

PHISHING DETECTION

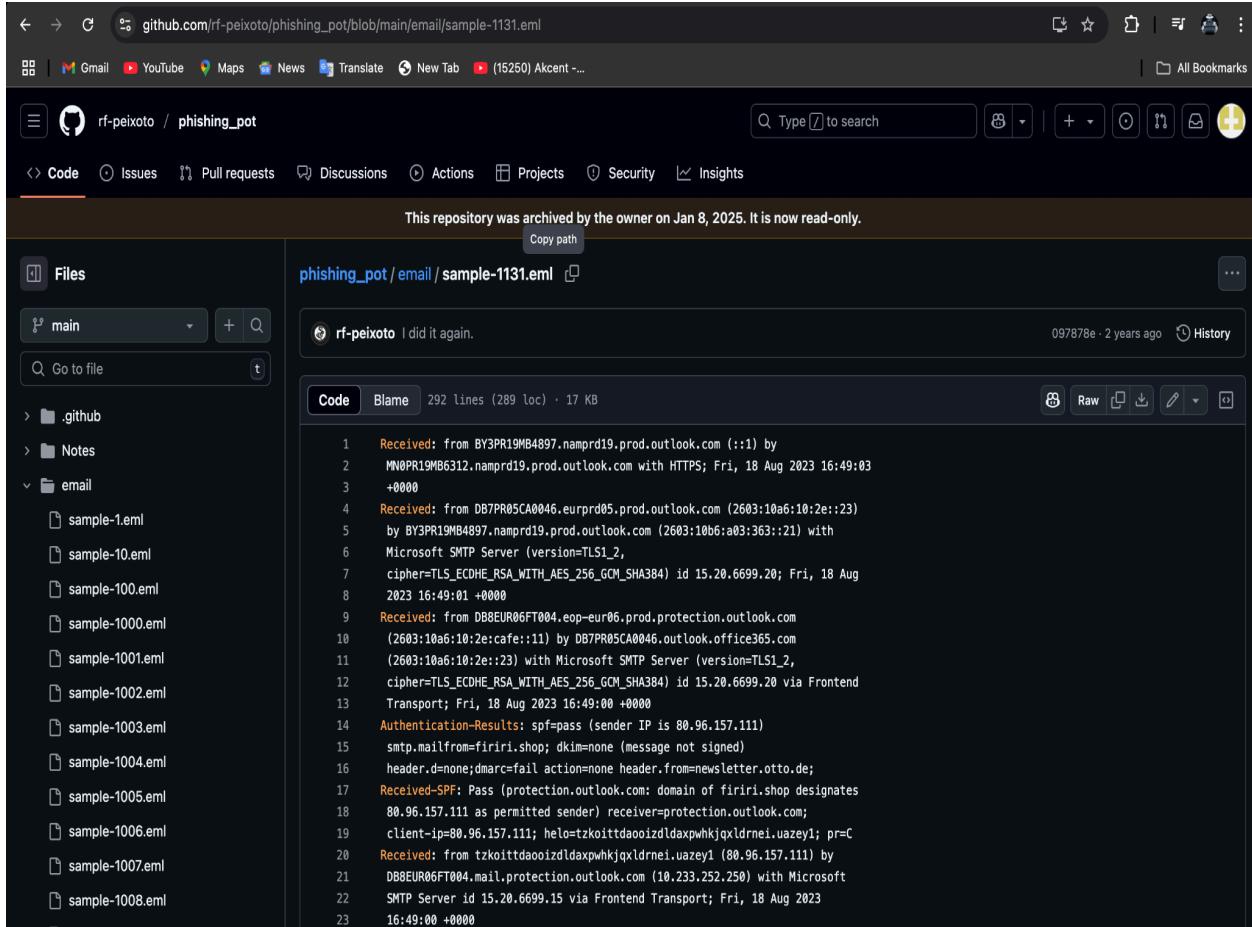
Hints/Mini Guide:

- 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 .

