PHISHING DETECTION

Hints/Mini Guide:

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

2.Examine sender's email address for spoofing.

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

4.Identify suspicious links or attachments.

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

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

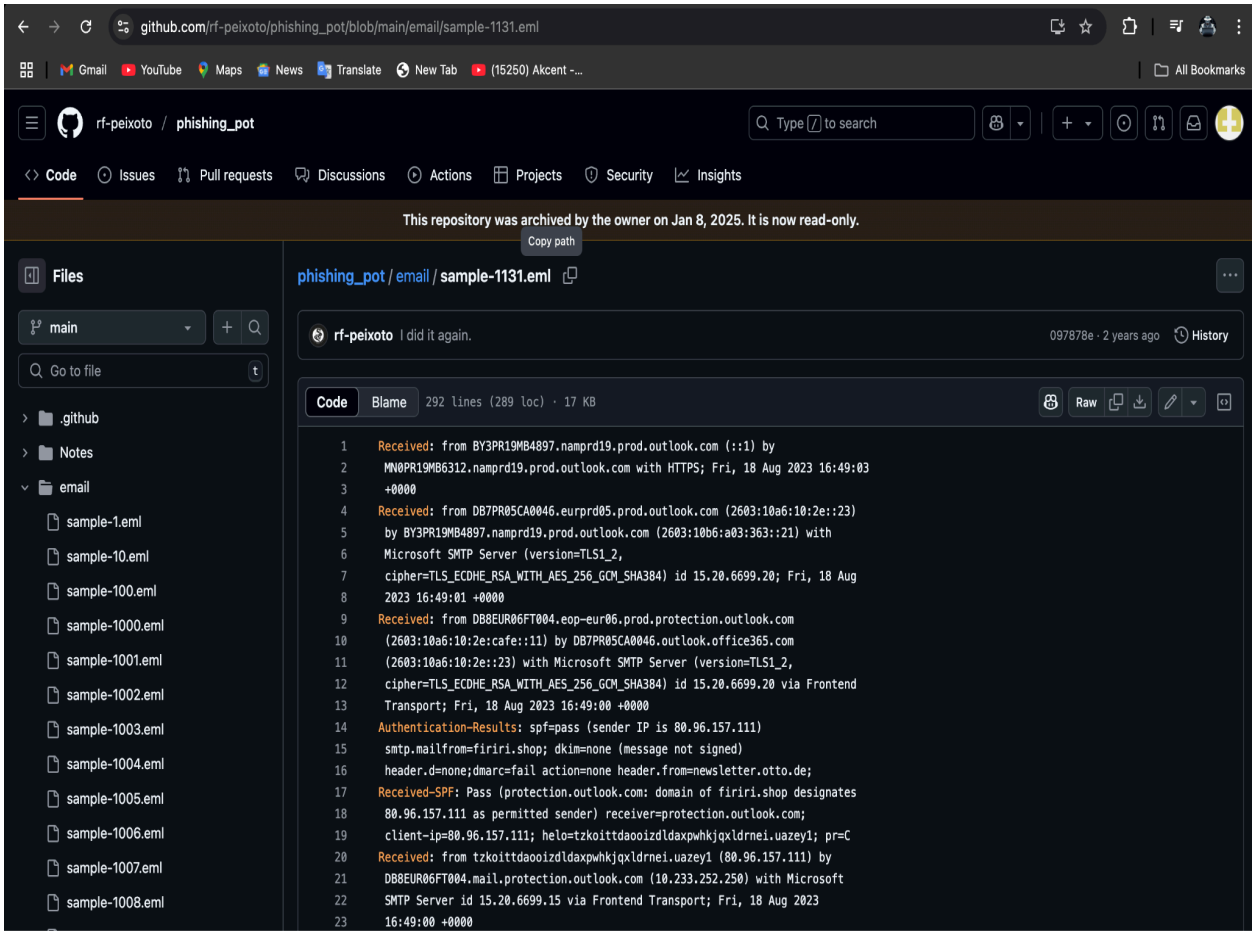
7.Verify presence of spelling or grammar errors.

8.Summarize phishing traits found in the email.

Outcome: : Awareness of phishing tactics and email threat analysis skills

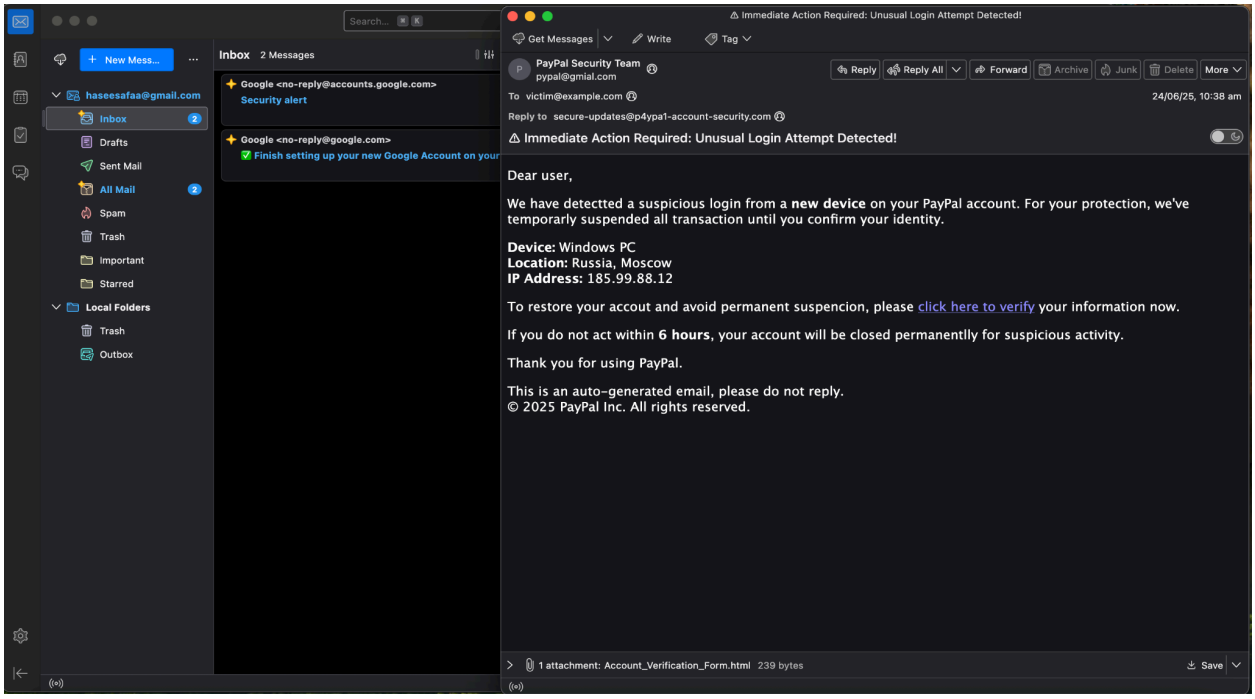
ANSWERS

- We can download sample phishing emails from github or any other online resources in .eml format or .html format .

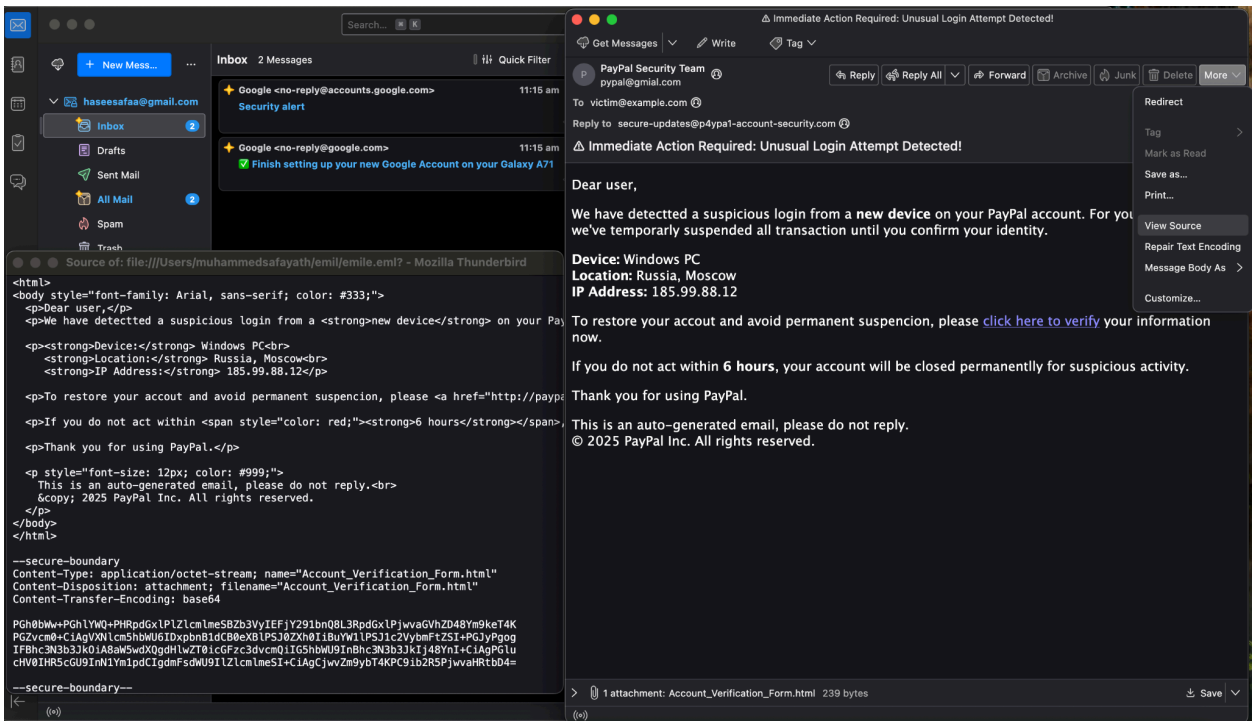


- Detect Spoofed Display name and analyse the email header and content on the emial. Here I am using Thunderbird For analysis .

