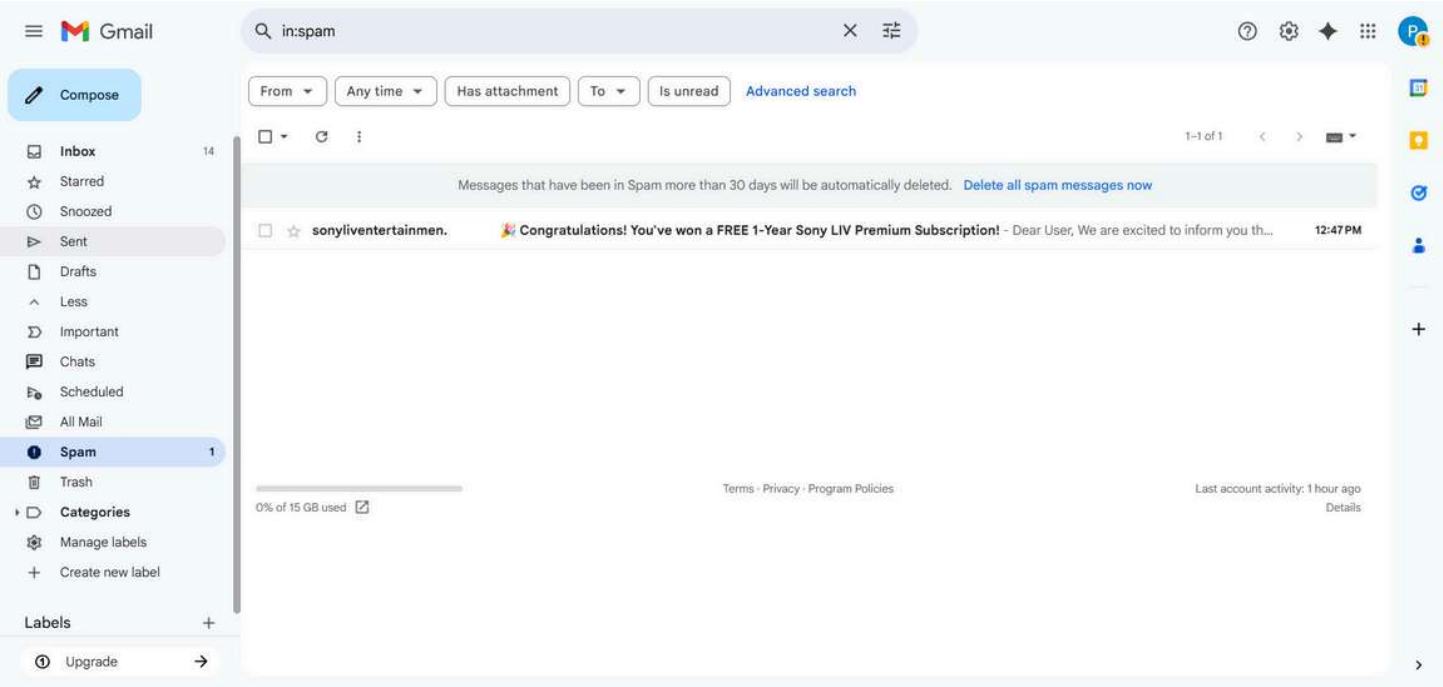
ELEVATE LABS CYBERSECURITY INTERNSHIP

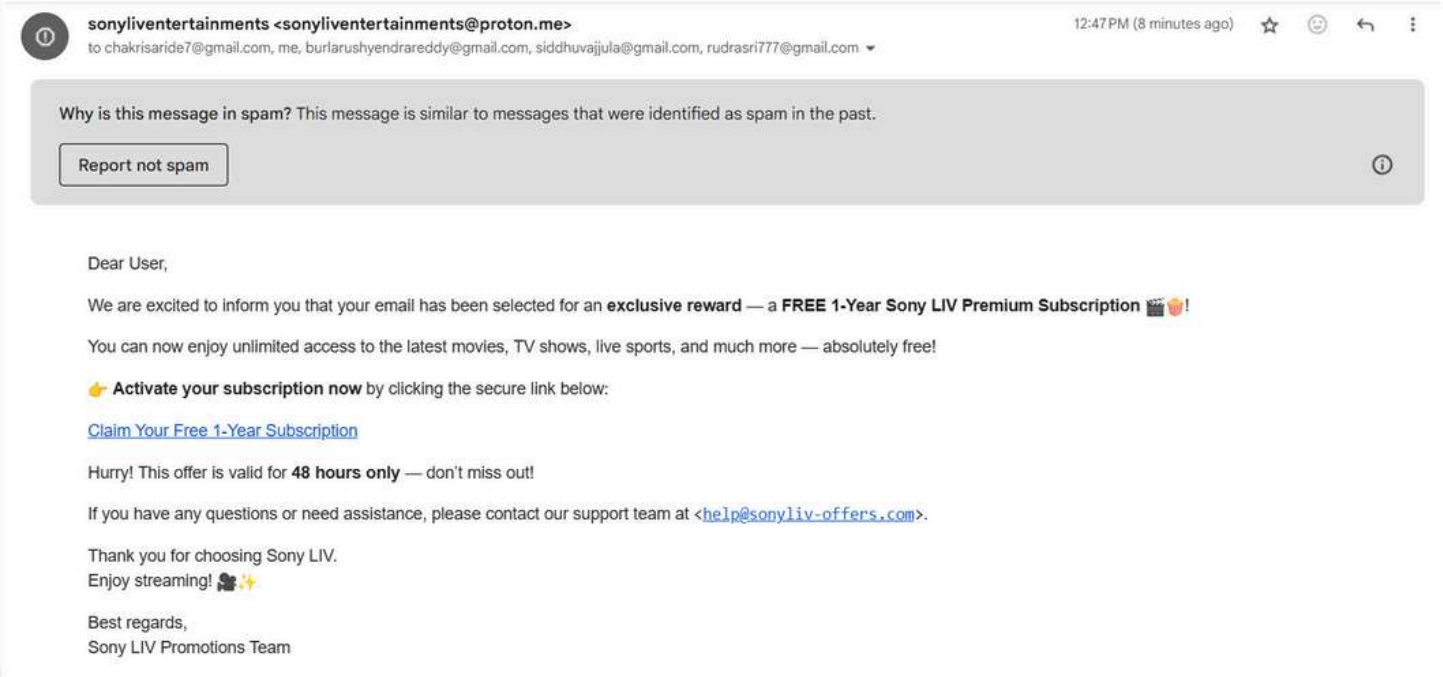
TASK-2

1)

Initially i checked my inbox for any phishing mails that exist i have not found any so me and my friends created create a spam mail named sonyliventertainments made it look like a spam mail stating that user got a free subscription of sonyliv for a year with a link that’s leading to some other website



This is how the mail looks



sonyliventertainments <sonyliventertainments@proton.me> 12:47 PM (8 minutes ago)

to chakrisaride7@gmail.com, me, burlarushyendrareddy@gmail.com, siddhuvajjula@gmail.com, rudrasri777@gmail.com

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

Report not spam

Dear User,

We are excited to inform you that your email has been selected for an **exclusive reward** — a **FREE 1-Year Sony LIV Premium Subscription** 🎬🍿!

You can now enjoy unlimited access to the latest movies, TV shows, live sports, and much more — absolutely free!

👉 **Activate your subscription now** by clicking the secure link below:

Claim Your Free 1-Year Subscription

Hurry! This offer is valid for **48 hours only** — don't miss out!