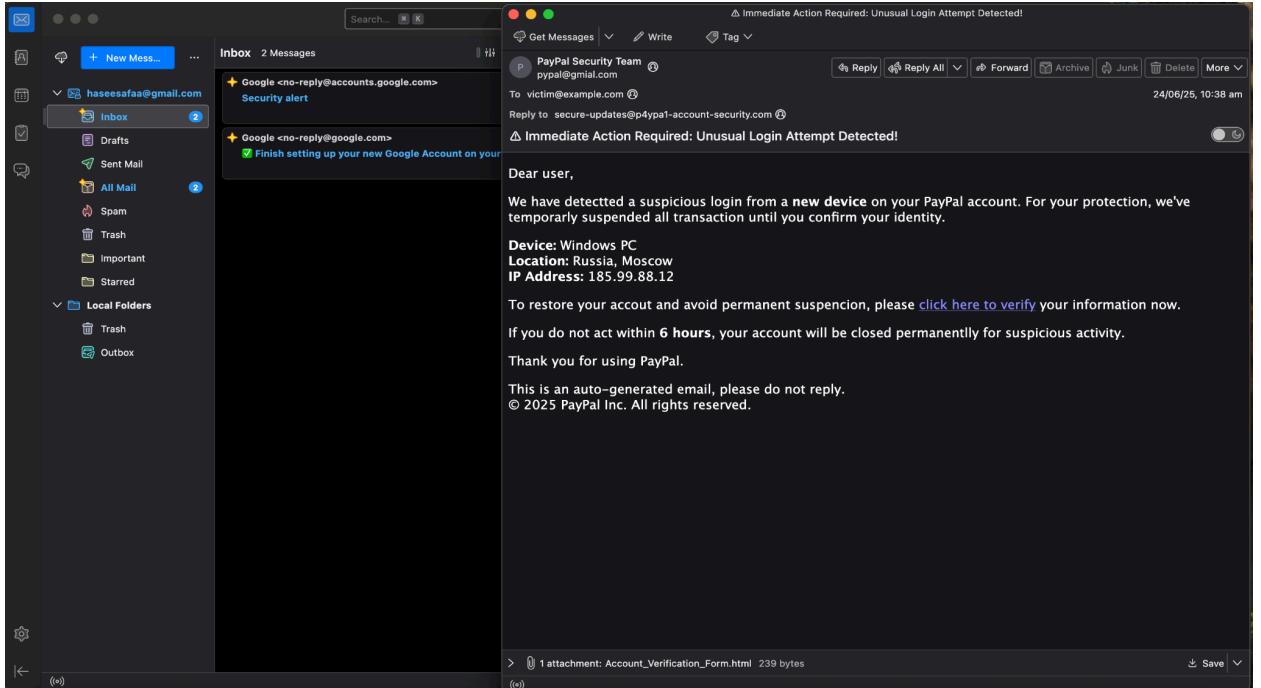


The screenshot shows a GitHub repository page for 'rf-peixoto/phishing_pot'. The repository has been archived by the owner on Jan 8, 2025, and is now read-only. The main directory 'main' contains several EML files, including 'sample-1.eml', 'sample-10.eml', 'sample-100.eml', 'sample-1000.eml', 'sample-1001.eml', 'sample-1002.eml', 'sample-1003.eml', 'sample-1004.eml', 'sample-1005.eml', 'sample-1006.eml', 'sample-1007.eml', and 'sample-1008.eml'. A specific file, 'sample-1131.eml', is selected and displayed in the code editor. The code content is as follows:

