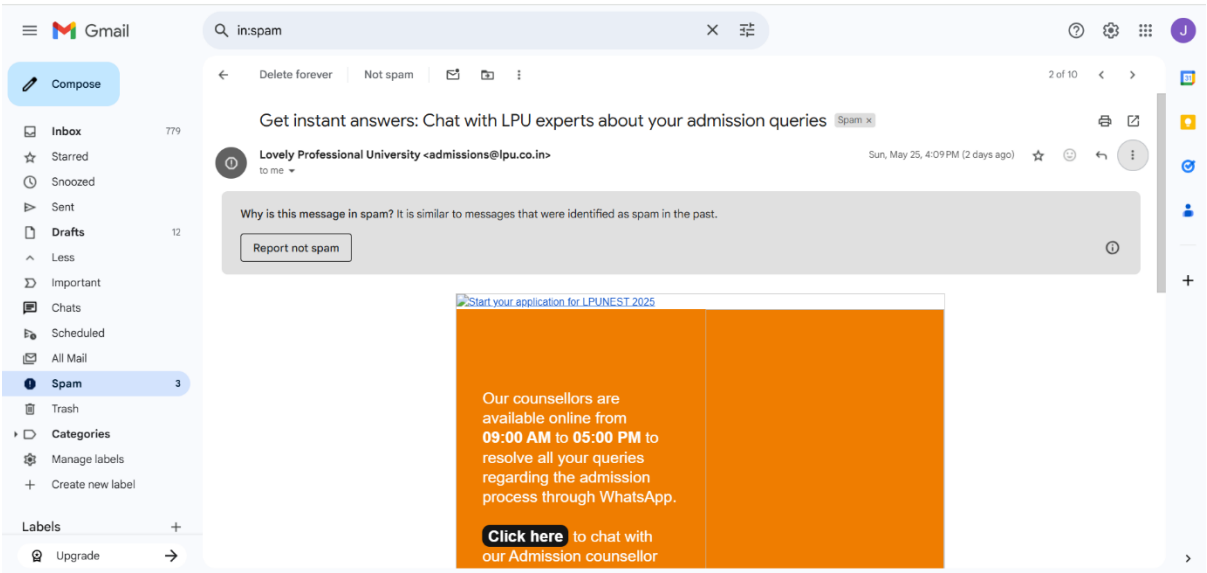
Analyze a Phishing Email Sample

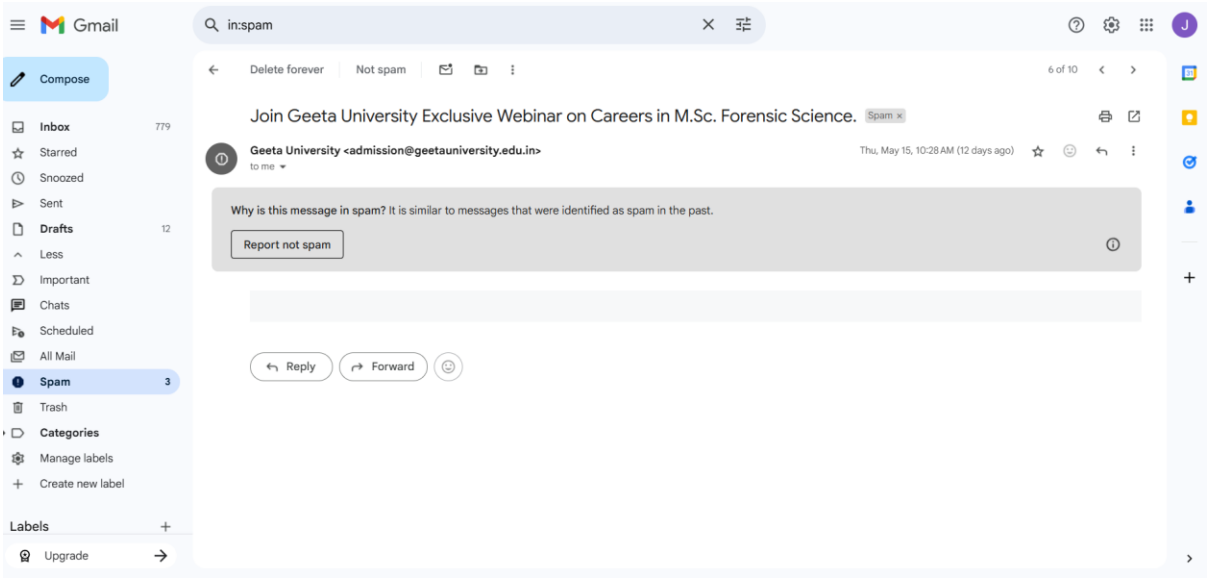
Objective: Identify phishing characteristics in a suspicious email sample.