  This is what a phishing email looks like :-

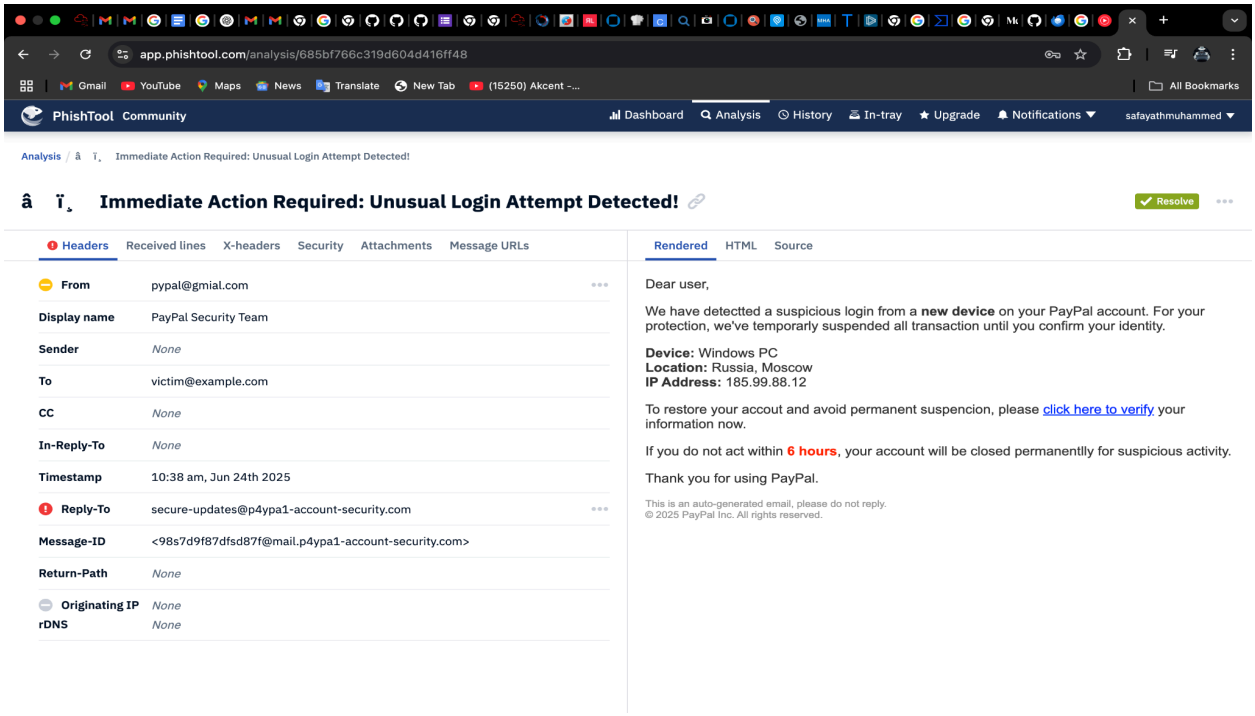


- Let us analyze email header for more details - raw html source code
- Every tool used here is mentioned below the screenshot.



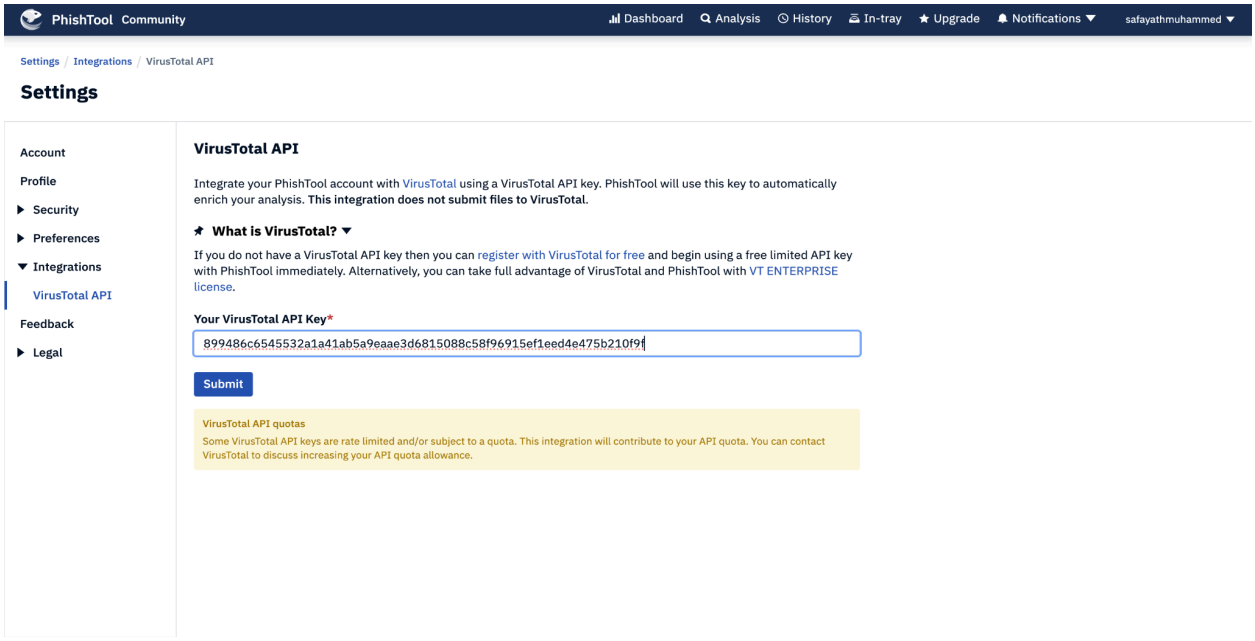
Thunderbird

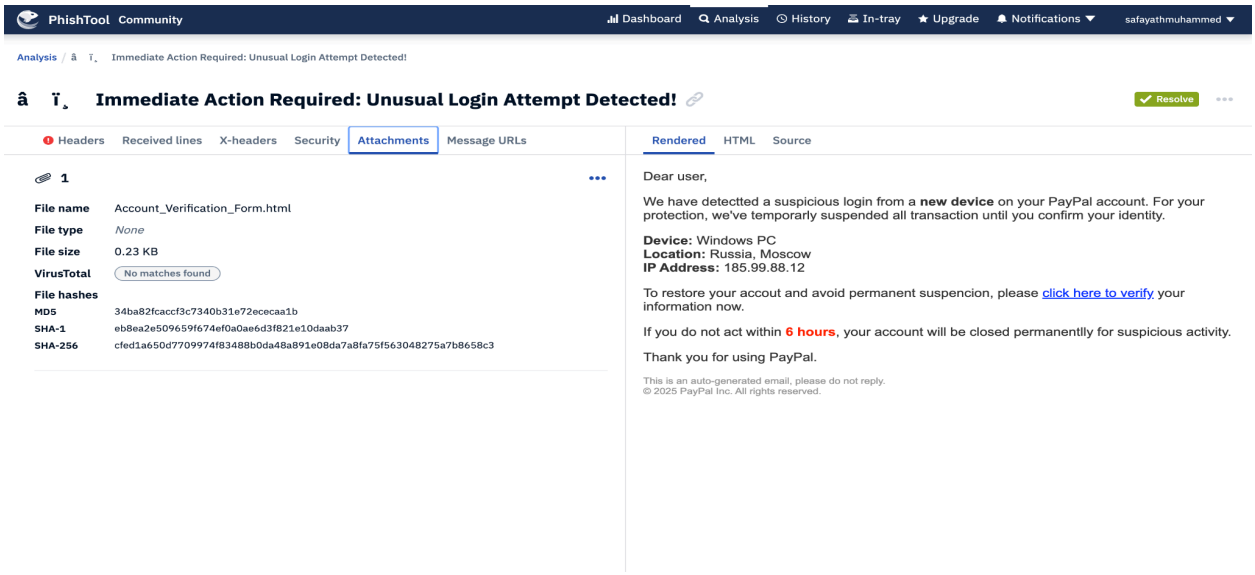
- The sender is trying to impersonate the “PayPal Security Team” here . and there is an attachment , spelling mistake and suspicious url.
- The sender's email id doesn't look legitimate and sure it is not from the paypal security team. - pypal@gmial.com