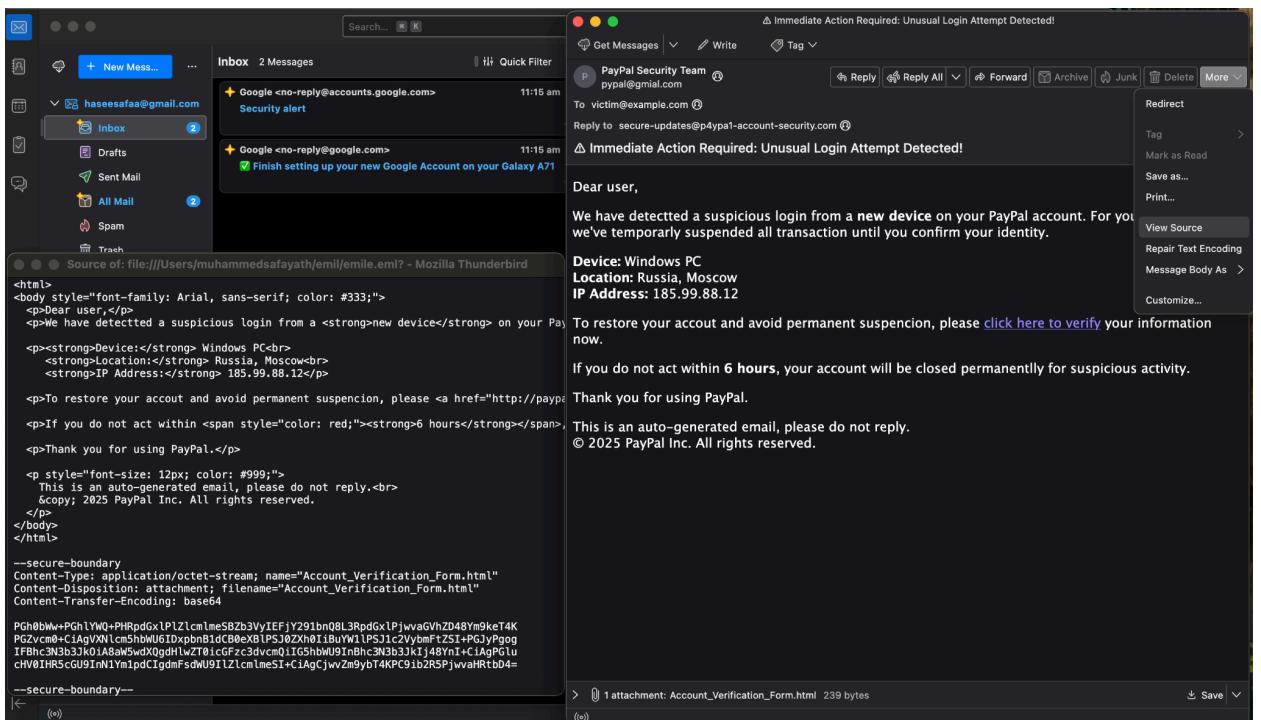
```
1 Received: from BY3PR19MB6312.namprd19.prod.outlook.com (::1) by
2 MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Fri, 18 Aug 2023 16:49:03
3 +0000
4 Received: from DB7PR05CA0046.eurprd05.prod.outlook.com (2603:10a6:10:2e::23)
5 by BY3PR19MB6312.namprd19.prod.outlook.com (2603:10b6:a03:363::21) with
6 Microsoft SMTP Server (version=TLS1_2,
7 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6699.20; Fri, 18 Aug
8 2023 16:49:01 +0000
9 Received: from DB8EUR06FT004.eop-eur06.prod.protection.outlook.com
10 (2603:10a6:10:2e:cafe::11) by DB7PR05CA0046.outlook.office365.com
11 (2603:10a6:10:2e::23) with Microsoft SMTP Server (version=TLS1_2,
12 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6699.20 via Frontend
13 Transport; Fri, 18 Aug 2023 16:49:00 +0000
14 Authentication-Results: spf=pass (sender IP is 80.96.157.111)
15 smtp.mailfrom=firiri.shop; dkim=none (message not signed)
16 header.d=none; dmarc=fail action=none header.from=newsletter.otto.de;
17 Received-SPF: Pass (protection.outlook.com: domain of firiri.shop designates
18 80.96.157.111 as permitted sender) receiver=protection.outlook.com;
19 client-ip=80.96.157.111; helo=tzkoittdaooizldaxpwhkjxldrnei.uazey1; pr=C
20 Received: from tzkoittdaooizldaxpwhkjxldrnei.uazey1 (80.96.157.111) by
21 DB8EUR06FT004.mail.protection.outlook.com (10.233.252.250) with Microsoft
22 SMTP Server id 15.20.6699.15 via Frontend Transport; Fri, 18 Aug 2023
23 16:49:00 +0000
```

- 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

The screenshot shows a browser window for 'app.phishtool.com/analysis/685bf766c319d604d416ff48'. The title bar says 'Analysis / Immediate Action Required: Unusual Login Attempt Detected!'. The main content area has a heading 'Immediate Action Required: Unusual Login Attempt Detected!' with a link to 'Resolve'. Below this, there are two tabs: 'Headers' (selected) and 'Rendered'. The 'Headers' tab lists various email headers with their values. The 'Rendered' tab shows the raw message content, which is a template for a PayPal phishing email. It includes sections for the user, device information, and instructions for account recovery.