Tools: Email client or saved email file (text), free online header analyzer.

Deliverables: A report listing phishing indicators found

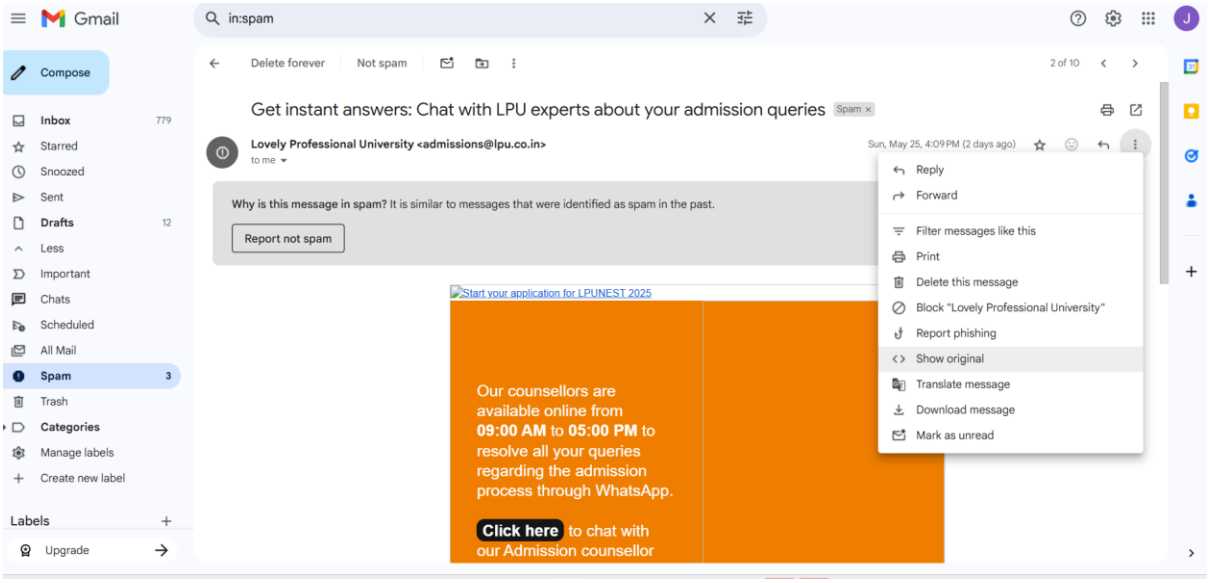
1. **Obtain a sample phishing email (many free samples online).**



