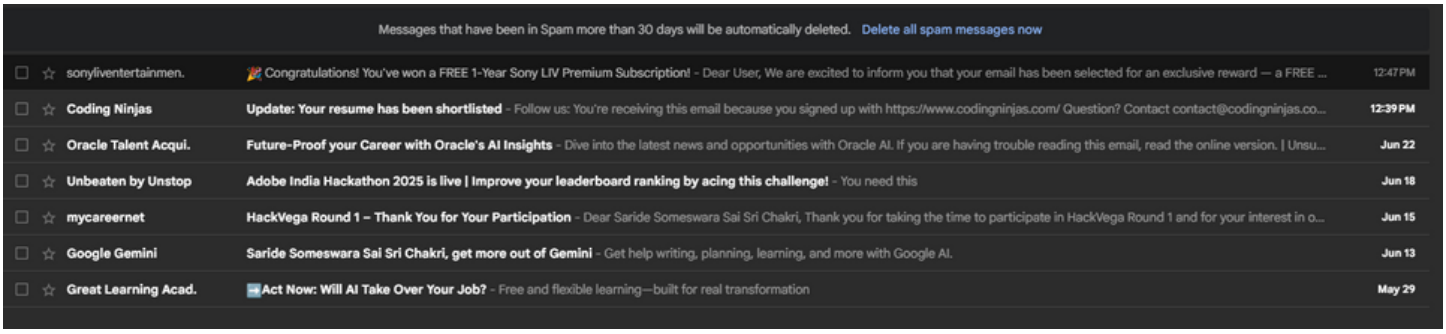
ELEVATE LABS CYBER SECURITY INTERNSHIP

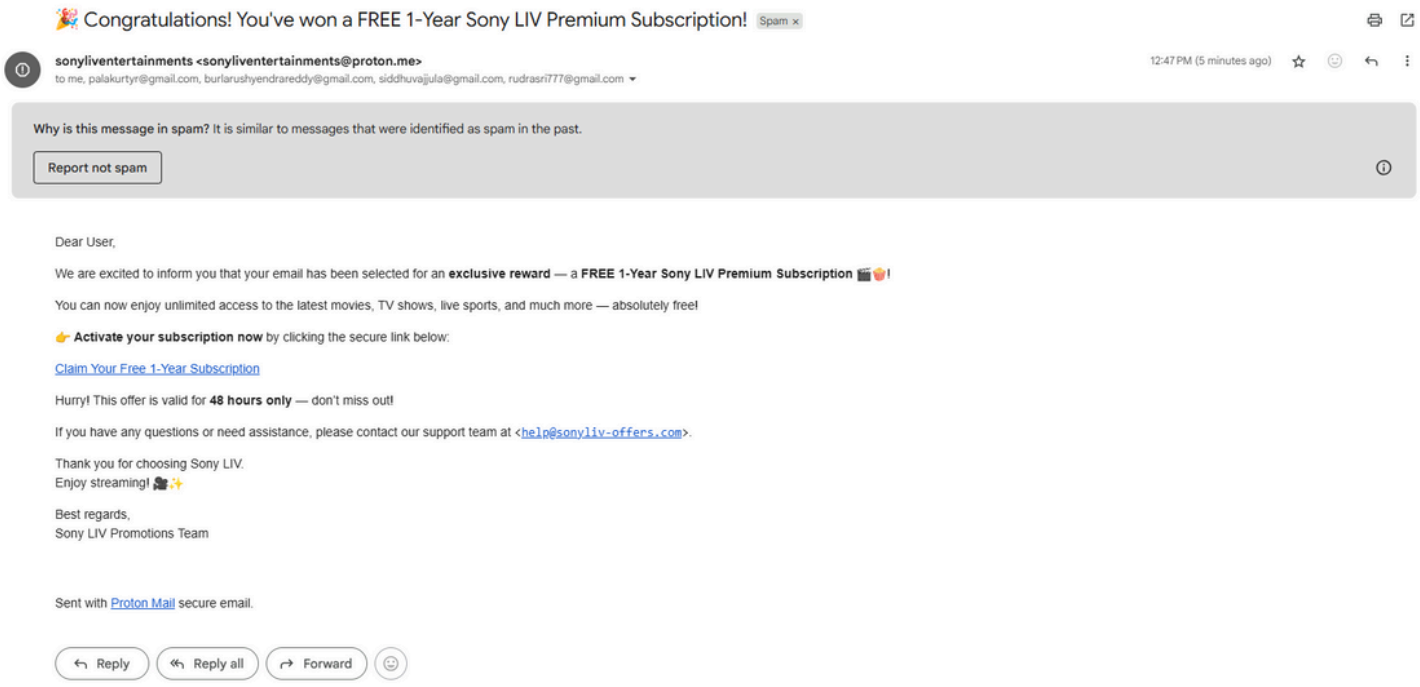
Task-2:

1.Obtain a sample phishing email

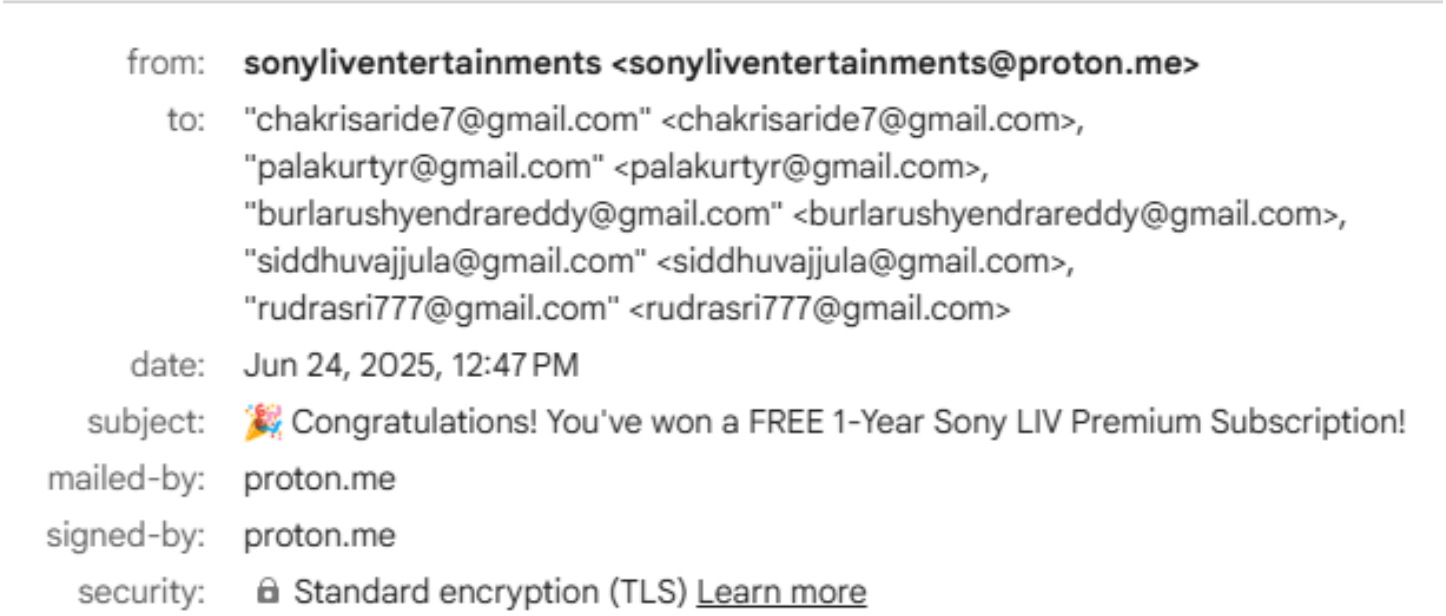
To do this task I sent a fake proton mail to me and my friends as sonyliventertainments saying we got a free one year subscription to the sonyliv and it was sent directly to spam.