Headers	Received lines	X-headers	Security	Attachments	Message URLs	Rendered	HTML	Source
From	pypal@gmial.com					Dear user,		
Display name	PayPal Security Team					We have detected a suspicious login from a new device on your PayPal account. For your protection, we've temporarily suspended all transaction until you confirm your identity.		
Sender	<i>None</i>					Device: Windows PC		
To	victim@example.com					Location: Russia, Moscow		
CC	<i>None</i>					IP Address: 185.99.88.12		
In-Reply-To	<i>None</i>					To restore your account and avoid permanent suspension, please click here to verify your information now.		
Timestamp	10:38 am, Jun 24th 2025					If you do not act within 6 hours , your account will be closed permanently for suspicious activity.		
Reply-To	secure-updates@p4ypa1-account-security.com					Thank you for using PayPal.		
Message-ID	<98s7d9f87dfsd87f@mail.p4ypa1-account-security.com>					This is an auto-generated email, please do not reply. © 2025 PayPal Inc. All rights reserved.		
Return-Path	<i>None</i>							
Originating IP	<i>None</i>							
rDNS	<i>None</i>							

Phishtool

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

The screenshot shows the 'Settings' page under 'Integrations'. The left sidebar has a 'VirusTotal API' section selected. The main content area has a heading 'VirusTotal API'. It explains how to integrate Phishtool with VirusTotal using a VirusTotal API key. A 'What is VirusTotal?' section provides a brief overview. Below this, a form allows users to enter their VirusTotal API key. A note about API quotas is displayed in a yellow box at the bottom.

Account	VirusTotal API
Profile	Integrate your Phishtool account with VirusTotal using a VirusTotal API key. Phishtool will use this key to automatically enrich your analysis. This integration does not submit files to VirusTotal.
► Security	
► Preferences	
▼ Integrations	
VirusTotal API	
Feedback	
► Legal	

What is VirusTotal? ▾
If you do not have a VirusTotal API key then you can [register with VirusTotal for free](#) and begin using a free limited API key with Phishtool immediately. Alternatively, you can take full advantage of VirusTotal and Phishtool with [VT ENTERPRISE license](#).

Your VirusTotal API Key*

Submit

VirusTotal API quotas
Some VirusTotal API keys are rate limited and/or subject to a quota. This integration will contribute to your API quota. You can contact VirusTotal to discuss increasing your API quota allowance.

PhishTool Community

Analysis / Immediate Action Required: Unusual Login Attempt Detected!

Immediate Action Required: Unusual Login Attempt Detected! 

Attachments

	File name	File type	File size	VirusTotal	File hashes	...
1	Account_Verification_Form.html	None	0.23 KB	No matches found	MD5: 34ba82fcacfc3c7340b31e72ececaa1b SHA-1: eb8ea2e509659f674af00a0ae6d31821e10daab37 SHA-256: cfed1a650d7709974f83488b0da48a891e08da7a8fa75f563048275a7b8658c3	Rendered HTML Source

Dear user,

We have detected a suspicious login from a **new device** on your PayPal account. For your protection, we've temporarily suspended all transaction until you confirm your identity.

Device: Windows PC
Location: Russia, Moscow
IP Address: 185.99.88.12

To restore your account and avoid permanent suspension, please [click here to verify](#) your information now.

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

Thank you for using PayPal.

This is an auto-generated email, please do not reply.
 © 2025 PayPal Inc. All rights reserved.

- 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

Sandbox ▾ Quick Scans ▾ File Collections Resources ▾ Request Info ▾

IP, Domain, Hash... More ▾

Analysis Overview

Submission name: Account_Verification_Form.html
 Size: 239B
 Type: [html](#)
 Mime: text/html
 SHA256: [cfed1a650d7709974f83488b0da48a891e08da7a8fa75f563048275a7b8658c3](#)
 Submitted At: 2025-06-25 14:18:43 (UTC)
 Last Anti-Virus Scan: 2025-06-25 14:18:43 (UTC)
 Last Sandbox Report: 2025-06-25 14:18:43 (UTC)

Anti-Virus Results

MetaDefender [🔗](#)
 Multi Scan Analysis

 Clean

[More Details](#)

Analysis Overview

no specific threat
 AV Detection: Marked as clean
 X Post ⌂ Link E-Mail
 0 Community Score 0

Back to top

Defend the endpoint. Join the world's most secure businesses on the first cloud-native endpoint protection platform built to stop breaches.