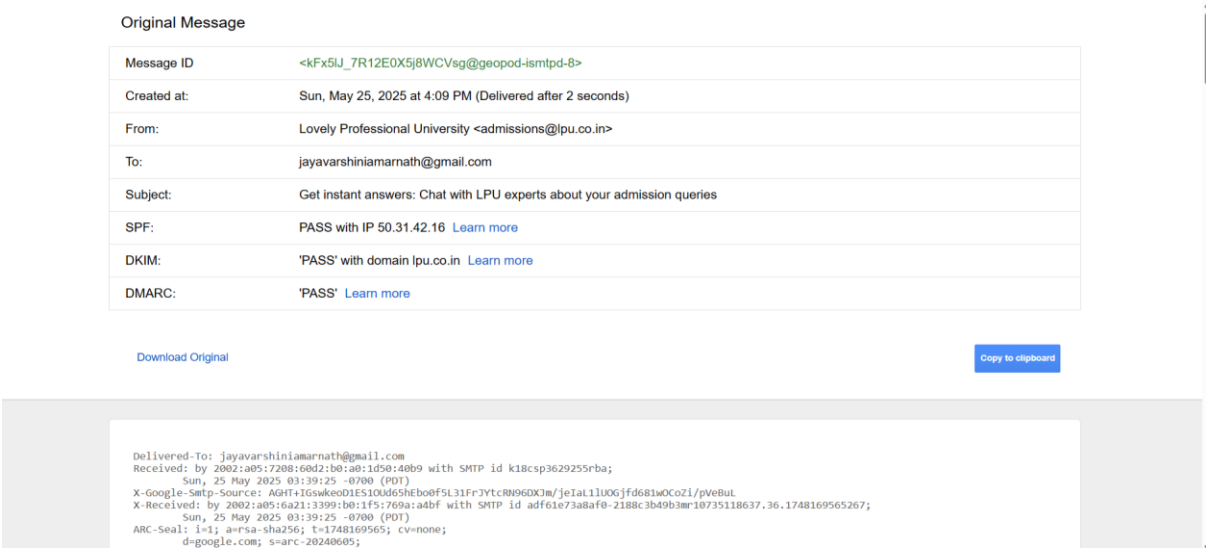


I have mentioned two spam emails from my email list . These are the sample phishing email .

2. Examine sender's email address for spoofing.

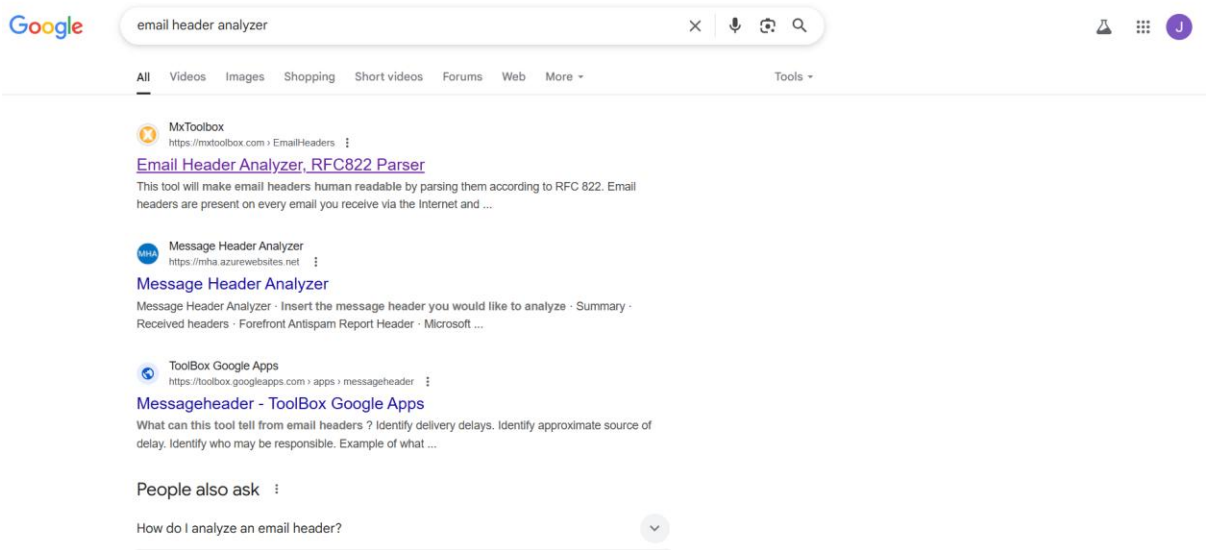


Verify and use the show original option to identify the email sender , and easy to check the spoofing attack .