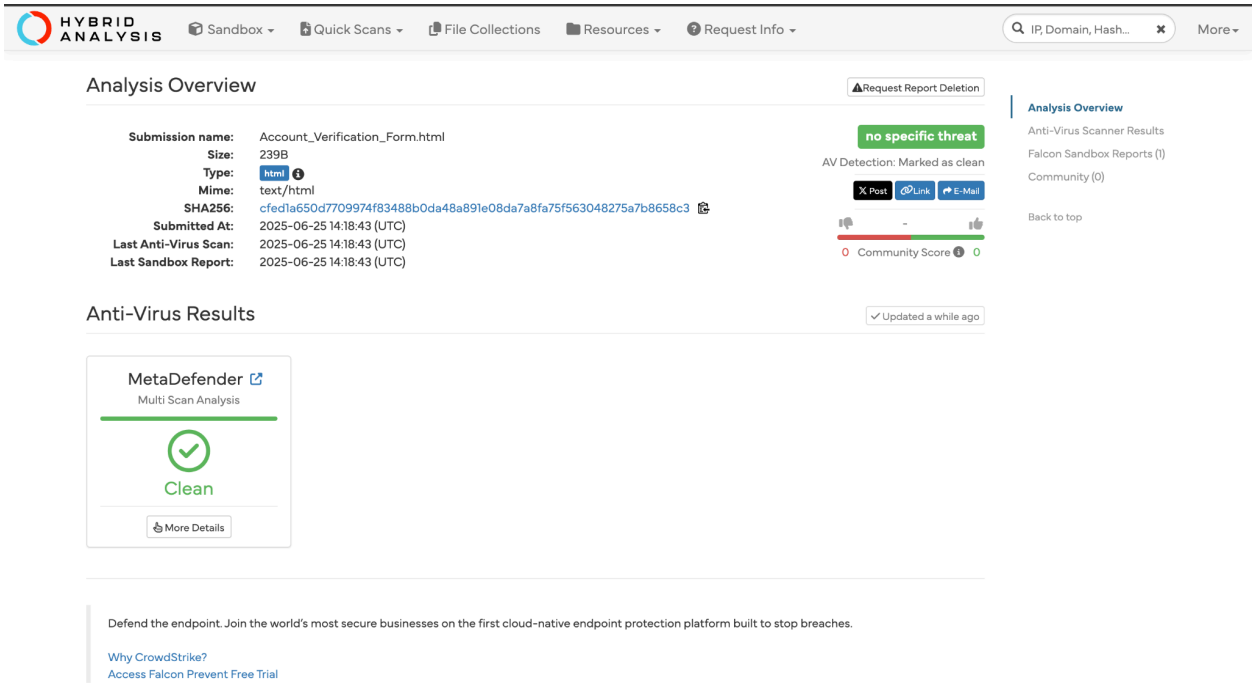
Phishtool

Integrate Phishtool with Virus tootal (VT) - API - For attachment analysis - Malware analysis





- This shows the attachment is not harmful and which is checked with a virus total massive malware database. But let us examine more , there are a lot of tools for malware - sandbox analysis and other analysis , we have to go to multiple tools. So we can find more information , but just one tool can not provide as much information and confirmation as we want . Especially if we are working in a business environment .

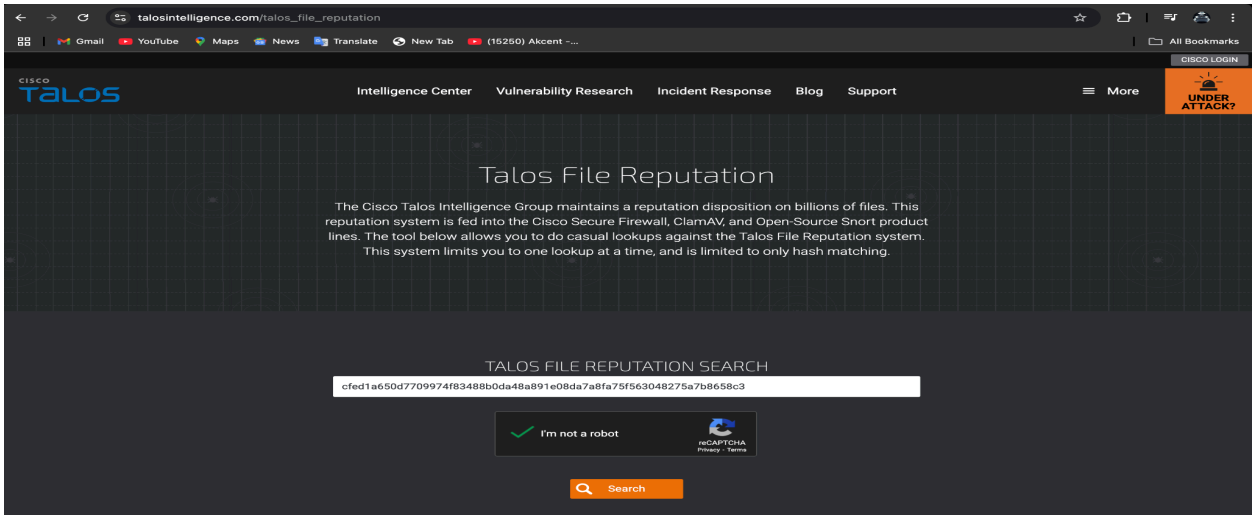


Hybrid analysis

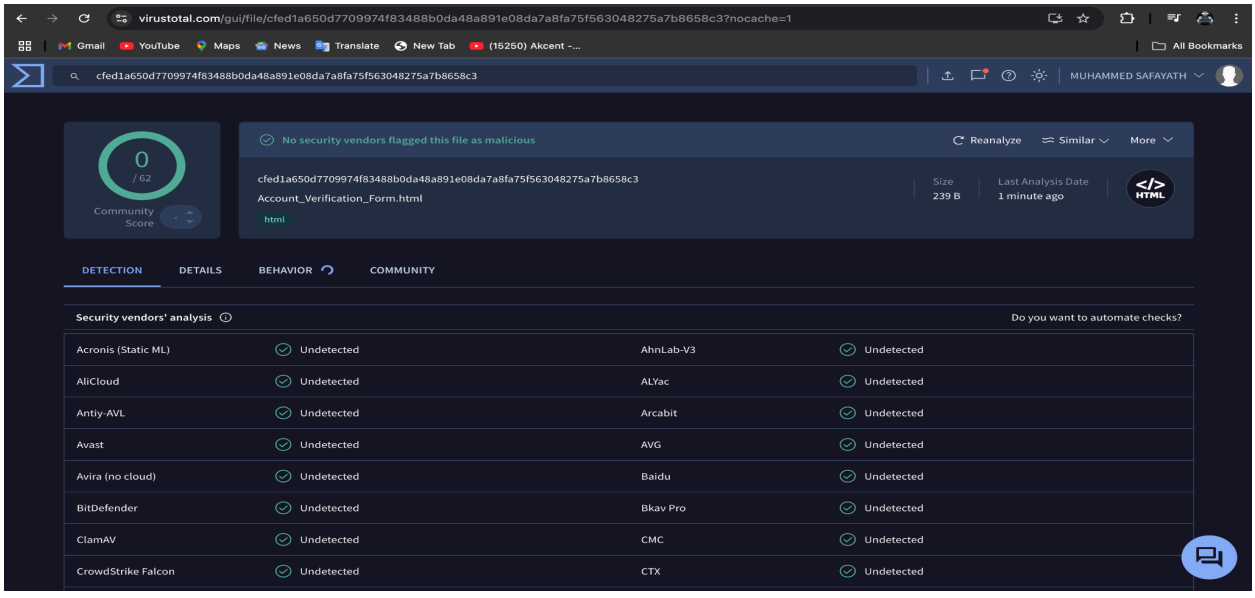
- Above image confirms there is no threat detected in the attachment file as per the analysis of MetaDefender .
- Collect the hash of the attached file and run in VT(virus total) or Cisco Talos.

```
muhammedsafayath@MUHAMMEDs-MacBook-Air Downloads % cd ../Desktop
muhammedsafayath@MUHAMMEDs-MacBook-Air Desktop % shasum Account_Verification_Form.html
eb8ea2e509659f674ef0a0ae6d3f821e10daab37  Account_Verification_Form.html
muhammedsafayath@MUHAMMEDs-MacBook-Air Desktop % md5 Account_Verification_Form.html
MD5 (Account_Verification_Form.html) = 34ba82fcaccf3c7340b31e72ececaa1b
muhammedsafayath@MUHAMMEDs-MacBook-Air Desktop % shasum -a 256 Account_Verification_Form.html
cfed1a650d7709974f83488b0da48a891e08da7a8fa75f563048275a7b8658c3  Account_Verification_Form.html
muhammedsafayath@MUHAMMEDs-MacBook-Air Desktop %
```