[Why CrowdStrike?](#)
[Access Falcon Prevent Free Trial](#)

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) = 34ba82fcacccf3c7340b31e72ececac1b
[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

The Cisco Talos Intelligence Group maintains a reputation disposition on billions of files. This reputation system is fed into the Cisco Secure Firewall, ClamAV, and Open-Source Snort product lines. The tool below allows you to do casual lookups against the Talos File Reputation system. This system limits you to one lookup at a time, and is limited to only hash matching.

Scanning in Talos

Security vendors' analysis		Do you want to automate checks?	
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	ALYac	Undetected
Anti-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected
CrowdStrike Falcon	Undetected	CTX	Undetected

Scanned the Hash in vt - No threat detected

- Examining Malicious URL ■

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

The screenshot shows the CyberChef web application. On the left, the 'Operations' sidebar lists various tools like Fang URL, Defang URL, URL Decode, URL Encode, Extract URLs, Split Colour Channels, Randomize Colour Palette, Image Hue/Saturation/Lightness, To Quoted Printable, From Quoted Printable, Extract domains, Fernet Decrypt, Fernet Encrypt, Parse URI, and Favourites. The main area has tabs for 'Recipe' (Extract URLs) and 'Input'. The 'Input' tab contains the following text:

```

</body>
</html>

--secure-boundary
Content-Type: application/octet-stream; name="Account_Verification_Form.html"
Content-Disposition: attachment; filename="Account_Verification_Form.html"
Content-Transfer-Encoding: base64
PGh0bWw+PGh1YWQ+PHRpdGx1PlZlcmImeSBzb3VyIEFjY291bnQ8L3RpGxlpjwvaGVhZD48Ym9keT4K
PGZvcm0+CiAgVXNlcm5hbWU6IDxpbnB1dCB0eXBpSj02Xh01ibuyW1lPSj1c2VybmtZSI+PGJyPgog
IFBhc3N3b3JkO1A8aw5wdxQgdHlwZT0icGFzc3dvcmQiiG5hbWl9InBh3N3b3JkIj48YnI+CiAgPGlu
chV0IHR5cGU9InN1Ym1pdClgdmFsdWU91lZlcmImeSI+CiAgCjwvZm9ybT4KPC91b2R5PjwvaHRtbD4=
--secure-boundary--
|
```

The 'Output' tab shows the result: "Total found: 1" and the URL "http://paypal-verification-securelogin.com/update".

Cyberchef

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

The screenshot shows the 'convertcsv.com/url-extractor.htm' website. It has sections for 'What can this tool do?' and 'What are my options?'. Under 'Step 1: Select your input', there are tabs for 'Enter Data', 'Choose File', and 'Enter URL'. A checkbox for 'Scan list of web pages' is checked. Below is a text area containing the same base64-encoded HTML payload as the CyberChef screenshot. Buttons at the bottom include 'Clear Input', 'Example', 'Step 2: Choose output options (optional)', 'Step 3: Extract URLs', 'Extract', 'Extract To Excel', and 'Result Data'.

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 .

The screenshot shows the PhishTool Community dashboard. At the top, there are navigation links: Dashboard, Analysis, History, In-tray, Upgrade, Notifications, and a user profile for 'safayathmuhammed'. Below the header, a message reads: 'Analysis / Immediate Action Required: Unusual Login Attempt Detected!'. There is a green 'Resolve' button with a checkmark. The main content area has tabs for Headers, Received lines, X-headers, Security, Attachments, and 'Message URLs' (which is selected). On the left, there are filters and a summary of the detected URL: Domain - paypal-verification-securelogin.com, Path - /update, Scheme - HTTP, Port - 80, and VirusTotal score - 0/97. The main body of the message contains a warning to the user about a suspicious login from a new device, temporary account suspension, and instructions to click a link to verify their identity. It also states that if no action is taken within 6 hours, the account will be closed permanently. The message concludes with a note that it is auto-generated and includes a copyright notice for PayPal.

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.

