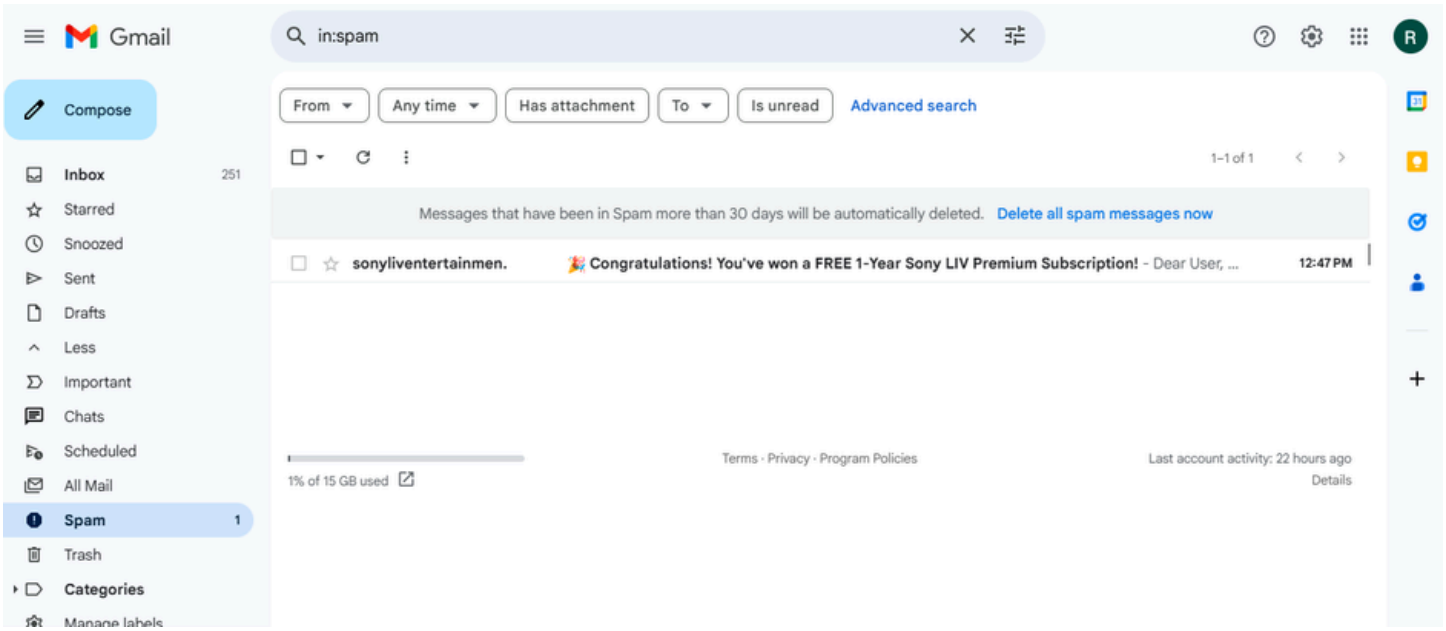
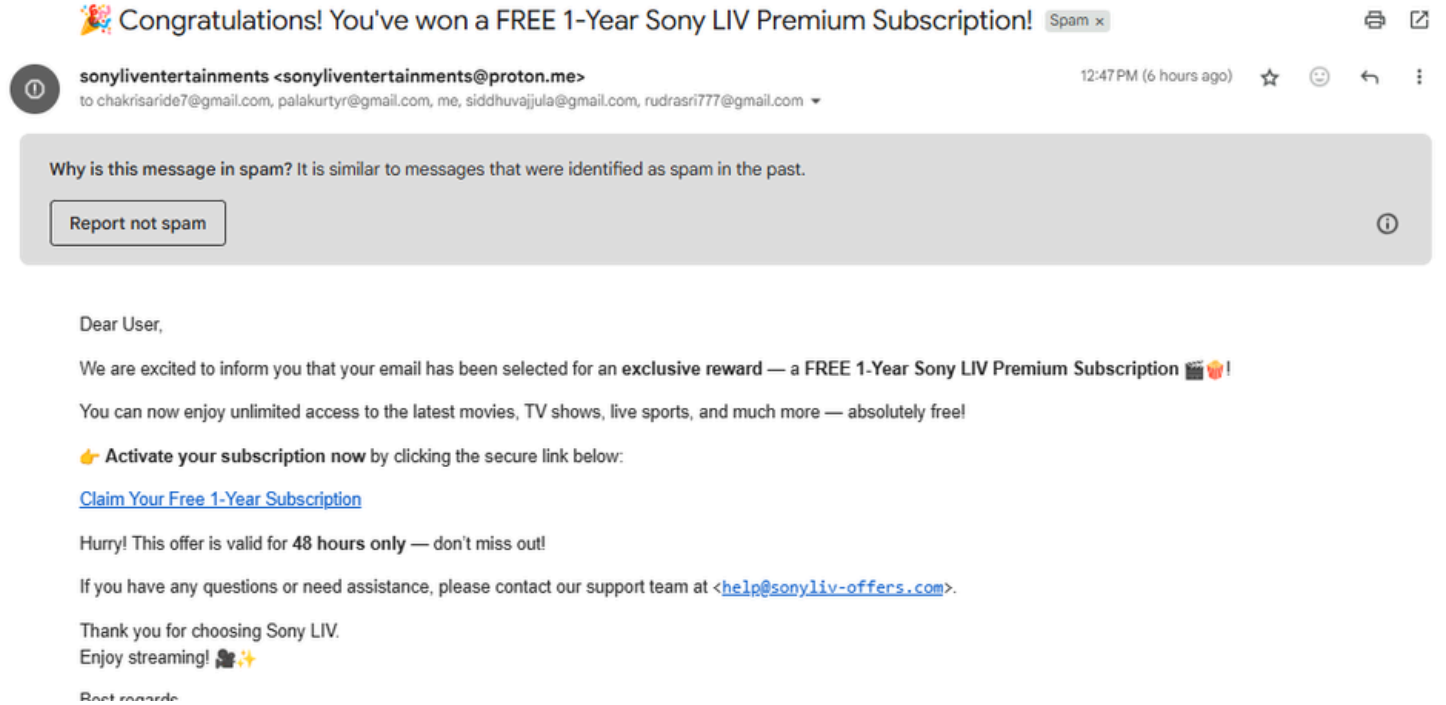
ELEVATE LABS CYBER SECURITY INTERNSHIP

