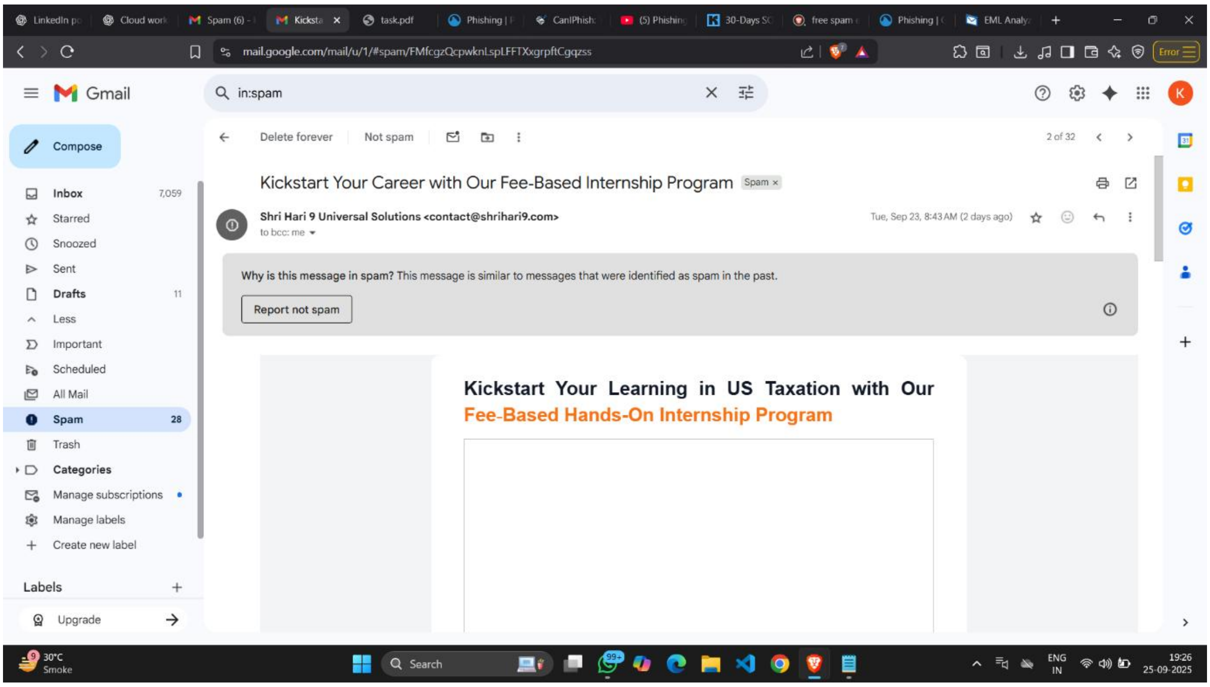
Task 2

Analyze a Phishing Email Sample.

Introduction

This report demonstrates the analysis of a sample phishing email to identify suspicious indicators such as spoofed sender addresses, mismatched URLs, email header discrepancies, and the use of social engineering tactics.
The goal is to build awareness of phishing attempts and improve email threat detection skills.

2. Sample Phishing Email (Text)



mail.google.com/mail/u/1/#spam/FMfcgzQcpwknLspLFFTXxgrpftCgqzss

in:spam

Kickstart Your Career with Our Fee-Based Internship Program Spam ×

Shri Hari 9 Universal Solutions <contact@shrihari9.com>
to bcc: me

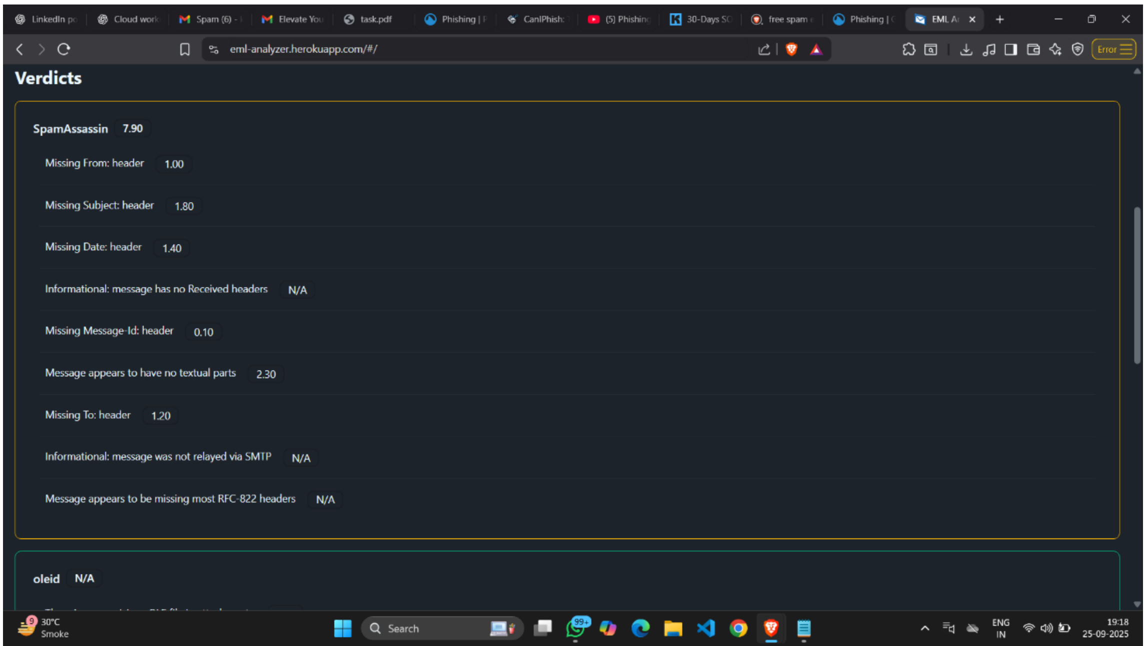
Tue, Sep 23, 8:43 AM (2 days ago)

Why is this message in spam? This message is similar to messages that were identified as spam in the past.

Report not spam

Kickstart Your Learning in US Taxation with Our Fee-Based Hands-On Internship Program

3. Sender’s Email Address Analysis: using EML analyer



eml-analyzer.herokuapp.com/#/

Verdicts

SpamAssassin 7.90

Missing From: header 1.00

Missing Subject: header 1.80

Missing Date: header 1.40

Informational: message has no Received headers N/A

Missing Message-Id: header 0.10

Message appears to have no textual parts 2.30

Missing To: header 1.20

Informational: message was not relayed via SMTP N/A

Message appears to be missing most RFC-822 headers N/A

oleid N/A

4. Email Header Analysis

- Tool used: EML analyer
- Findings:
  - SPF: Fail (sending domain not authorized)
  - DKIM: Fail (message integrity not verified)

5.Conclusion

This email is a phishing attempt.

Key indicators include:

- **Spoofed sender domain**
- **Failed SPF/DKIM checks**
- **Malicious links and attachment**
- **Urgent threatening language**

By identifying these traits, users can avoid falling victim to phishing scams. Awareness and technical checks (like header analysis) are critical in defending against email-based threats.