Collecting hash of the attachment

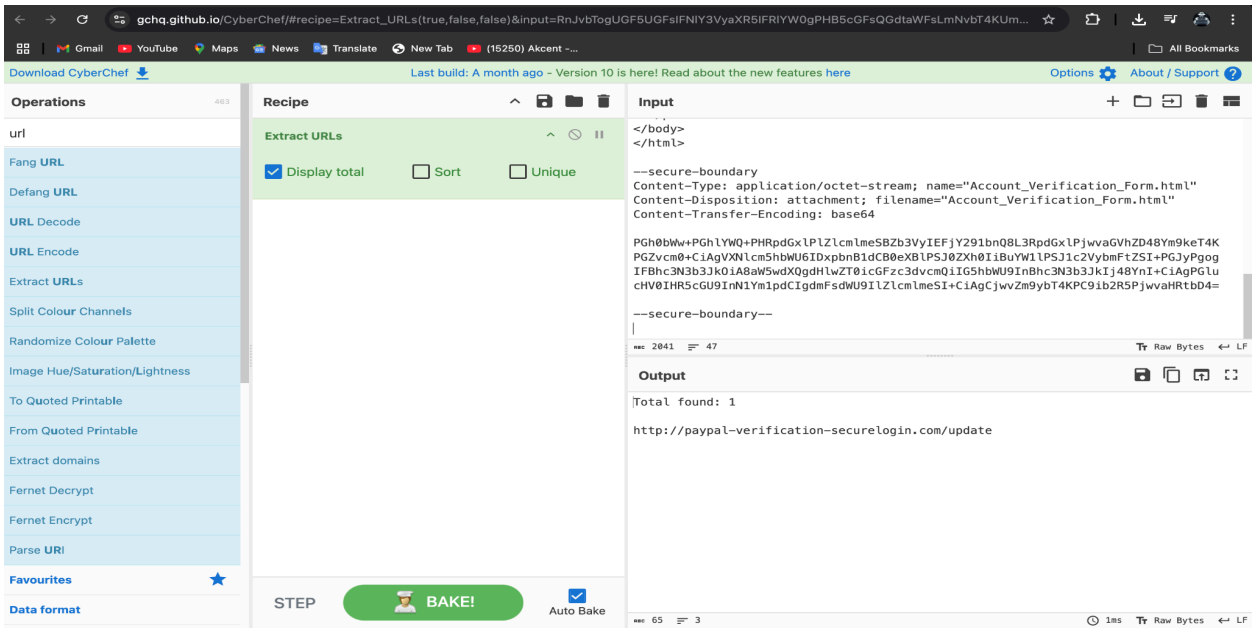


Scanning in Talos



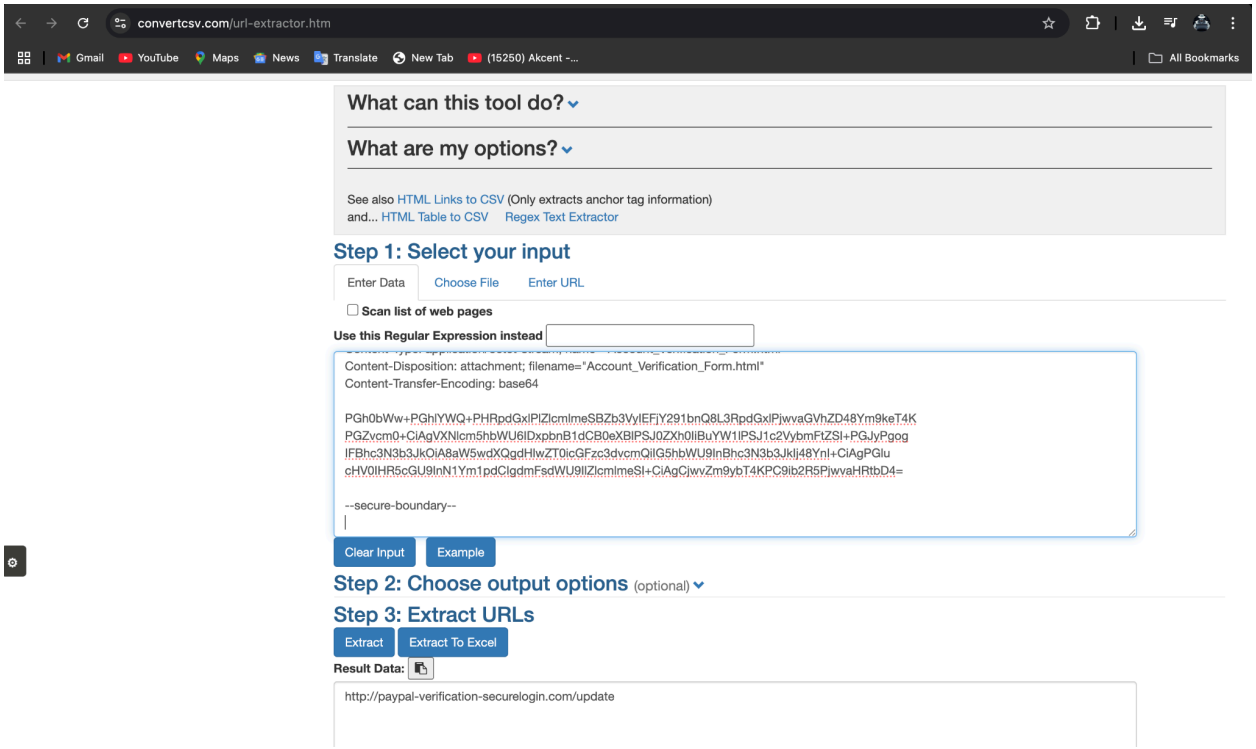
Scanned the Hash in vt - No threat detected

- Examining Malicious URL [redacted]
  - Copy and paste the HTML source code on cyberchef to get hidden URL
  - Make sure you defang it when you use URL or IP

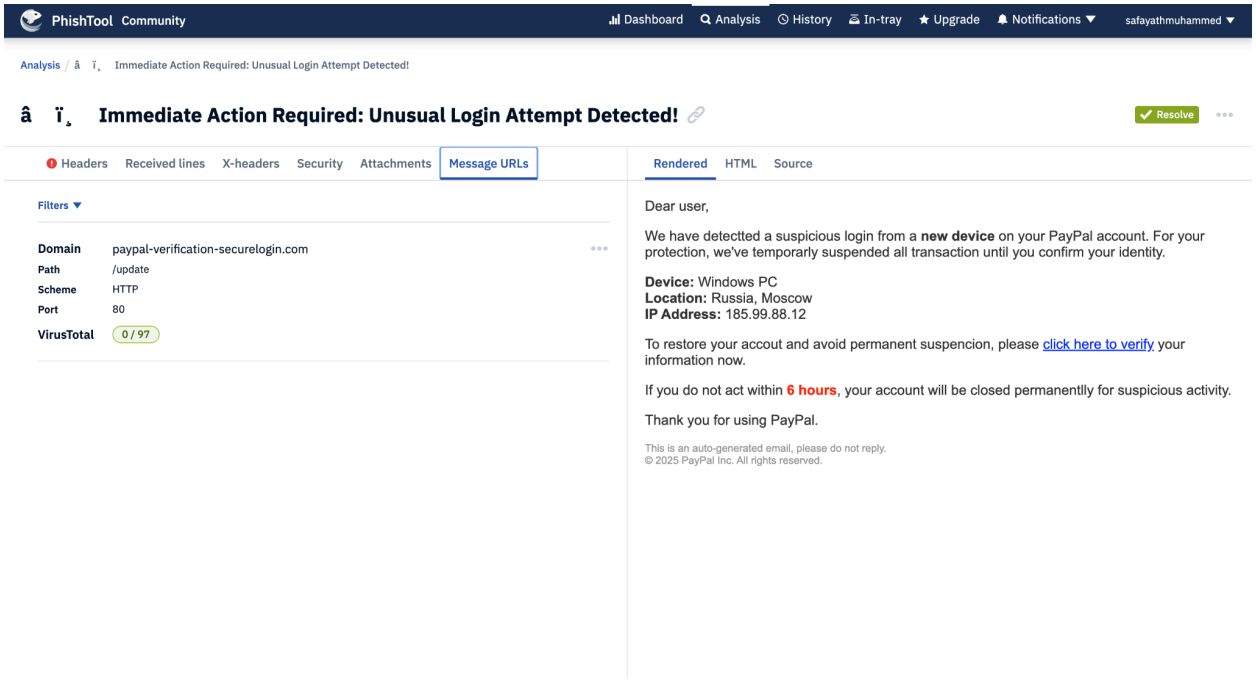


Cyberchef

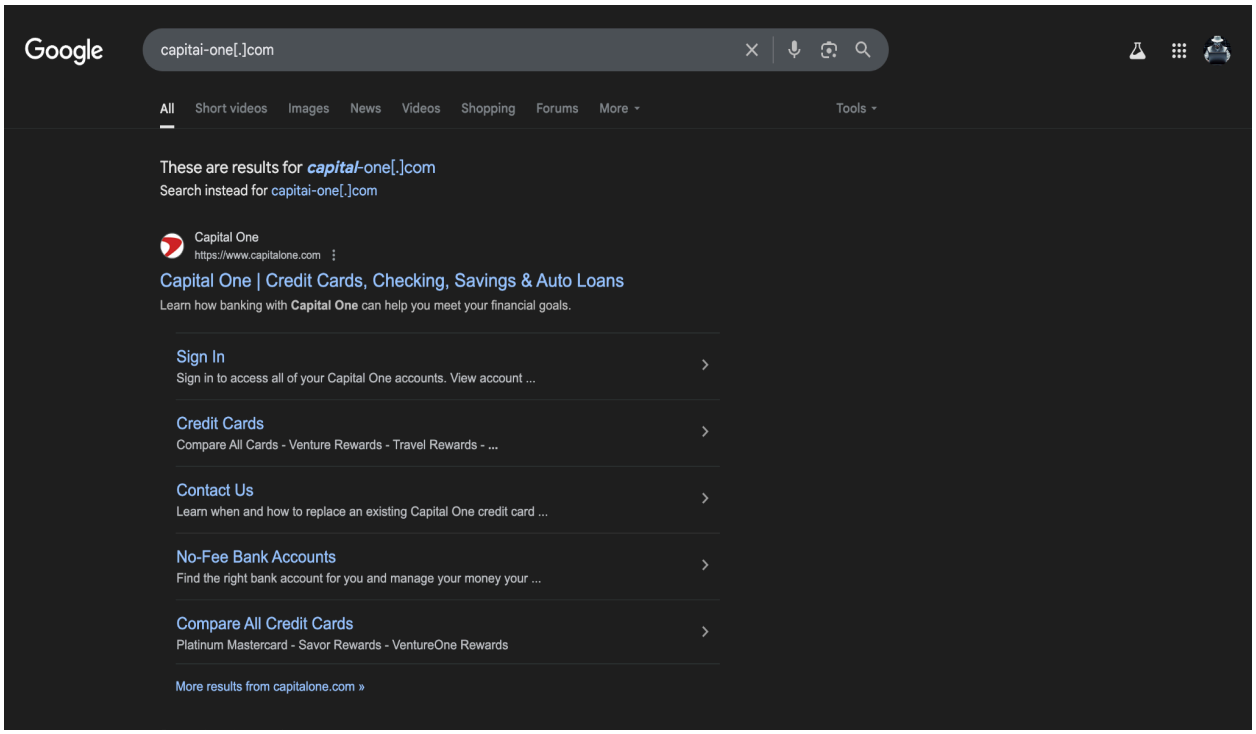
- You can also use this website - https://convertcsv.com/url-extractor.htm