Task-2:

1. Email Identification

Since I couldn't find a real phishing email in my inbox, my friends and I crafted a fake spam email for analysis. We created a message appearing to be from “sonyliventertainments” offering a free one-year SonyLIV subscription, with a link redirecting to an unrelated website—mimicking typical phishing behavior.





2. Header Analysis for Spoofing

I analyzed the email header and found that it was sent from a **ProtonMail** domain, not an official Sony domain. Although the sender's display name was "sonyliventertainments", this can easily be forged. While SPF, DKIM, and DMARC checks passed, they only confirm the email came through ProtonMail servers—not that it's truly from Sony. The email lacked any Sony branding or official links, making it appear untrustworthy and fake. The subject line also uses a typical phishing tactic—offering a fake reward to entice clicks.

Original Message

Message ID	<cJKSg3j4aHTCVXNWuthdkfSI1Wo43vmH21M6IEQ5xhn2peu_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 185.70.43.25 Learn more
DKIM:	'PASS' with domain proton.me Learn more
DMARC:	'PASS' Learn more

3. Header Analyzer Tool

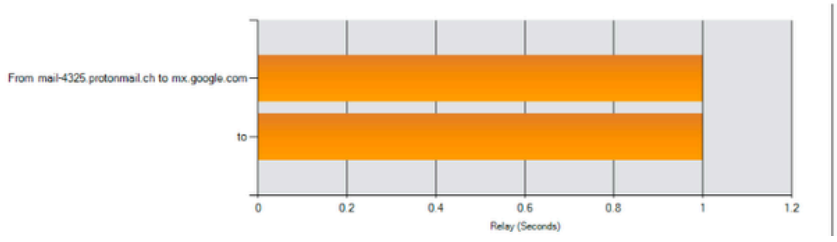
Using an online email header analyzer, I observed that **DKIM was not authenticated**, which suggests that the domain used is likely forged. This strongly indicates a phishing attempt since legitimate senders would have properly authenticated headers.

Delivery Information

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

Relay Information

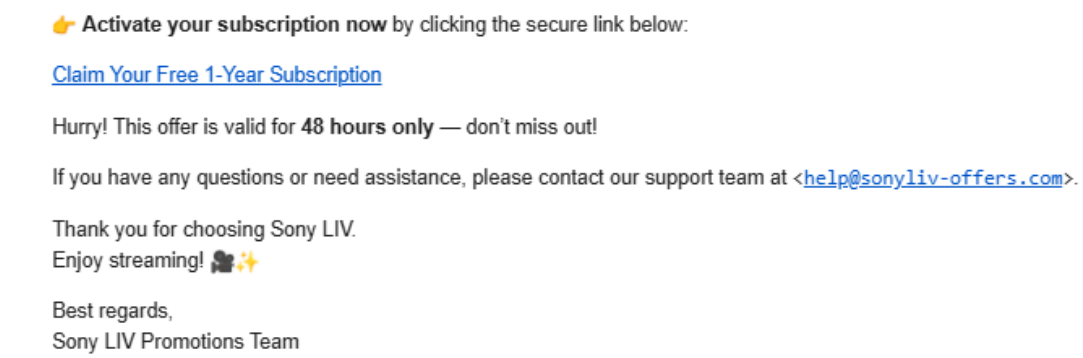
Received Delay:	0 seconds



We can see that DKIM isn't authenticated, the sender domain isn't authenticated. This could be mostly a phishing attempt.

4. Suspicious Links

The email includes a hyperlink labeled “Claim your 1-year Subscription.” Upon clicking, it redirects to an unverified and possibly malicious website. Entering personal details on such a site could result in credential theft or unauthorized access to sensitive accounts.


