CONFORM YOUR RECENT PAYPAL ACTIVITY

The above image is the Email Header

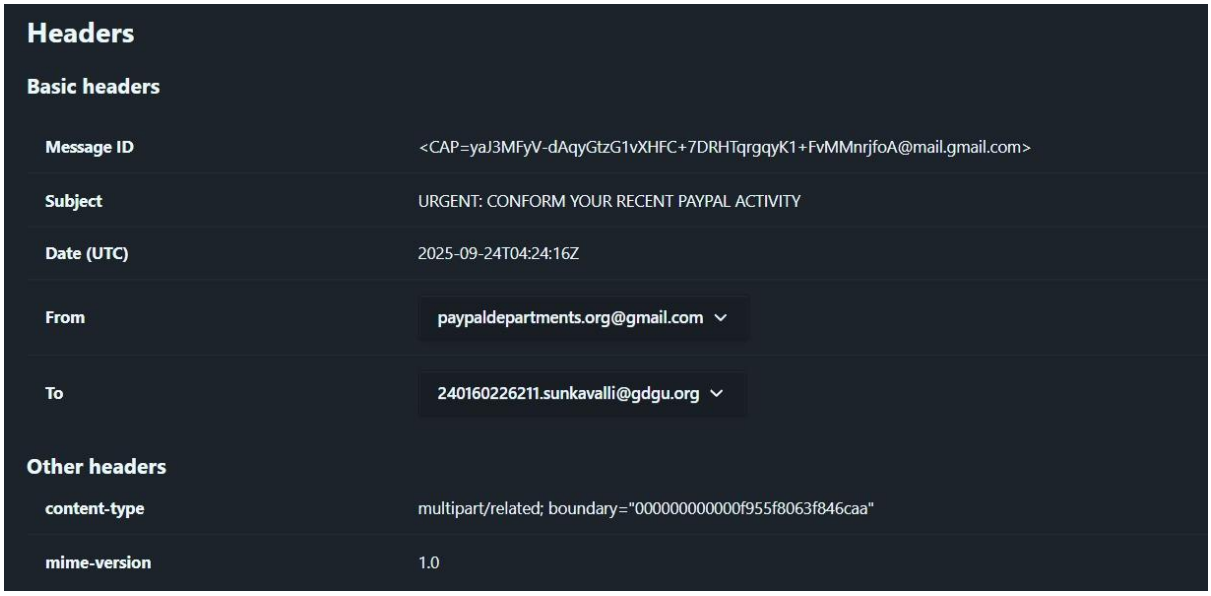
WHAT IS INSIDE AN EMAIL HEADER:

1. **From:** – Who the email *claims* to be from.
   - Example: From: PayPal <support@paypal.com>
   - Suspicious if it's actually from: paypaldepartments.org@gmail.com
2. **To:** – Recipient's address. Here, it is 240160226211.sunkavalli@gdgu.org
3. **Subject:** – The subject line. Often urgent or in ALL CAPS in phishing.
4. **Message-ID:** – A unique ID for the email. Usually matches the sending domain. Odd domains mean spoofing.
5. **Date:** – When the email was sent, i.e., Wed, Sep 24, 2025
6. **Authentication-Results**: – Shows results of security checks:
   - **SPF** (Sender Policy Framework) → did the sender's IP match the domain's allowed servers?
   - **DKIM** (DomainKeys Identified Mail) → was the email digitally signed?
   - **DMARC** → Did SPF/DKIM results align with the domain policy?

ANALYZING THE EMAIL HEADER THROUGH "EML ANALYZER":

Here, I am using EML Analyzer https://eml-analyzer.herokuapp.com/ to analyse my header file. The following content tells the complete analysis, explaining its terms and results.