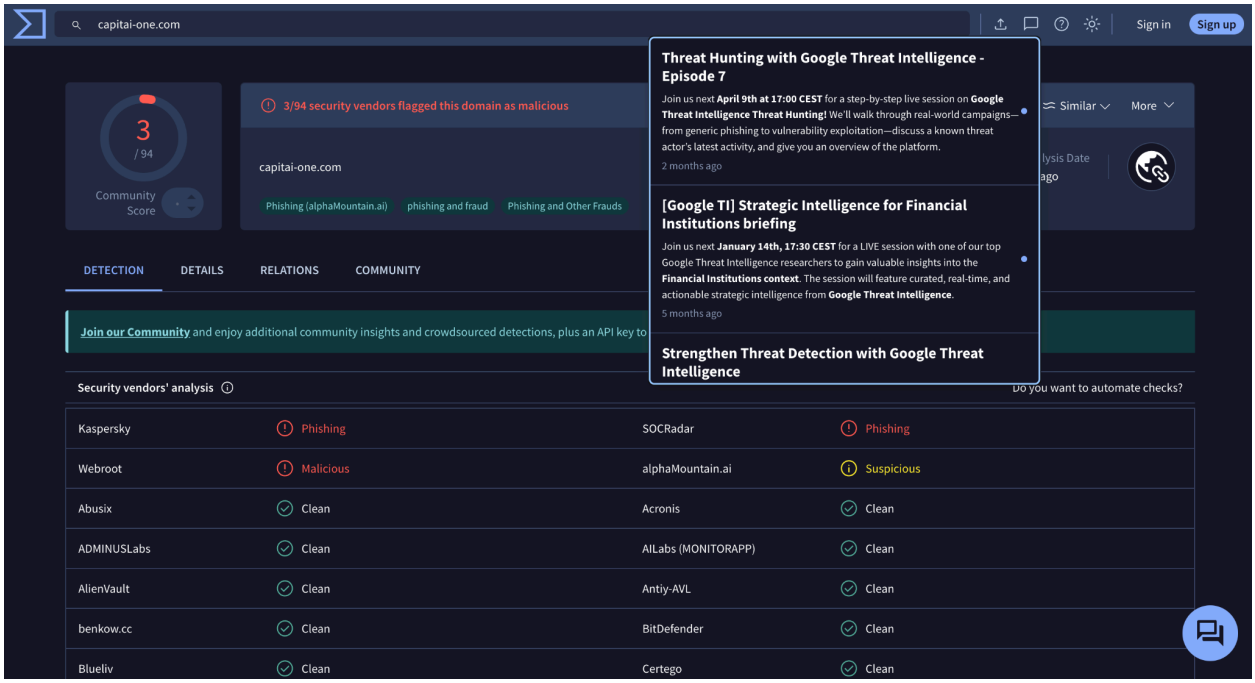
Yes, as an all in one tool Phish tool can provide these details also , but depending on only one tool is not recommended as a security professional .



So now we got the malicious link attacked in this mail - but I have tested it and confirmed it is not malicious , but I can prove how it looks when a malicious email is detected and how to detect it on another phishing email . look into the image below , make sure the url is defanged.

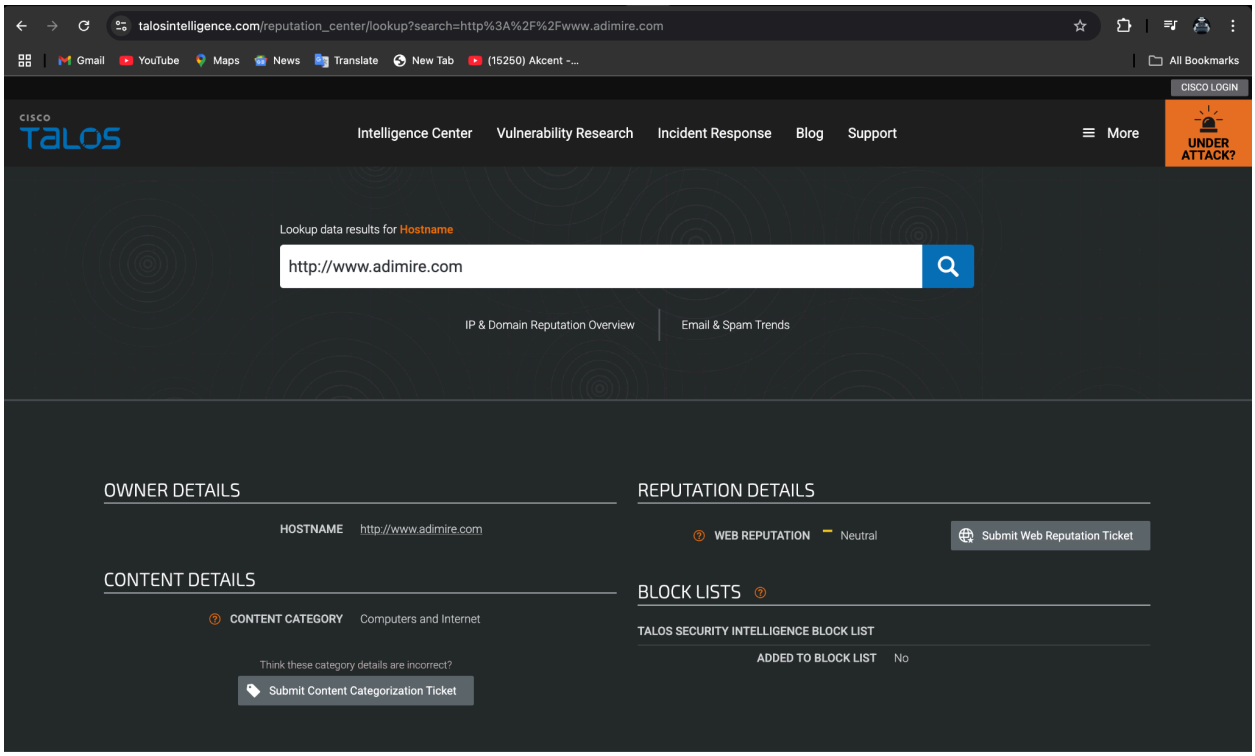


- So the Link is a luring link that looks legitimate to this banking site - interesting .
- Let us find the Url reputation -

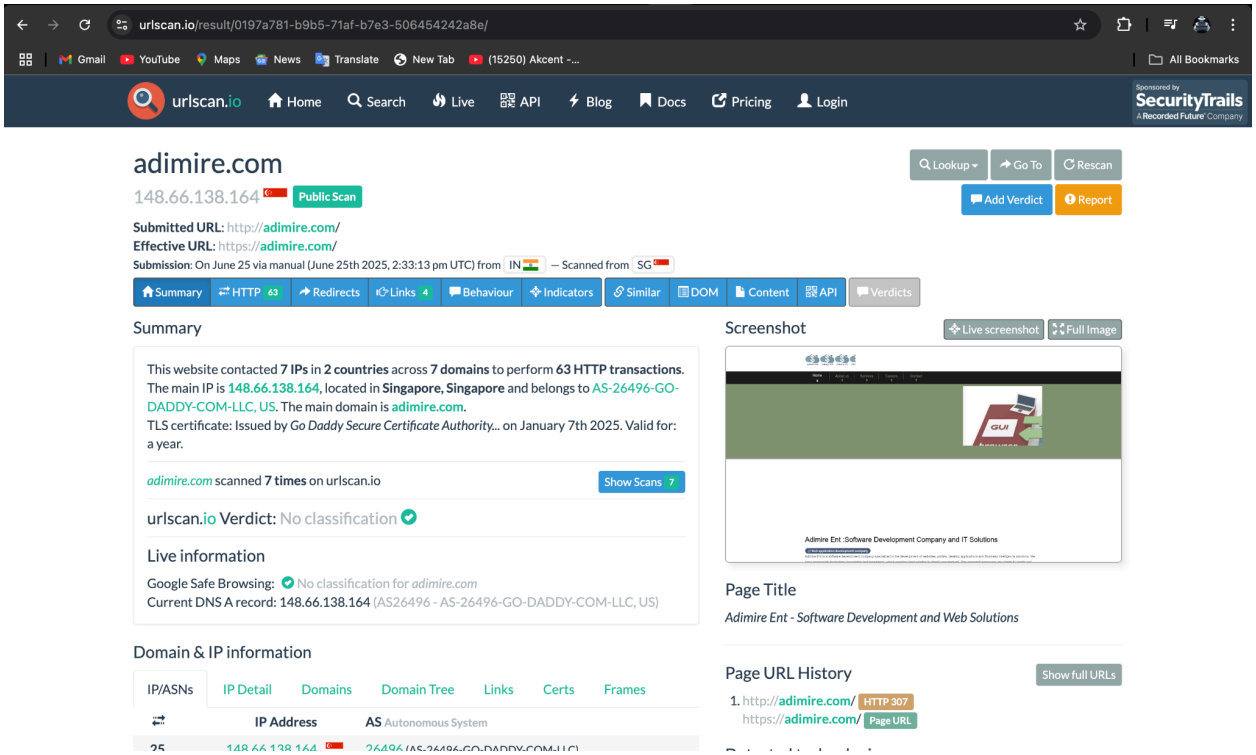


VT says it is absolutely suspicious .