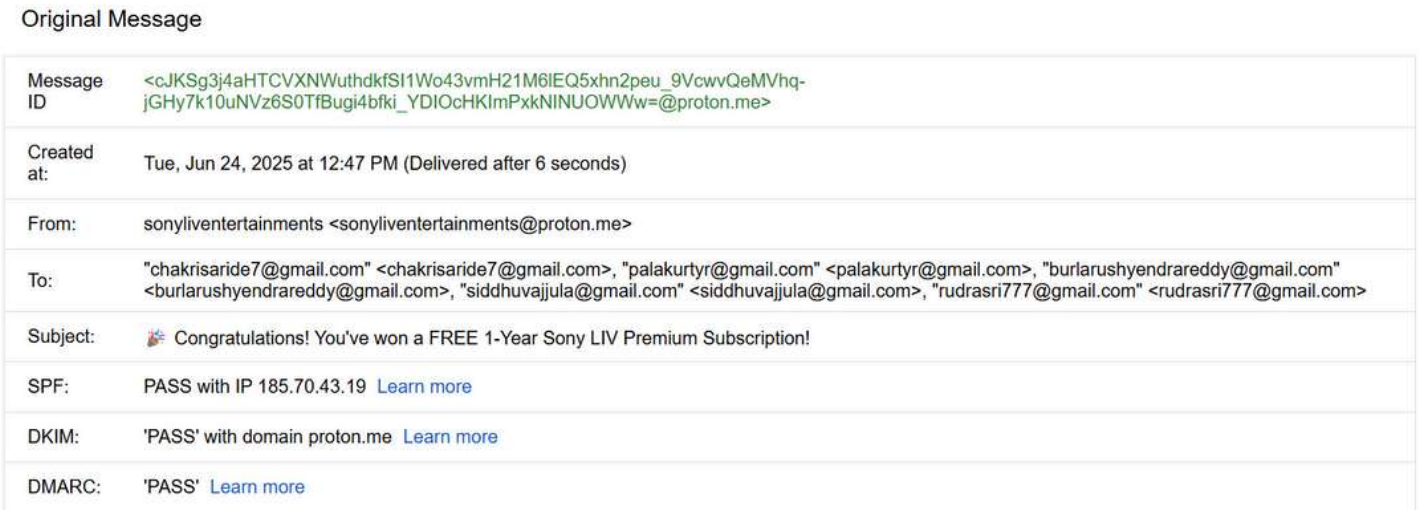
If you have any questions or need assistance, please contact our support team at <help@sonyliv-offers.com>.

Thank you for choosing Sony LIV.
Enjoy streaming! 🎥✨

Best regards,
Sony LIV Promotions Team

2)

I'll examine the email header for spoofing



Original Message

Message ID	<cJKSg3j4aHTCVXNWuthdkfSI1Wo43vmH21M6lEQ5xhn2peu_9VcwvQeMVhq-jGHy7k10uNVz6S0TfBugi4bfki_YDIOcHKImPxkNINUOWWw=@proton.me>
Created at:	Tue, Jun 24, 2025 at 12:47 PM (Delivered after 6 seconds)
From:	sonyliventertainments <sonyliventertainments@proton.me>
To:	"chakrisaride7@gmail.com" <chakrisaride7@gmail.com>, "palakurtyr@gmail.com" <palakurtyr@gmail.com>, "burlarushyendrareddy@gmail.com" <burlarushyendrareddy@gmail.com>, "siddhuvajjula@gmail.com" <siddhuvajjula@gmail.com>, "rudrasri777@gmail.com" <rudrasri777@gmail.com>
Subject:	🎉 Congratulations! You've won a FREE 1-Year Sony LIV Premium Subscription!
SPF:	PASS with IP 185.70.43.19 Learn more
DKIM:	'PASS' with domain proton.me Learn more
DMARC:	'PASS' Learn more

this is the header of the mail i got

by analyzing i can say that the email uses a ProtonMail domain instead of an official Sony domain, which is a clear sign that it's not legitimate. Even though the display name is set as sonyliventertainments, that can be easily faked and doesn't prove anything about the sender's identity. SPF, DKIM, and DMARC checks all passed, but they only verify that the email was allowed by ProtonMail's servers, not that it's actually from Sony. There's no use of Sony's branding, official domain, or any verified links, which makes it look unprofessional and suspicious. The subject line is also a common phishing tactic, using a fake reward message to