👉 **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>.

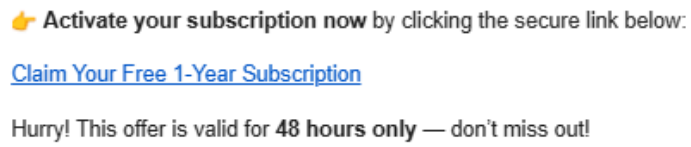
Thank you for choosing Sony LIV.
Enjoy streaming! 🎥✨

Best regards,
Sony LIV Promotions Team

We can see that DKIM isn’t authenticated, the sender domain isn’t authenticated. This could be mostly a phishing attempt.

5. Urgency Tactic

The email pressures the recipient by stating that the offer will expire in **48 hours**, a common psychological tactic used in phishing to provoke quick, thoughtless actions.

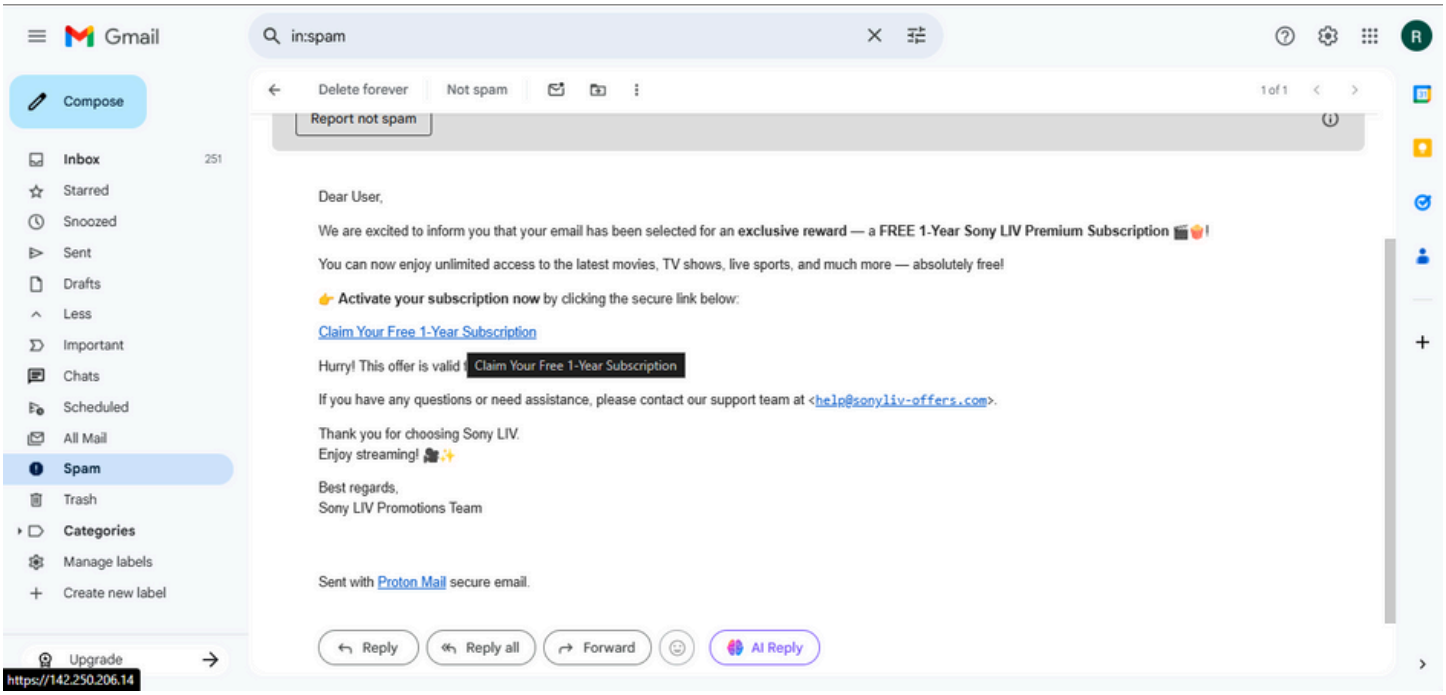

👉 **Activate your subscription now** by clicking the secure link below:

Claim Your Free 1-Year Subscription

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

6. Mismatched URL

By hovering over the provided link, it becomes clear that the URL redirects to a **random IP address**, not a legitimate **SonyLIV** website. This is a strong indicator of phishing, as legitimate companies never use such tactics.



7. Language and Grammar

The email is written with **grammatically correct** language and a professional tone. While this makes it appear legitimate, many advanced phishing emails are carefully worded to avoid suspicion.

8. Summary of Phishing Indicators

This email displays several key phishing traits:

- It promises a **free SonyLIV subscription**, which is likely too good to be true.
- Creates urgency with a **48-hour expiry warning**.
- Uses a generic greeting like “Dear user” instead of the recipient’s name.
- The **support email** ends in an unofficial domain like @sonylivoffers.com, not the real Sony domain.
  All these signs collectively point to a **phishing attempt**.