Intern Name: S. Sai Amrutha
Mail: 240160226211.sunkavalli@gdgu.org



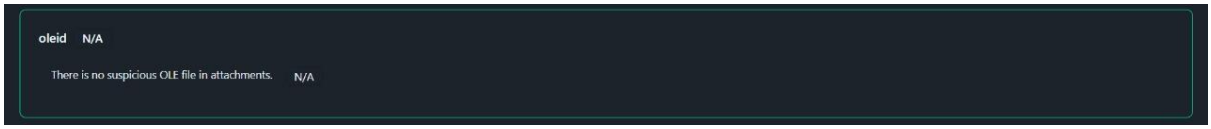
The above image screenshot is the Header from the EML Analyzer

BASIC HEADERS:

- **Message ID:** CAP=yaJ3MFyV-dAqyGtzG1vXHFC...@mail.gmail.com
  - Unique identifier assigned to the email by the sending server.
- **Subject:** URGENT: CONFIRM YOUR RECENT PAYPAL ACTIVITY
  - Suspicious because it creates a sense of urgency (common in phishing).
- **Date (UTC):** 2025-09-24T04:24:16Z
  - The exact time the email was sent.
- **From:** paypaldepartments.org@gmail.com
  - Looks suspicious — PayPal would not use a Gmail address.
- **To:** 240160226211.sunkavalli@gdgu.org
  - The intended recipient (your ID email).

OTHER HEADERS:

- **Content-Type:** multipart/related
  - Means the email contains multiple parts, possibly text + images or attachments.
- **MIME-Version:** 1.0
  - Standard email formatting version.



The above image is an OLEID analysis from EML Analyzer

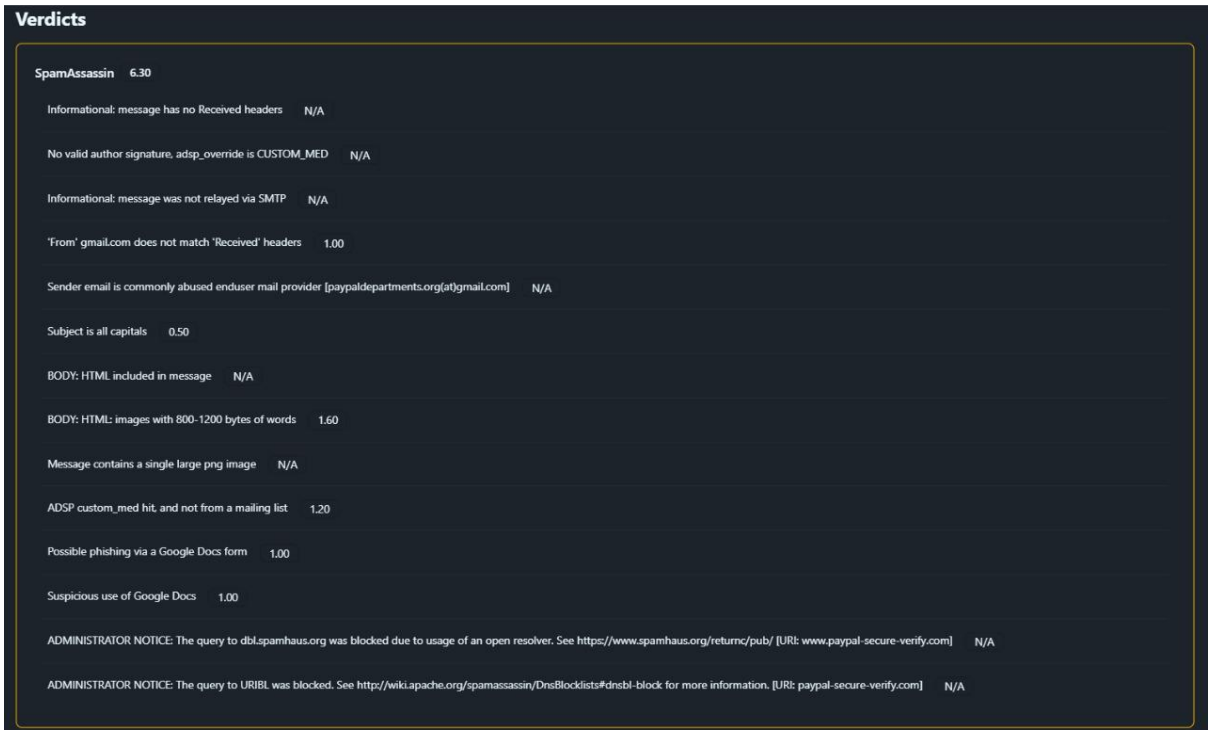
OLEID ANALYSIS:

OLEID is a script to analyse **OLE (Object Linking and Embedding) files** such as MS Office documents (e.g., Word, Excel), to detect specific characteristics usually found in malicious files.

