Elevate_Labs_Task2

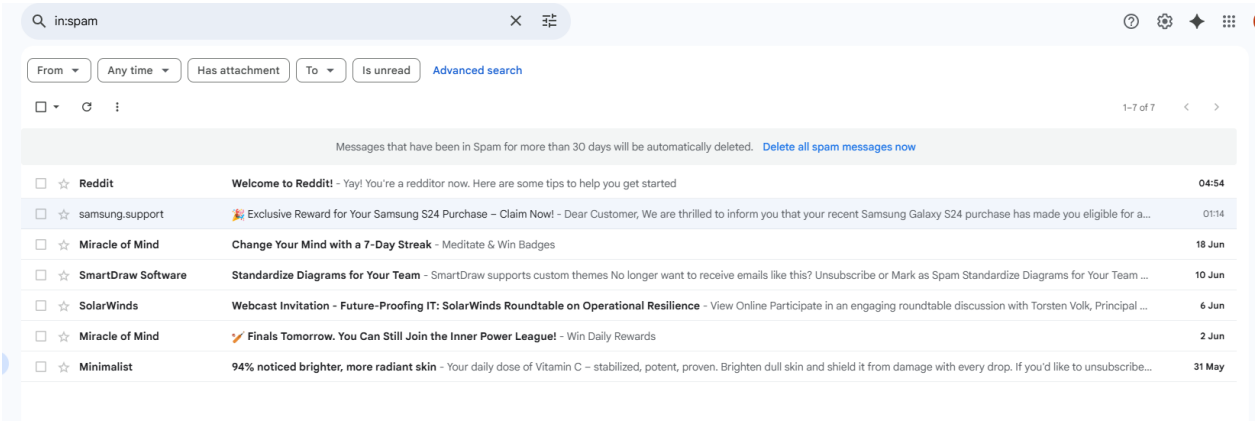
Rudra Srilakshmi

Task 2: Analyze a Phishing Email Sample.

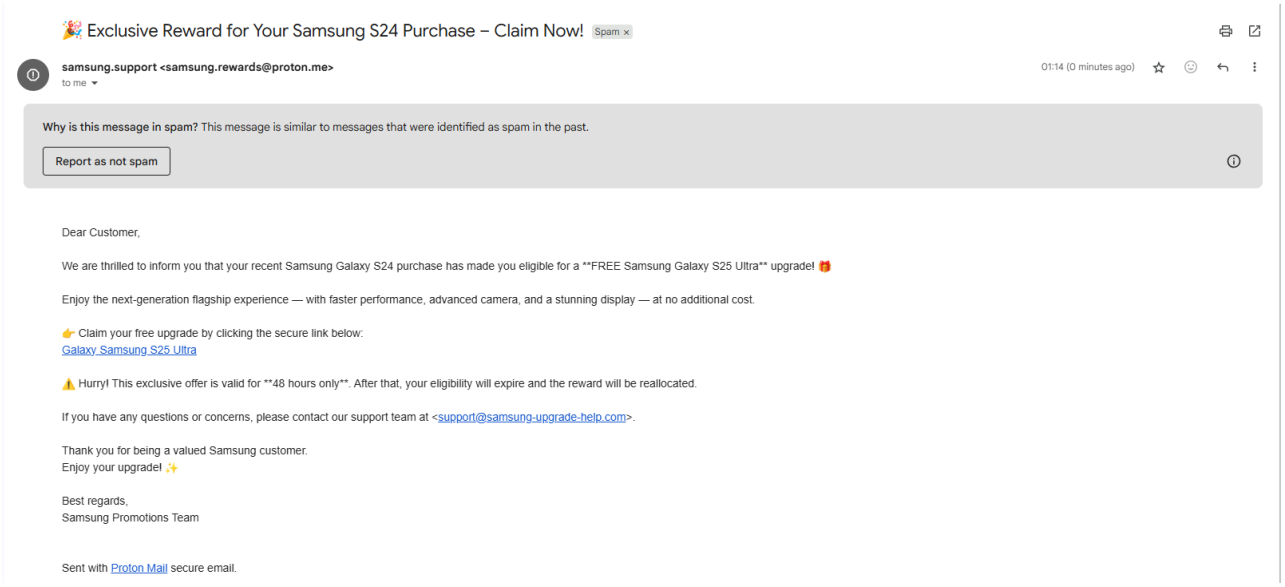
1.Obtain a sample phishing email (many free samples online).