3)

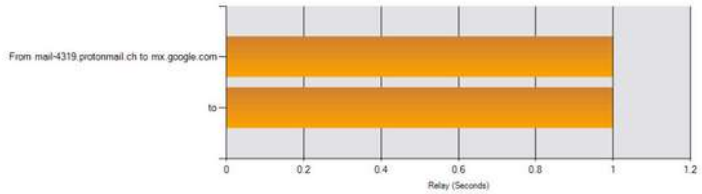
Using an online mail header analyzer the report i got is

Delivery Information

- DMARC Compliant
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

Relay Information

Received Delay:	0 seconds



Can see that DKIM isn't authenticated this means that the sending domain which it is pretending to be isn't authenticated so this is mostly a phishing attempt.

4)

Dear User,

We are excited to inform you that your email has been selected for an **exclusive reward** — a **FREE 1-Year Sony LIV Premium Subscription** 🎬🍿!

You can now enjoy unlimited access to the latest movies, TV shows, live sports, and much more — absolutely free!

👉 **Activate your subscription now** by clicking the secure link below:

Claim Your Free 1-Year Subscription

Hurry! This offer is valid for **48 hours only** — don't miss out!

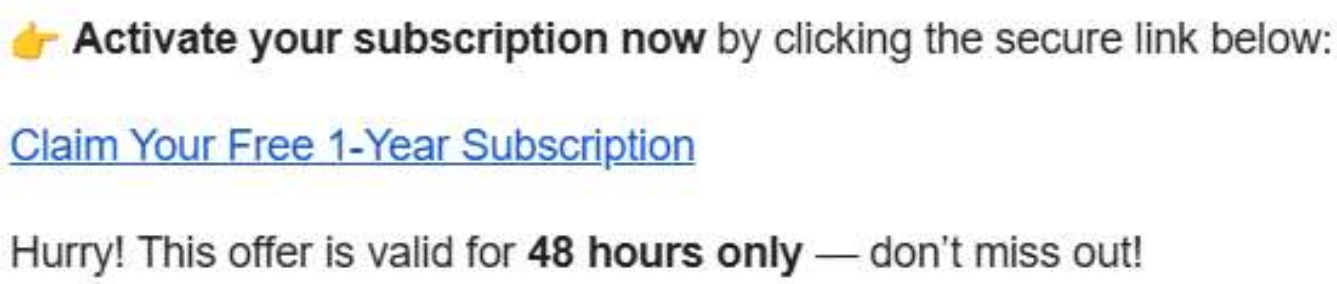
If you have any questions or need assistance, please contact our support team at <help@sonyliv-offers.com>.

Thank you for choosing Sony LIV.
Enjoy streaming! 🎥✨

Best regards,
Sony LIV Promotions Team

There is a hyperlink stating that Claim your offer which might be an unsecure website when entered and if any details are provided this may lead to leaking of the users sensitive information such as passwords and anything important that exists in that account.

