

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.

Messages that have been in Spam more than 30 days will be automatically deleted. Delete all spam messages now			
<input type="checkbox"/>	☆ sonyliventertainmen.	Congratulations! You've won a FREE 1-Year Sony LIV Premium Subscription! - Dear User, We are excited to inform you that your email has been selected for an exclusive reward — a FREE ...	12:47 PM
<input type="checkbox"/>	☆ Coding Ninjas	Update: Your resume has been shortlisted - Follow us: You're receiving this email because you signed up with https://www.codingninjas.com/ Question? Contact contact@codingninjas.co...	12:39 PM
<input type="checkbox"/>	☆ Oracle Talent Acqui.	Future-Proof your Career with Oracle's AI Insights - Dive into the latest news and opportunities with Oracle AI. If you are having trouble reading this email, read the online version. Unsu...	Jun 22
<input type="checkbox"/>	☆ Unbeaten by Unstop	Adobe India Hackathon 2025 is live Improve your leaderboard ranking by acing this challenge! - You need this	Jun 18
<input type="checkbox"/>	☆ mycareernet	HackVega Round 1 – Thank You for Your Participation - Dear Saride Someswara Sai Sri Chakri, Thank you for taking the time to participate in HackVega Round 1 and for your interest in o...	Jun 15
<input type="checkbox"/>	☆ Google Gemini	Saride Someswara Sai Sri Chakri, get more out of Gemini - Get help writing, planning, learning, and more with Google AI.	Jun 13
<input type="checkbox"/>	☆ Great Learning Acad.	Act Now: Will AI Take Over Your Job? - Free and flexible learning—built for real transformation	May 29

The mail contains the following

Congratulations! You've won a FREE 1-Year Sony LIV Premium Subscription! Spam x

sonyliventertainments <sonyliventertainments@proton.me>
to me, palakurtyr@gmail.com, burlarushyendrarreddy@gmail.com, siddhuva@jula@gmail.com, rudrasri777@gmail.com ▾

12:47 PM (5 minutes ago) ☆ 😊 ↶ ⋮

Why is this message in spam? It 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

Sent with [Proton Mail](#) secure email.

↶ Reply

↶ Reply all

↷ Forward

😊

2.Examine sender's email address for spoofing.

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>
date: Jun 24, 2025, 12:47 PM
subject: 🎉 Congratulations! You've won a FREE 1-Year Sony LIV Premium Subscription!
mailed-by: proton.me
signed-by: proton.me
security: 🔒 Standard encryption (TLS) [Learn more](#)

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:

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>
date: Jun 24, 2025, 12:47 PM
subject: 🎉 Congratulations! You've won a FREE 1-Year Sony LIV Premium Subscription!
mailed-by: proton.me
signed-by: proton.me
security: 🔒 Standard encryption (TLS) [Learn more](#)

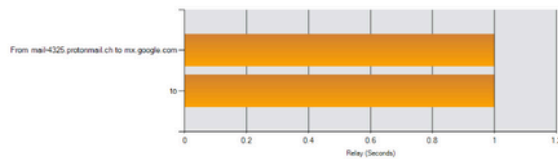
Here after analysing the header using the tool [Email Header Analyzer, RFC822 Parser](#) it stated that DKIM (DomainKeys Identified Mail) Authentication is failed.

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 possible credential leakage if we try to login.

7. Verify presence of spelling or grammar errors.

There was no identified grammar mistakes, here the grammar 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.