Result: "No suspicious OLE file in attachments"

- This means there were no malicious document attachments (like Word/Excel macros).

VERDICTS (THE RESULTS MADE BY THE SPAM-DETECTION SYSTEM):



These are checks done to identify if the email is phishing or spam:

- **No Received Headers:** Suspicious — legitimate emails usually pass through multiple servers, leaving traces.
- **No valid author signature:** No DKIM/author verification.
- **Message not relayed via SMTP:** Another red flag — may be spoofed.
- **From Gmail.com does not match Received headers:** Sender is pretending to be Gmail, but headers don't align.
- **Sender email abused:** The address paypaldepartments.org@gmail.com is known to be misused.

- **Subject is all capitals:** A classic spam signal (urgent attention-grabbing).
- **Body:** HTML included: Message is HTML formatted (common in phishing).
- **Large PNG image:** Sometimes phishing mails use a big image to bypass text filters.
- **ADSP custom med hit:** Mail failed sender authentication.
- **Possible phishing via Google Docs form:** Attackers may have used fake forms to collect data.
- **Suspicious use of Google Docs:** Confirms phishing attempt.
- **Spam Haus/URIBL notice:** URL in the mail is blacklisted (paypal-secure-verify.com).

SPAM ASSASSIN (RESULTS): ***6.30***

SOCIAL ENGINEERING ELEMENTS:

Social engineering is when attackers trick people into giving away information, clicking harmful links, or doing actions that help the attacker — instead of directly hacking computers. It's basically hacking the human mind using psychology.

- **Urgency:** Subject line pushes the victim to act immediately.
- **Authority:** Pretends to be PayPal.
- **Fear:** Suggests account problems.
- **Deception:** Fake sender email and suspicious link.

SUMMARIZING PHISHING TRAITS FOUND IN THE EMAIL:

→ Mismatched sender (display name implies PayPal, but actual email is a consumer Gmail address: paypaldepartments.org@gmail.com).
→ Missing or incomplete Received header chain (suggests header forging or incomplete raw capture).
→ No valid DKIM/ADSP/author signature (authentication failed or absent).
→ Subject in all caps (attention/urgency tactic).
→ HTML body with large images or image-as-button (visual spoofing).
→ Link likely points to a non-PayPal domain (e.g., paypal-secure-verify.com) — scanner flagged possible Google Docs/form hosting.
→ Content uses urgent/threatening language ("confirm within 24 hours", "account will be blocked") — social engineering pressure.
→ Use of a free email provider to impersonate a corporate domain (commonly abused sender).
→ Scanner couldn't complete blacklist checks (admin notices)—you should independently check URIBL/Spamhaus/VirusTotal.

Intern Name: S. Sai Amrutha
Mail: 240160226211.sunkavalli@gdgu.org

CONCLUSION:

The analysis of the phishing email sample revealed several strong indicators of malicious intent, including a spoofed sender address, missing or failed authentication checks (SPF/DKIM/DMARC), urgent and threatening language, suspicious links, and grammatical errors. Header analysis showed mismatches between the claimed sender and the actual source, while body inspection highlighted the use of urgency and fake login links to pressure the user into revealing sensitive information.

This exercise demonstrated how phishing emails exploit both technical weaknesses and human psychology. By performing header analysis, inspecting links through hover checks, and reviewing the message content critically, I gained hands-on experience in identifying phishing attempts. The task has strengthened my understanding of email forensics and improved my awareness of common cyber threats, highlighting the importance of vigilance and proper reporting in cybersecurity.

****