The screenshot shows a Google search results page for the query 'capital-one[.]com'. The search bar at the top contains the query. Below the search bar, there are standard search filters: All, Short videos, Images, News, Videos, Shopping, Forums, More, and Tools. The main content area displays search results for Capital One. The first result is the official Capital One website, featuring the logo and the text 'Capital One | Credit Cards, Checking, Savings & Auto Loans'. Below the result, there are several links: 'Sign In', 'Credit Cards', 'Contact Us', 'No-Fee Bank Accounts', and 'Compare All Credit Cards'. Each link has a brief description and a right-pointing arrow indicating it leads to more information or a specific page. At the bottom of the search results, there is a link to 'More results from capitalone.com'.

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

The screenshot shows the VirusTotal domain analysis page for `capitaI-one.com`. Key findings include:

- Community Score:** 3 / 94
- Malicious Flags:** 3/94 security vendors flagged this domain as malicious.
- Category:** Phishing (alphaMountain.ai), phishing and fraud, Phishing and Other Frauds
- Detection:** Security vendors' analysis results:

VirusTotal	Category	SOCRadar	Category
Kaspersky	Phishing		Phishing
Webroot	Malicious	alphaMountain.ai	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
benkow.cc	Clean	BitDefender	Clean
Blueliv	Clean	Certego	Clean

VT says it is absolutely suspicious .

Use Cisco Talos also for URL reputation .

The screenshot shows the Cisco Talos Reputation Center for the URL `http://www.adimire.com`. Key details include:

- OWNER DETAILS:** Hostname: `http://www.adimire.com`
- CONTENT DETAILS:** Content Category: Computers and Internet
- REPUTATION DETAILS:** Web Reputation: Neutral
- BLOCK LISTS:** TALOS SECURITY INTELLIGENCE BLOCK LIST
- OTHER:** Under Attack indicator, Submit Web Reputation Ticket, Submit Content Categorization Ticket buttons.

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

The screenshot shows the urlscan.io interface for the URL adimire.com. Key details include:

- Submitted URL:** <http://adimire.com/>
- Effective URL:** <https://adimire.com/>
- Submission:** On June 25 via manual (June 25th 2025, 2:33:13 pm UTC) from IN (Singapore) - Scanned from SG (Singapore)
- Summary:** This website contacted 7 IPs in 2 countries across 7 domains to perform 63 HTTP transactions. The main IP is 148.66.138.164, located in Singapore, Singapore and belongs to AS-26496-GO-DADDY-COM-LLC, US. The main domain is adimire.com.
- Verdict:** No classification
- Domain & IP information:** IP Address: 148.66.138.164, AS Autonomous System: AS26496 - GO-DADDY-COM-LLC, US.
- Screenshot:** Shows a screenshot of the Adimire Ent website with a green header and a logo.

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.

The screenshot shows the url2png.com interface. Key features displayed include:

- POWERFUL SCREENSHOT AUTOMATION FOR YOUR APP**
- A SCREENSHOT IS WORTH 1,000,000 WORDS**
- Url:** <http://www.adimire.com>
- reCAPTCHA:** I'm not a robot
- Your users demand visual information.**
- Imagine this power embedded in your app, website, or business process. The possibilities are endless with our intuitive API.**
- Features listed:**
 - > Thumbnails or 1:1 resolution
 - > Capture the entire height of the page
 - > Complete viewport control
 - > Override user agents, default languages
 - > Inject your own CSS on any page
 - > Controller shutter with javascript
 - > And more..

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

Message Header Analyzer

Insert the message header you would like to analyze

```
dkim=fail header.d=p4ypa1-security.com;
dmarc=fail (p=REJECT) header.from=p4ypa1-security.com
Received: from mail.p4ypa1-security.com ([185.99.88.12])
by mx.google.com with SMTP id phish12345
Mon, 24 Jun 2025 11:59:50 -0530
From: "PayPal Security" <support@p4ypa1-security.com>
Reply-To: noreply@p4ypa1-security.com
To: victim@example.com
Subject: ⚠ Your PayPal Account Is On Hold – Immediate Action Required!
Date: Mon, 24 Jun 2025 11:58:43 +0530
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Message-ID: <20250624.115843@mail.p4ypa1-security.com>
X-Priority: 1
X-Mailer: Microsoft Outlook Express 6.0.2600.0000
```

Analyze headers | Clear | Copy | Submit feedback on GitHub

Subject: ⚠ Your PayPal Account Is On Hold – Immediate Action Required!