The mail contains the following



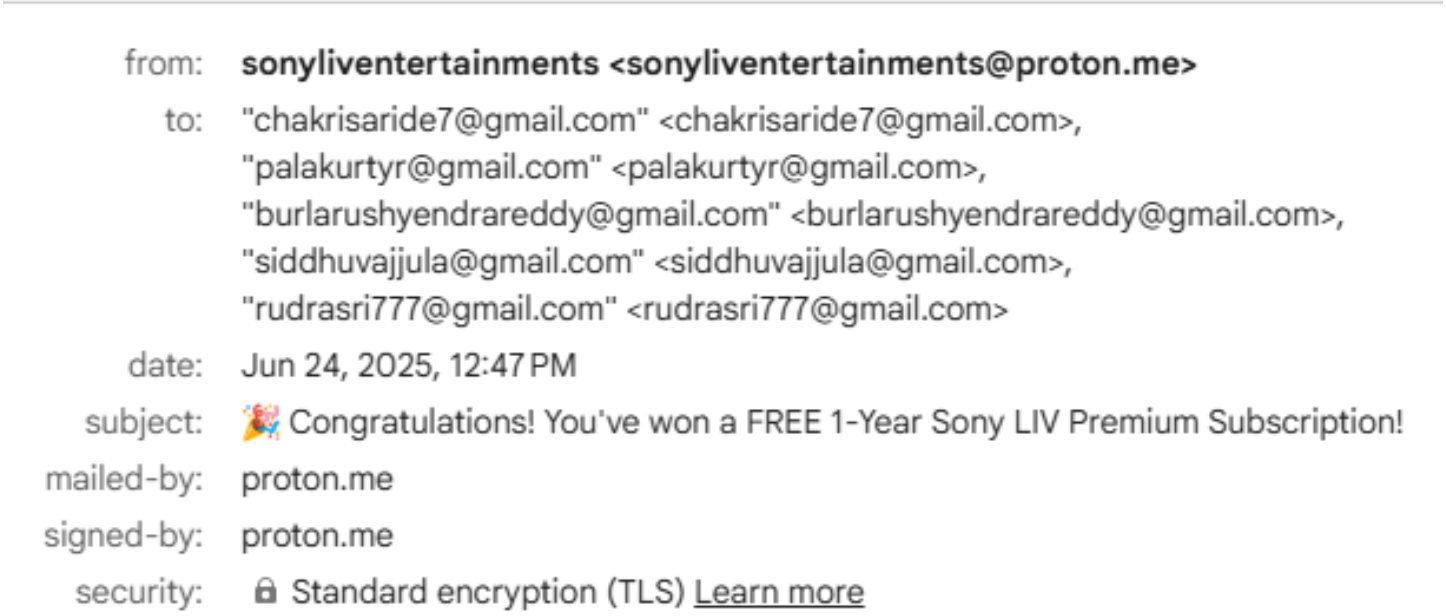
2.Examine sender's email address for spoofing.



The sender's email is sonyliventertainments@proton.me. At first glance, it seems to be from Sony LIV, but the domain is actually @proton.me, which is just a free email service—not an official Sony domain like @sonyliv.com. Anyone can set up an email like that to impersonate Sony. The name might say "sonyliventertainments," but that can easily be faked. Since it's not sent from a real Sony domain and lacks proper verification like SPF or DKIM to prove it's legitimate, I believe this email is spoofed and not really from Sony.

3.Check email headers for discrepancies.

Email header:



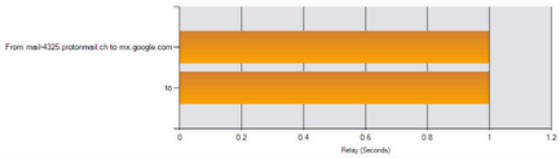
Here after analysing the header using the tool Email Header Analyzer, RFC822 Parser it stated that DKIM (DomainKeys Identified Mail) Authentication is failed.

Delivery Information

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

Relay Information

Received Delay:	0 seconds



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	mail-4325.protonmail.ch 185.70.43.25	mx.google.com	ESMTPS	6/24/2025 7:17:21 AM	✓
2	0 seconds		2002:a05:612c:1d16:b0:4d5:dfa6:5b26	SMTP	6/24/2025 7:17:21 AM	

4.Identify suspicious links or attachments.

Here in the mail there is a link saying **Claim Your Free 1-Year Subscription** and there is a small description that claim it before 48 hours.

👉 **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!

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

“Hurry! This offer is valid for 48 hours only — don’t miss out!” This creates urgency and pushes the user to click the link fast before verifying the legitimacy.

6.Note any mismatched URLs

Here when I try to open the link it is redirecting to google and there is possibe credential leakage if we try to login.

7.Verify presence of spelling or grammar errors.

There was no identified grammer mistakes, here the grammer is entirely clear

8.Summarize phishing traits found in the email.

Basically this mail looks fishy. First of all, they’re giving “free 1-year subscription” randomly — sounds too good. They wrote “Dear User” — no name, so that’s already sus. Then they’re saying the offer is valid only for 48 hours — trying to make me click fast. Even the sender mail ID is not official Sony. The link also looks shady — might be a fake site. Too many signs of phishing here — not clicking this for sure.