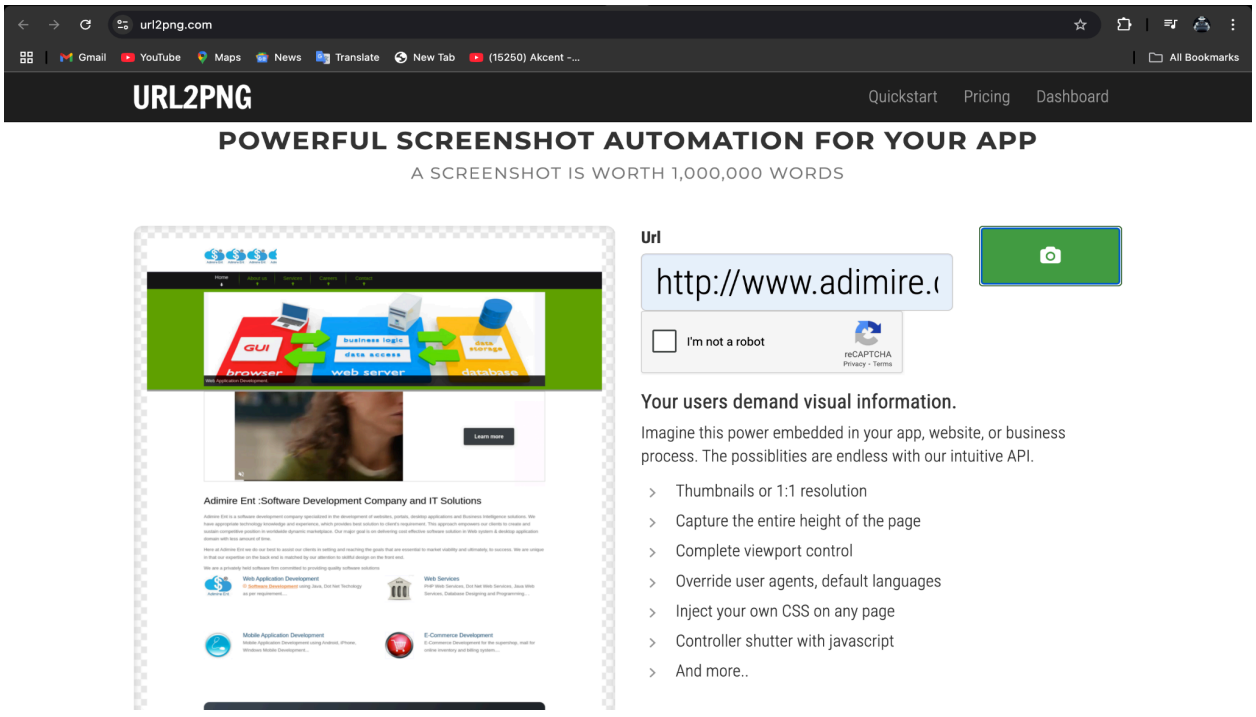
Use Cisco Talos also for URL reputation .



- A powerful tool for understanding the website from the suspicious URL - urlscan.io



This tool gives as much information as it can about the url , before clicking to any un trusted link do this check . It gives a screenshot of the website also , for screenshot we can use another tool also.

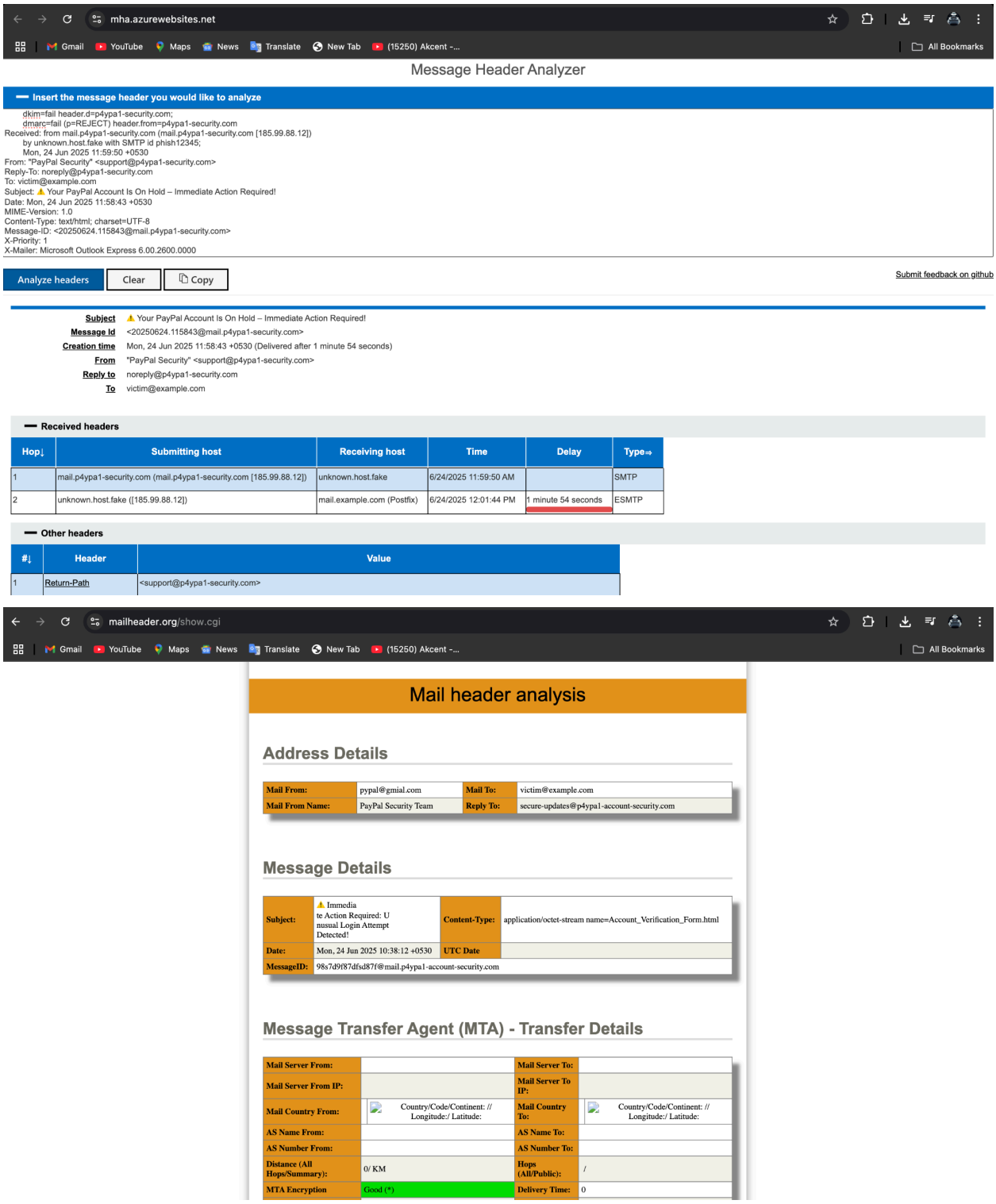


[url2png.com](url2png.com)