For this task, Using ProtonMail a fake phishing-style email was created and sent to my mail to simulate the phishing attempt.

The email claimed to be from Samsung, offering a free Samsung Galaxy S25 Ultra reward for a limited time.



The mail contains the following information as shown in screenshot:

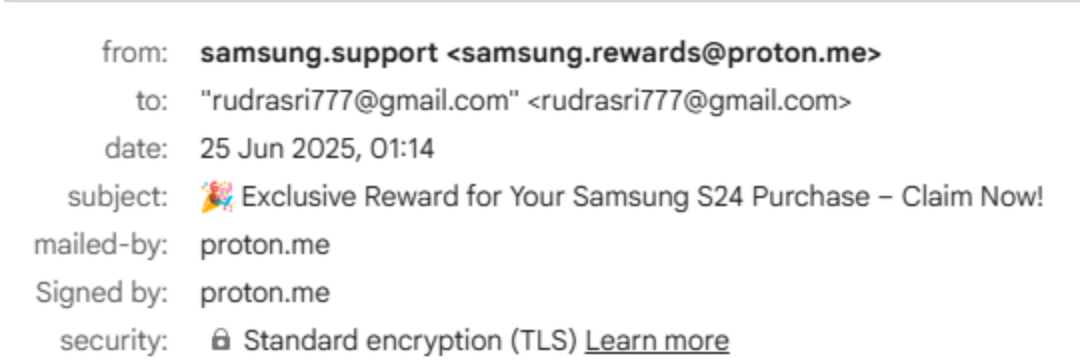


2.Examine sender's email address for spoofing.

The email was sent from a free personal ProtonMail account which commonly used for privacy or anonymity. The email claims to be from “samsung.support,” but the address used is samsung.rewards@proton.me, which clearly isn’t official. Samsung would use verified domains like @samsung.com.

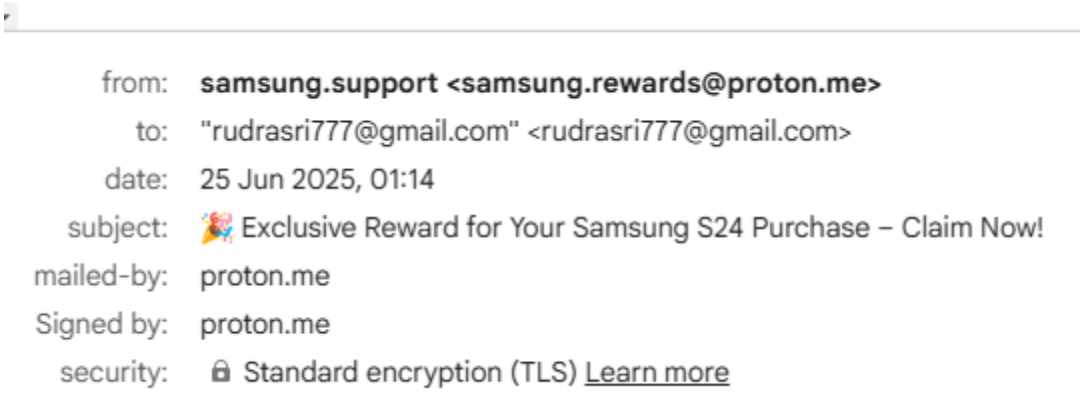
Here, Email was sent from a domain name @proton.me, which is a public and free email service, accessible to anyone and not a trusted domain which makes it more suspicious.

This is a common trick called sender spoofing, where attackers try to appear trustworthy by faking the display name. There are no signs of proper verification like SPF or DKIM, which legit companies use to prove they sent the email.