Message Id: <20250624.115843@mail.p4ypa1-security.com>

Creation time: Mon, 24 Jun 2025 11:58:43 +0530 (Delivered after 1 minute 54 seconds)

From: "PayPal Security" <support@p4ypa1-security.com>

Reply to: noreply@p4ypa1-security.com

To: victim@example.com

Received headers

Hop↓	Submitting host	Receiving host	Time	Delay	Type⇒
1	mail.p4ypa1-security.com (mail.p4ypa1-security.com [185.99.88.12])	unknown.host.fake	6/24/2025 11:59:50 AM		SMTP
2	unknown.host.fake ([185.99.88.12])	mail.example.com (Postfix)	6/24/2025 12:01:44 PM	1 minute 54 seconds	ESMTP

Other headers

#↓	Header	Value
1	Return-Path	<support@p4ypa1-security.com>

Mail header analysis

Address Details

Mail From:	pypal@gmail.com	Mail To:	victim@example.com
Mail From Name:	PayPal Security Team	Reply To:	secure-updates@p4ypa1-account-security.com

Message Details

Subject:	⚠ Immediate Action Required: Unusual Login Attempt Detected!	Content-Type:	application/octet-stream name=Account_Verification_Form.html
Date:	Mon, 24 Jun 2025 10:38:12 +0530	UTC Date:	
MessageID:	98s7d9f87dfs87f@mail.p4ypa1-account-security.com		

Message Transfer Agent (MTA) - Transfer Details

Mail Server From:		Mail Server To:	
Mail Server From IP:		Mail Server To IP:	
Mail Country From:		Country/Code/Continent: // Longitude/ Latitude:	
AS Name From:		AS Name To:	
AS Number From:		AS Number To:	
Distance (All Hops/Summary):	0/ KM	Hops (All/Public):	/
MTA Encryption:	Good (*)	Delivery Time:	0

- 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.

Security vendor	Result
Trustwave	Suspicious
Acronis	Clean
AILabs (MONITORAPP)	Clean
Antiy-AVL	Clean
benkow.cc	Clean
BlockList	Clean
Certego	Clean
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Artists Against 419	Clean
BitDefender	Clean
Blueliv	Clean
Chong Lua Dao	Clean

- 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 permanently for suspicious activity."

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

Spelling mistakes

e.g., "detectedt," "accout," "suspencion," "permanently"

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

Phishtool :-

PhishTool Community

Analysis / Immediate Action Required: Unusual Login Attempt Detected!

Immediate Action Required: Unusual Login Attempt Detected!

Headers Received lines X-headers **Security** Attachments Message URLs

Rendered HTML Source

SPF

Result None
 Originating IP None
rDNS None
Return-Path domain None
SPF record None

DKIM

Result None
Verification(s) 0 Signatures
Selector None
Signing domain None
Algorithm None
Verification None

DMARC

Result None
From domain None
DMARC record None

Dear user,

We have detected a suspicious login from a **new device** on your PayPal account. For your protection, we've temporarily suspended all transaction until you confirm your identity.

Device: Windows PC
Location: Russia, Moscow
IP Address: 185.99.88.12

To restore your account and avoid permanent suspension, please [click here to verify](#) your information now.

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

Thank you for using PayPal.

This is an auto-generated email, please do not reply.
 © 2025 PayPal Inc. All rights reserved.

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

chrome://settings/security

Settings Search settings

Privacy and security

- Protects against sites, downloads and extensions that are known to be dangerous. When you visit a site, Chrome sends an obfuscated portion of the URL to Google through a privacy server that hides your IP address. If a site does something suspicious, full URLs and bits of page content are also sent.
- No protection (not recommended)

Secure connections

Always use secure connections For sites that don't support secure connections, get warned before visiting the site

- Warns you for insecure public sites
- Warns you for insecure public and private sites Private sites might include things like your company's intranet