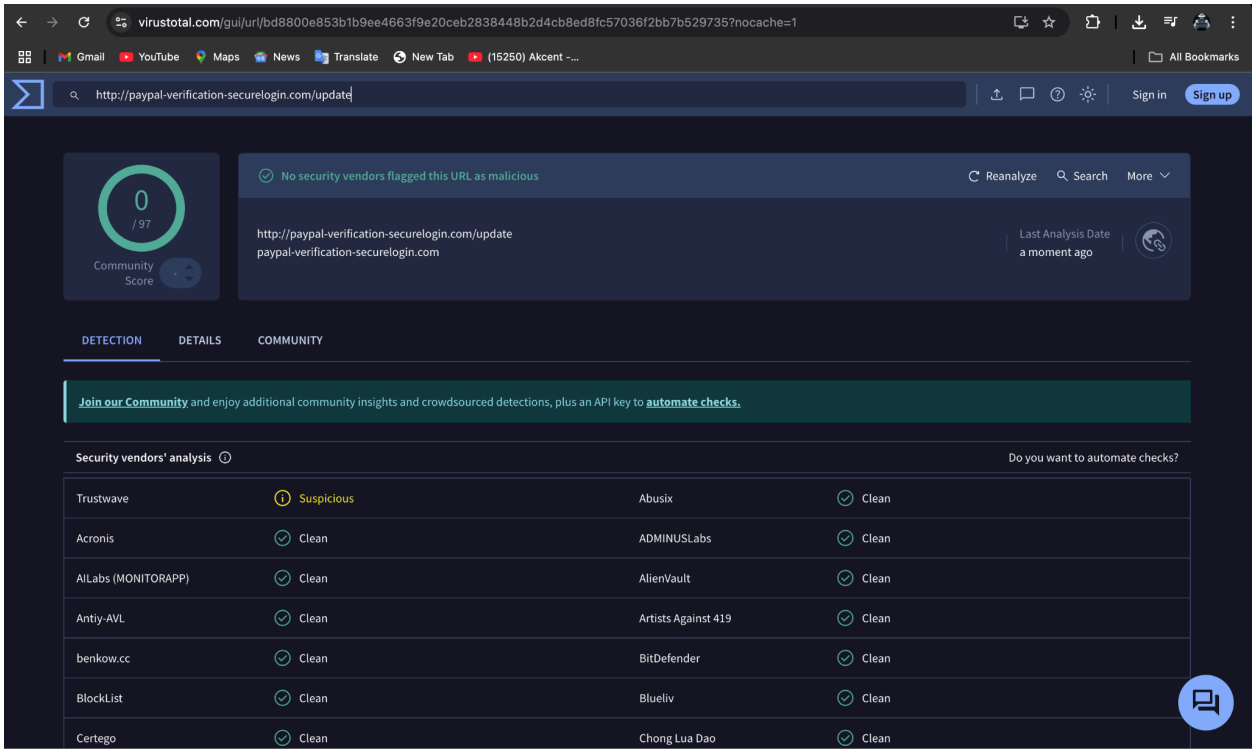
- Check the IP reputation also .
- If you are still in doubt about how we can extract all this data from the email header and source code use these tools also ➖

  1 - https://mha.azurewebsites.net/

  2 - mailheader.org



- I have mentioned above that the first email's suspicious link was not a threat because it does not exist in fact ,but the VT detected it may be a threat.



- Coming back to our paypal phishing email - we can see an Urgency tactic .

"If you do not act within **6 hours**, your account will be closed permanentlly for suspicious activity."

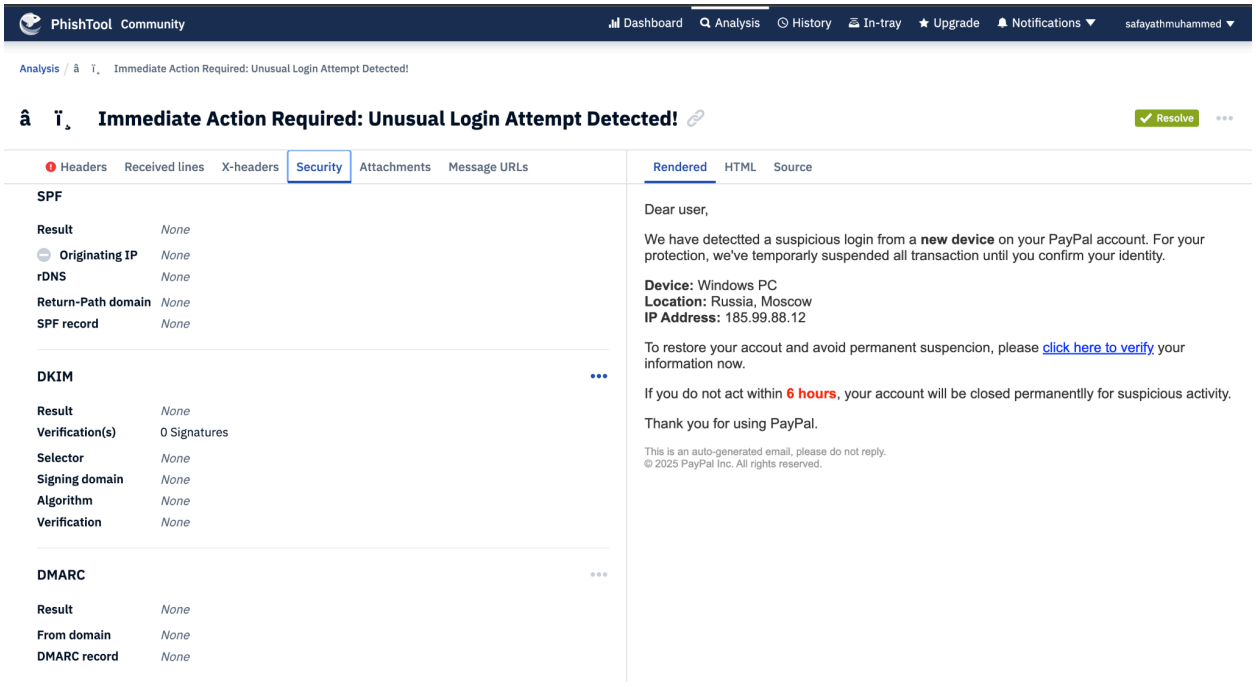
- Just read the phishing email carefully and you will see a lot of spelling mistakes.

Spelling mistakes

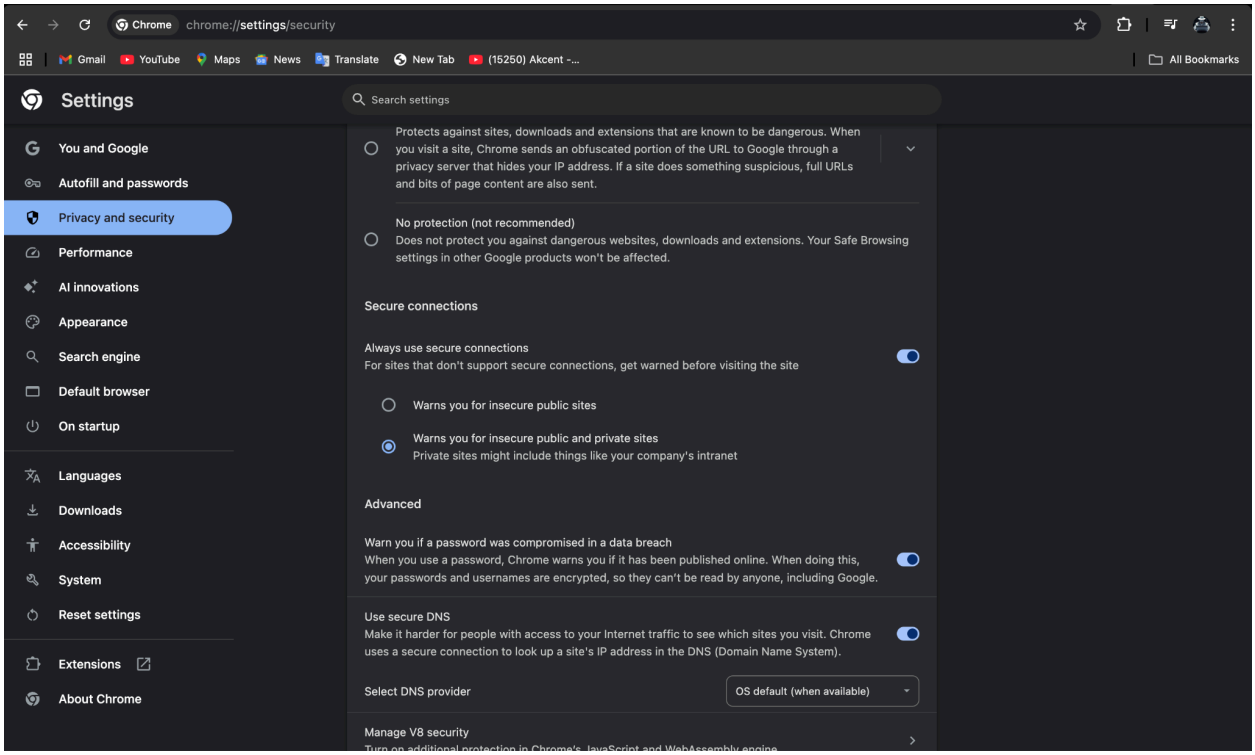
e.g., "detectted," "accout," "suspencion," "permanentlly"