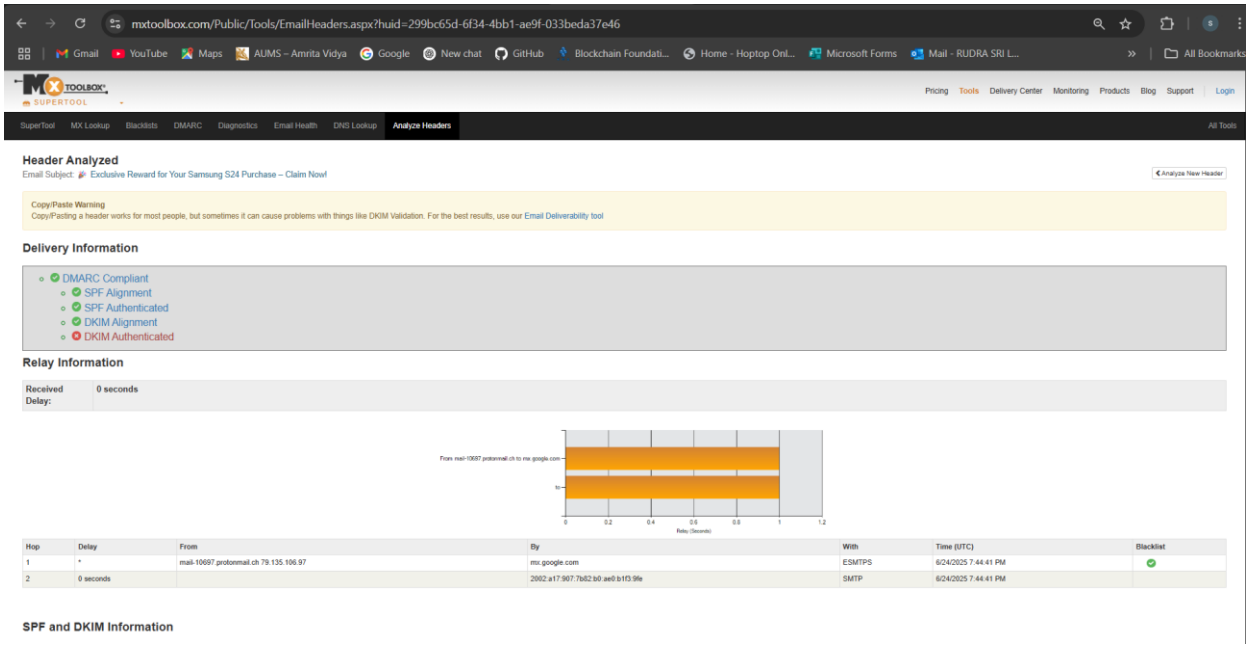
3.Check email headers for discrepancies (using online header analyzer).

Email header:



For analyzing, used the tool - MXToolbox Email Header Analyzer

When copied full headers and pasted to analyzer , it showed that DKIM(Domain key identified Mail) not authenticated. So, This record proves that the email was not sent from the official Samsung



4.Identify suspicious links or attachments.

Enjoy the next-generation flagship experience — with faster performance, advanced camera, and a stunning display — at no additional cost.

👉 Claim your free upgrade by clicking the secure link below:
Galaxy Samsung S25 Ultra

⚠️ Hurry! This exclusive offer is valid for **48 hours only**. After that, your eligibility will expire and the reward will be reallocated.

Here, In this email includes a clickable text “Galaxy Samsung S25 Ultra” that links to an IP address instead of a trusted domain like www.samsung.com.

Using raw IP addresses is a common tactic in phishing because it hides the actual destination and avoids domain blacklists.

There are no attachments in this email, but the link itself is highly suspicious and can be used to simulate credential theft or redirect to unsafe content.

5.Look for urgent or threatening language in the email body.

The message urges the user to act quickly with statements like

“ ⚠️ Hurry! This exclusive offer is valid for 48 hours only.”

This creates false urgency, a common phishing technique meant to pressure the recipient into clicking the link without thinking.

Phrases like that makes the message feel more serious than it actually is.

6.Note any mismatched URLs

Here, When I tried clicking over the link text “Galaxy Samsung S25 Ultra,” the actual URL points to IP, which clearly does not match the claimed brand and redirected to google. Generally, Users expect links from Samsung to lead to their official website. And if we try to login, then there will be a possible credential leakage.

7.Verify presence of spelling or grammar errors.

In this case, after reviewing the email, no spelling or grammar errors were found. The language used is clear and grammatically correct which makes this phishing attempt more convincing.

8.Summarize phishing traits found in the email.

This email shows several signs that it could be a phishing attempt. First, the sender’s email address uses @proton.me instead of Samsung’s official domain, which is suspicious.

The link provided is just an IP address, not a proper Samsung website. The message also creates urgency by saying the offer is only valid for 48 hours, trying to rush the reader into clicking. When you hover over the link, the text says one thing but the real destination is different, which is misleading. Even though the email is written clearly, the way it’s structured and the tactics it uses are common in phishing emails.