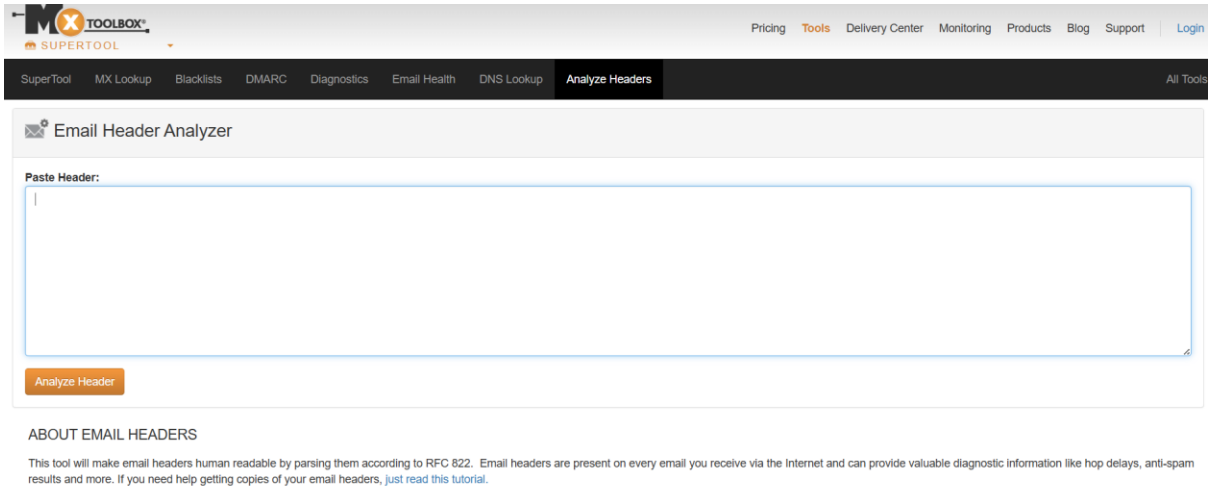


After clicking the show original option , it shows the clear history of the spoofing email.

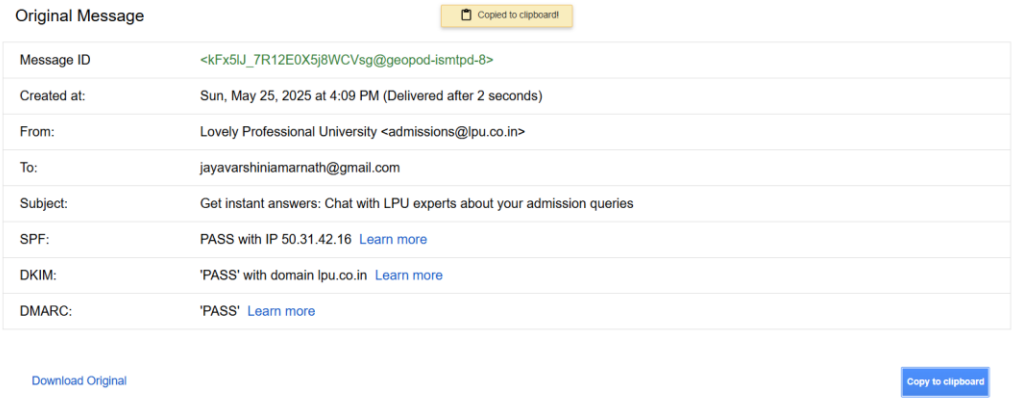
3. Check email headers for discrepancies (using online header analyzer).