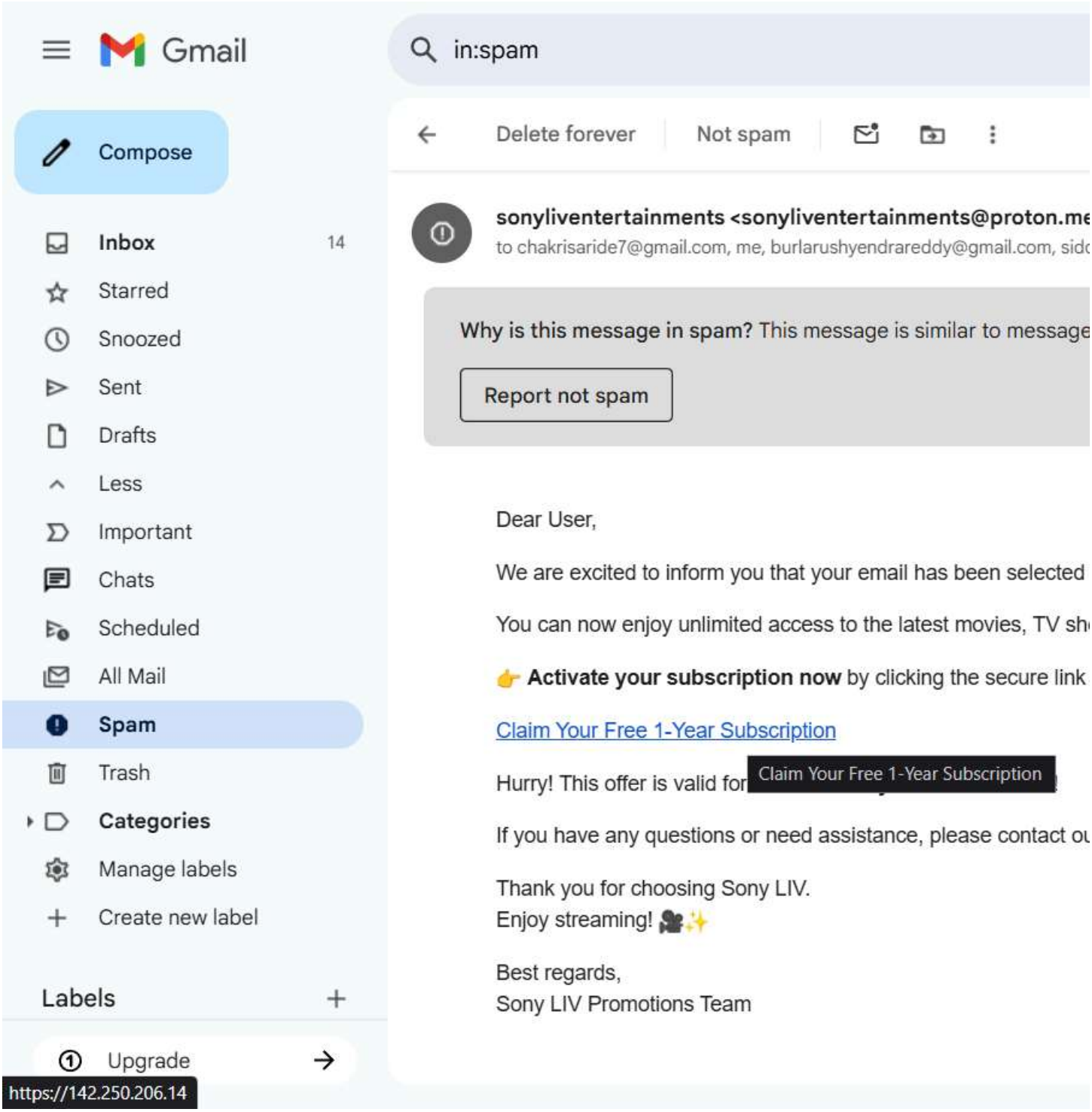
5)



can be clearly seen that the attacker is pushing by creating an urgency that the offer expires in 48 hours.

6)

While hovering over the link we can see that we are being redirected to some random IP(can be seen at bottom left) which clearly isn't a website of sonyliv.



7)

There are no major spelling or grammar errors in the text The language is clean and professional which can make the email seem more convincing however this is common in more polished phishing emails.

8)

This email has a few clear signs of phishing first it offers a free 1 year sony liv subscription

for only 48 hours it doesn’t use my name just says dear user which makes it feel like a bulk message the email address they give for support is not official it ends with sonyliv offers com instead of the real sony domain all these things together make it look suspicious and likely to be a phishing attempt.