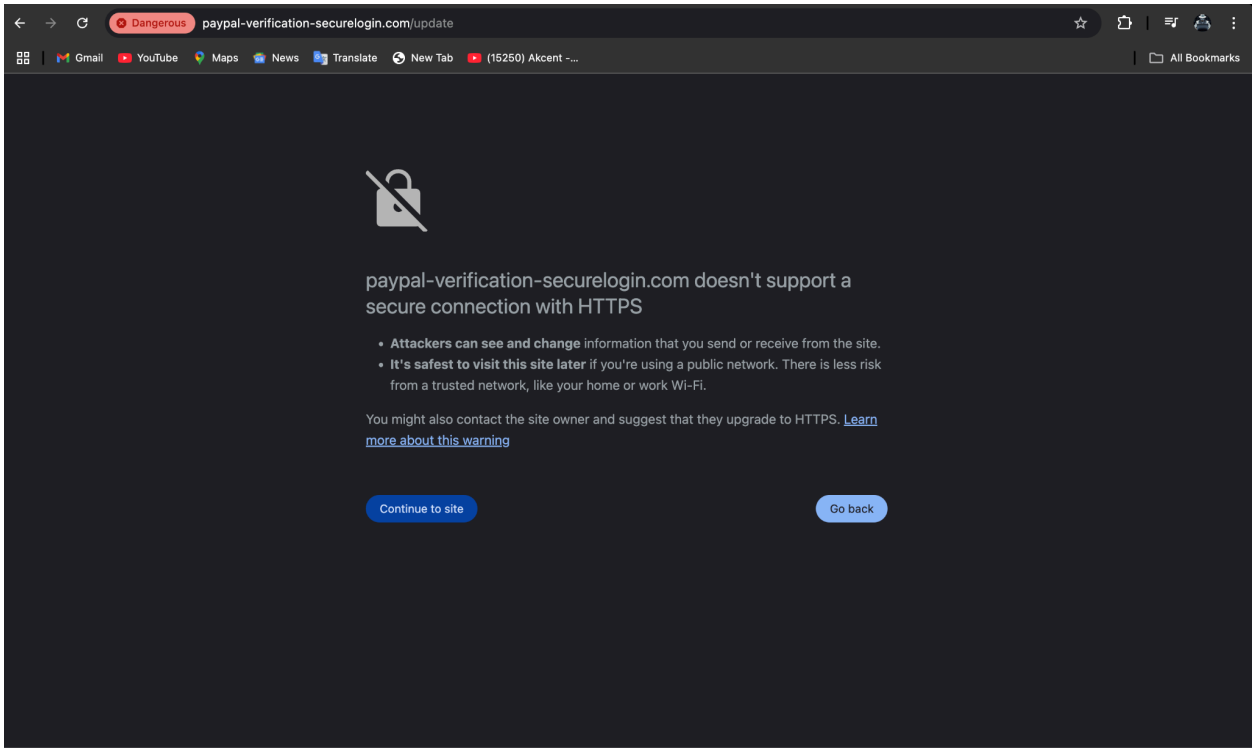
- Urgency and Spelling mistakes are signs of phishing attempts.
- And the another problem is no DKIM/DMARC/SPF

Phishtool :-

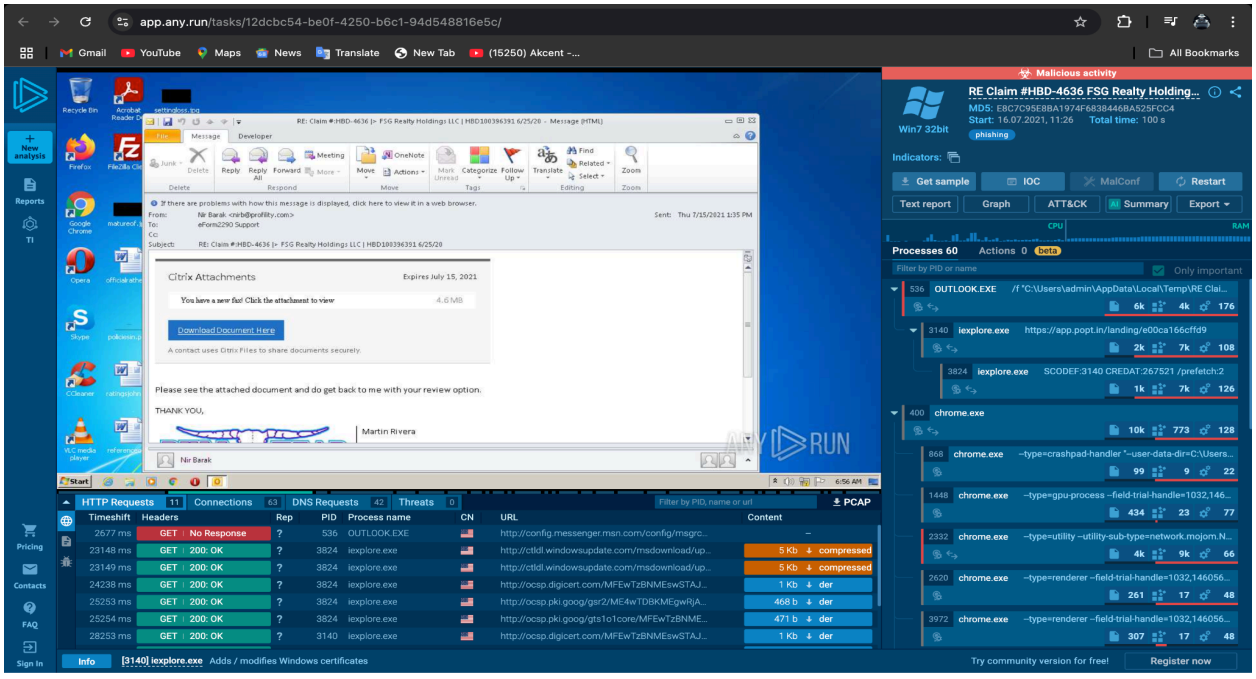


- Now how can we protect against mistaken clicking on suspicious url ?
  1 - Defang it - suspected[.]com
  2 - Use an updated browser and its security features(HSTS).



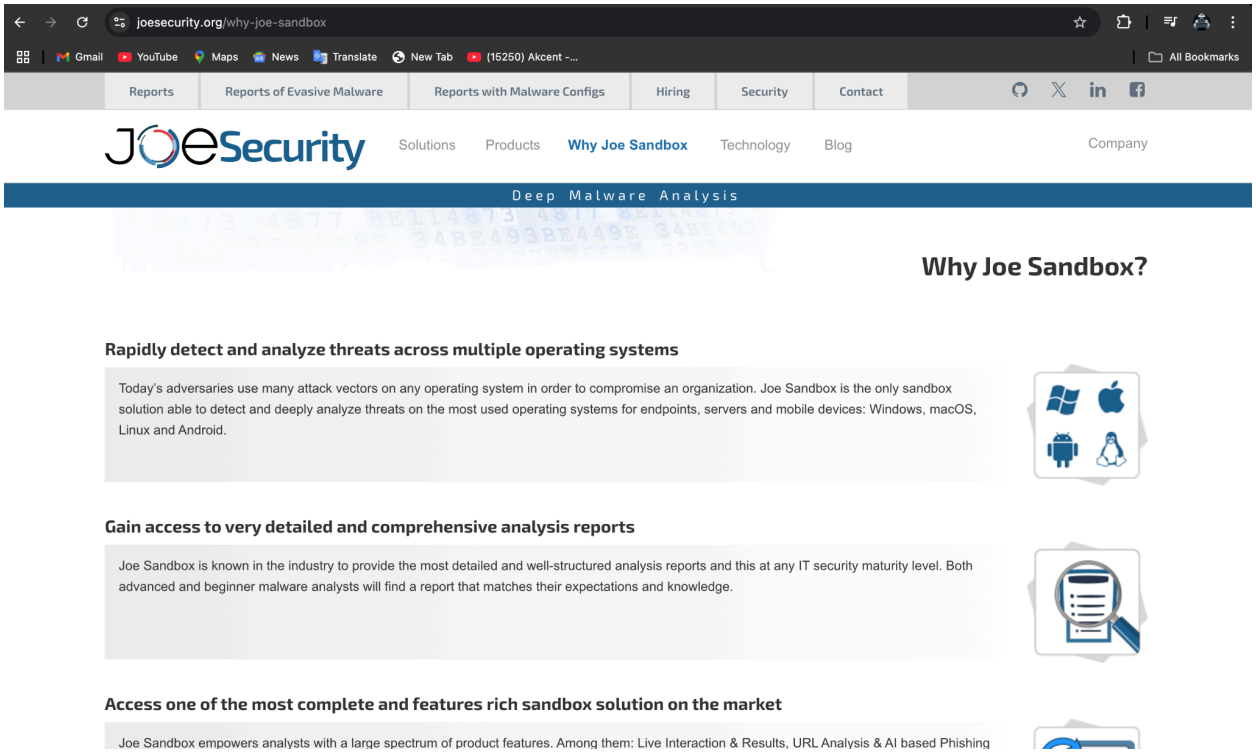


- Test the attachment in a sandbox environment like VT , Talos , Hybrid analysis , metadefender etc .
- Make sure you delete it if it is suspicious , if you forgot and later you mistakenly executed then you lost .
- Use any.run - a sandbox service for both study and analysis



Any.run

- Another tool with impressive features - joesecurity



  - Now let us make a table of what we found in this email , which in one look is legitimate but it is malicious and dangerous .

✅ What's Wrong Here (for your analysis report):

Phishing Technique	Description
Spoofed display name	`PayPal Security Team` looks trusted
Fake email	`pypal@gmial.com` mimics PayPal
Reply-To mismatch	Points to attacker domain: `p4ypa1-account-security.com`
Urgency	"Act within 6 hours or account will be closed"
Fear trigger	Claims suspicious login from Russia
Malicious URL	`http://paypal-verification-securelogin.com/update`

Hidden real URL	Hyperlinked as if legit (fake PayPal clone domain)
Spelling mistakes	e.g., “detectted,” “accout,” “suspencion,” “permanentlly”
Brand impersonation	Layout mimics PayPal
Attachment	`.html` form to collect credentials
Base64 encoded	Attachment encoded to hide intent
No DKIM/SPF	(simulate in your header analysis)