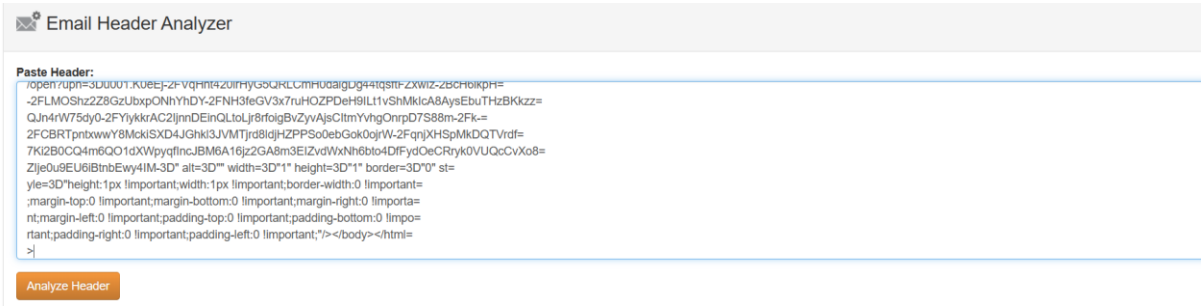
I have choose the MxToolbox Online header to analyse the email spoofing .



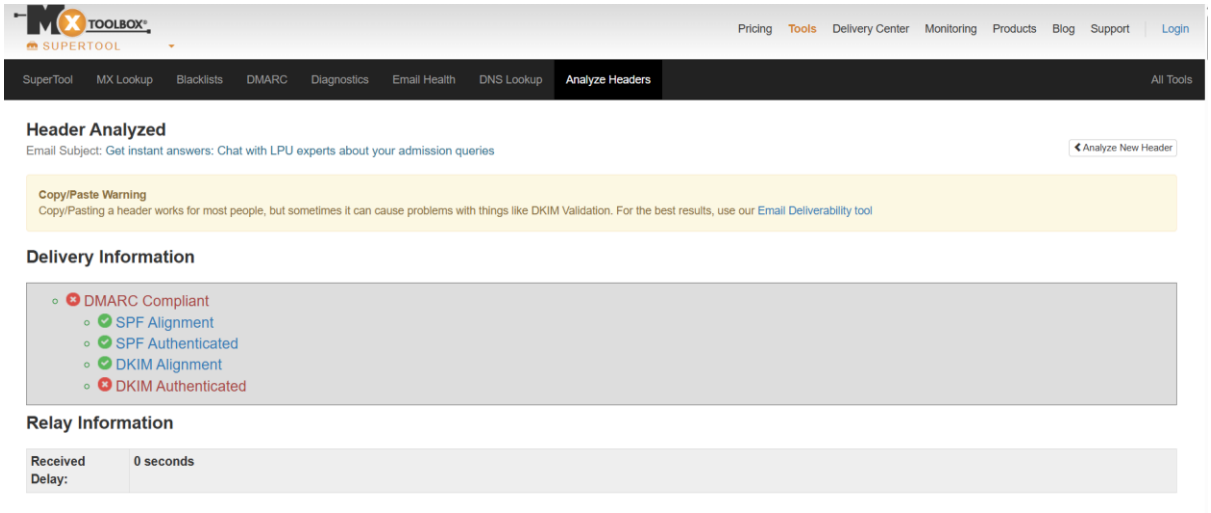
MxToolbox inside



Copy the code to analyse the email, and verify it is phishing email or not.



Click the Analyse Header to check the email.



It analysed the email and present their Delivery Information based on the email phishing .

1. DMARC COMPLIMENT
2. SPF ALIGNMENT
3. SPF AUTHENTICATED
4. DKIM ALIGNMENT
5. DKIM AUTHENTICATED

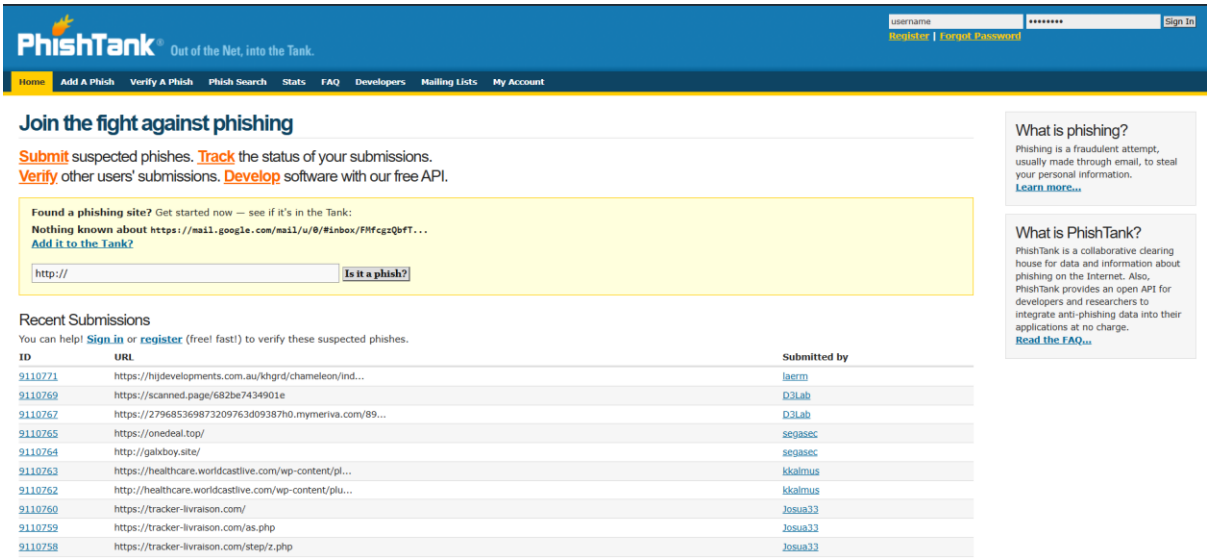
RELAY INFORMATION

PHISHING EMAIL EXPLAIN

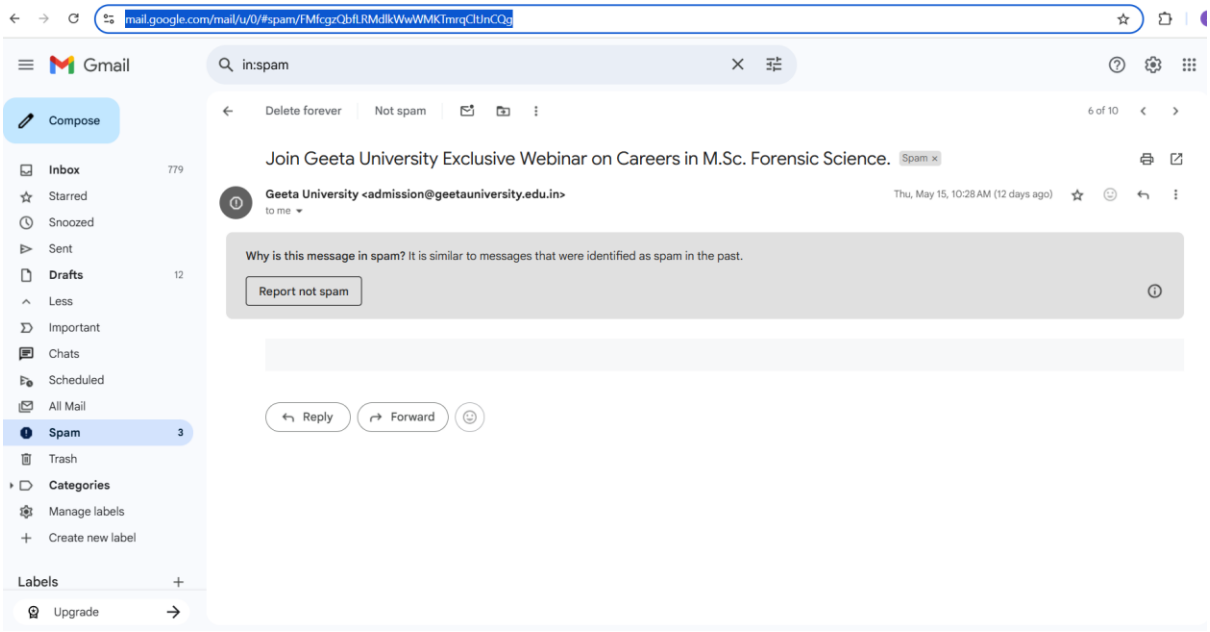
4. Identify suspicious links or attachments.

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

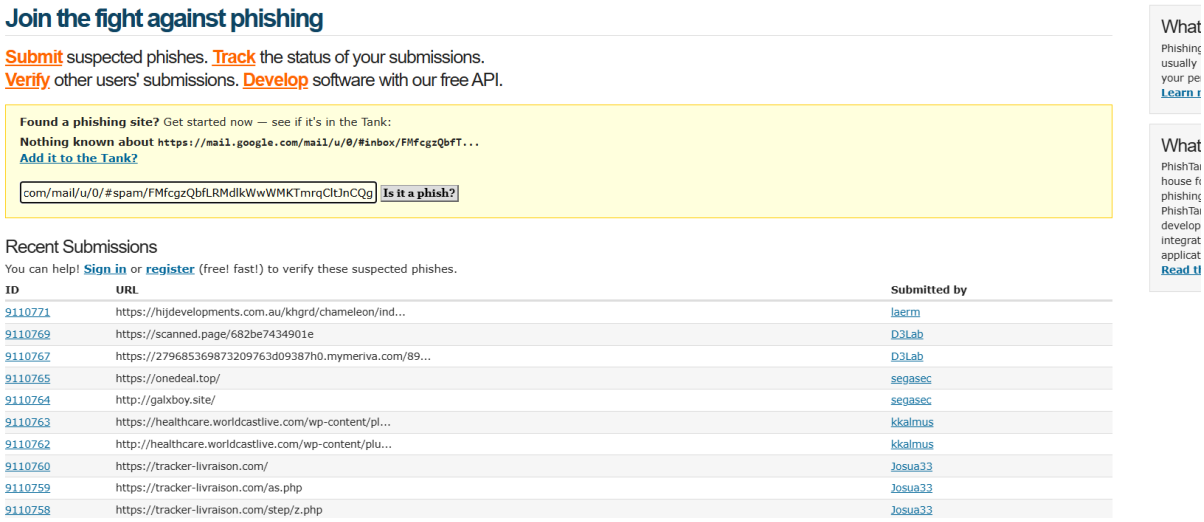
I have used Phishtank to verify the url whether its suspicious links or not.



PhishTank Website



Copy the url and paste the **phishtank** website to identify the suspicious link .



Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:
Nothing known about `https://mail.google.com/mail1/u/0/#inbox/FMfcgzQbfT...`
Add it to the Tank?

com/mail/u/0/#spam/FMfcgzQbfLRMdlkWwWMKTmrqClt JnCQg **Is it a phish?**

Recent Submissions

You can help! Sign in or register (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
9110771	https://hijdevelopments.com.au/khgrd/chameleon/ind...	laerm
9110769	https://scanned.page/682be7434901e	D3Lab
9110767	https://279685369873209763d09387h0.mymeriva.com/89...	D3Lab
9110765	https://onedeal.top/	segasec
9110764	http://galxboy.site/	segasec
9110763	https://healthcare.worldcastlive.com/wp-content/pl...	kkalmus
9110762	http://healthcare.worldcastlive.com/wp-content/plu...	kkalmus
9110760	https://tracker-livraison.com/	Josua33
9110759	https://tracker-livraison.com/as.php	Josua33
9110758	https://tracker-livraison.com/step/z.php	Josua33

Click **is it a phish** option to identify the email phishing URL.

6.Note any mismatched URLs (hover to see real link).

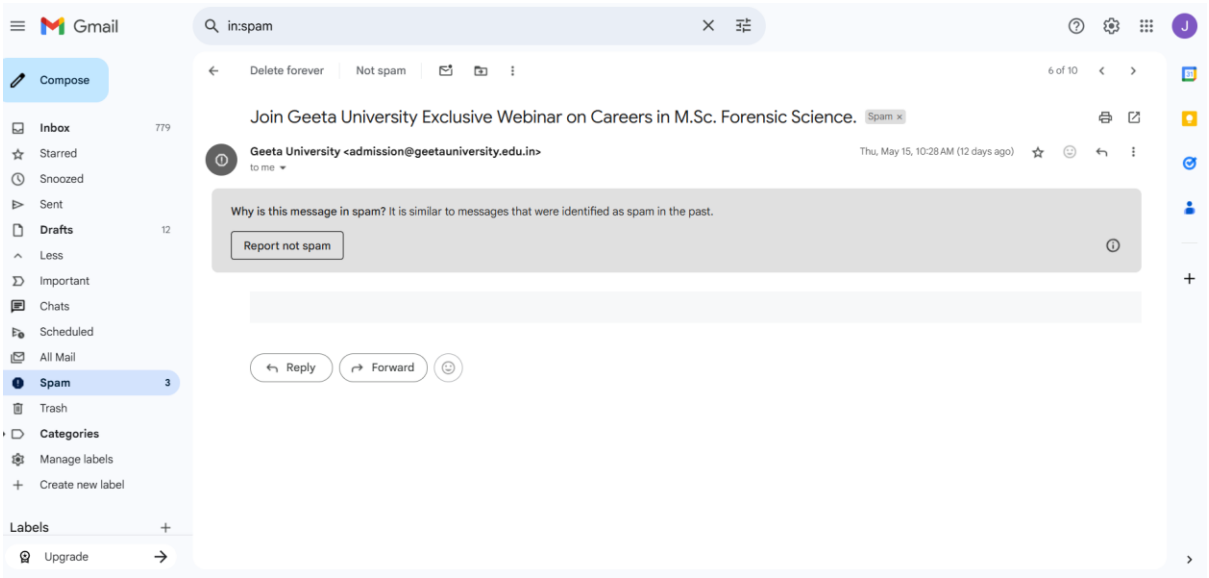
7.Verify presence of spelling or grammar errors.

Shown in Email	Real URL (on hover)	Suspicious?
https://gmail.com	http://login-gmail.fake.ru/login.html	☑ Yes

A **mismatched URL** means:

The **text you see** (like www.bank.com) is different from the **actual destination** (like http://malicious.ru/login).

8. Summarize phishing traits found in the email



The email from Geeta University (admissions@geetauniversity.edu.in) found in your spam folder has some traits commonly associated with phishing or spam emails. Here are the whisking (spam/phishing-like) traits identified:

1. Unsolicited Academic Offer: The email promotes a webinar on M.Sc. Forensic Science without prior engagement, which is a common tactic in phishing to attract clicks.

2. Generic Sender Address: The sender email (admission@geetauniversity.edu.in) may appear official but could be spoofed or mass-sent, leading Gmail to mark it as spam.

3. Similarity to Past Spam: Gmail specifically states that the message is "similar to messages that were identified as spam in the past."

4. Marketing Style Subject: The subject line ("Join Geeta University Exclusive Webinar…") uses enticing words like "Exclusive" and "Careers," which are often used in spam to lure users.

5. No Personalization: The message does not seem to be addressed personally, which is typical of mass-mail or phishing attempts.

6. Spam Label by Gmail: The presence in the Spam folder itself and the spam tag on the subject line strongly suggest it was flagged by Gmail's automated filters.

THANK YOU