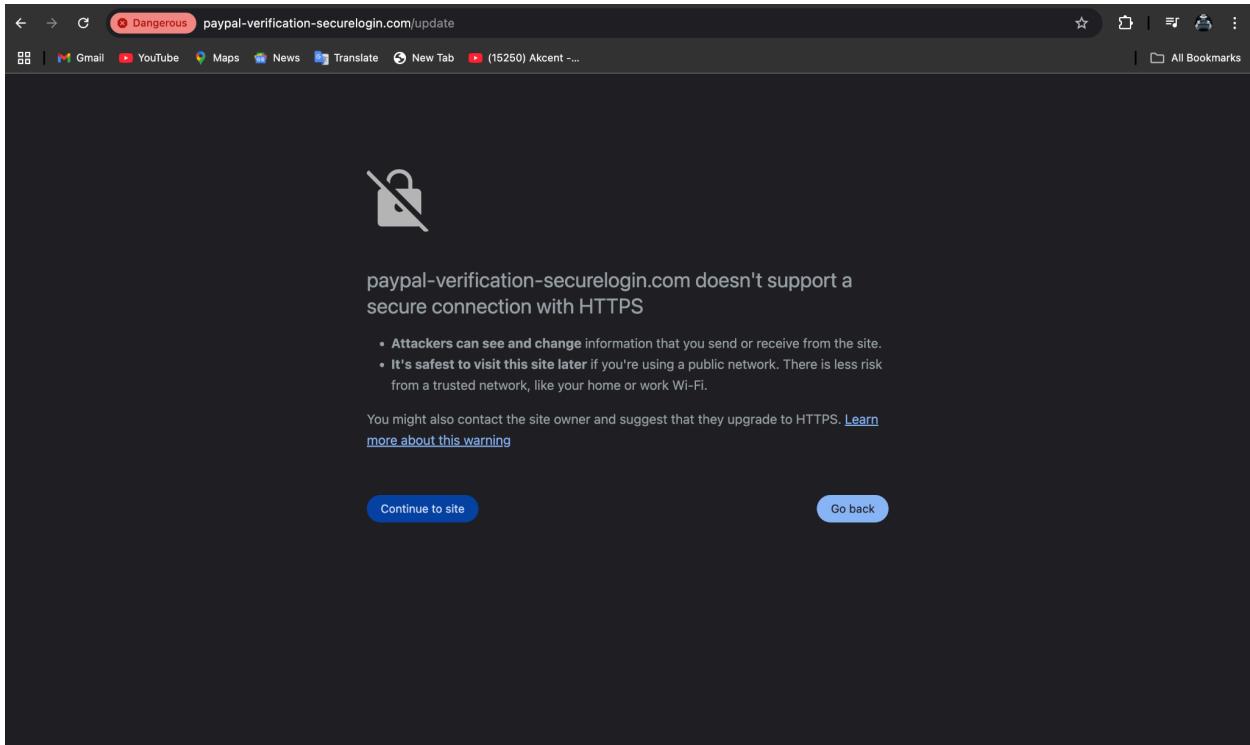
Advanced

Warn you if a password was compromised in a data breach When you use a password, Chrome warns you if it has been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.

Use secure DNS Make it harder for people with access to your Internet traffic to see which sites you visit. Chrome uses a secure connection to look up a site's IP address in the DNS (Domain Name System).

Select DNS provider OS default (when available)

Manage V8 security Turn on additional protection in Chrome's JavaScript and WebAssembly engine >



- 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

app.any.run/tasks/12dcbe54-be0f-4250-b6c1-94d548816e5c/

RE: Claim #HBD-4636 FSG Realty Holdings... [REDACTED] 6/25/2021 - Message (HTML)

From: Nr Barak <nrbarak@paypal.com>

To: [REDACTED]

Subject: RE: Claim #HBD-4636 [REDACTED] FSG Realty Holdings LLC | HBD103394391 6/25/2021

Expires July 15, 2021

Download Document Here

Please see the attached document and do get back to me with your review option.

THANK YOU,

Martin Rivera

Nr Barak

HTTP Requests 11 Connections 63 DNS Requests 42 Threats 0

PCAP

Process 536 OUTLOOK.EXE /C:/Users/admin/AppData/Local/Temp/RE Cl... 3140 iexplore.exe https://app.popit.in/landing/e00ca166cfdf9 3824 iexplore.exe SCODEF:3140 CREDAT:267521/prefetch:2 400 chrome.exe 868 chrome.exe -type=crashpad-handler -user-data-dir=C:/Users... 1448 chrome.exe -type=gpu-process -field-trial-handle=1032:146056... 2332 chrome.exe -type=utility -utility-sub-type=network.mojom.N... 2620 chrome.exe -type=renderer -field-trial-handle=1032:146056... 3972 chrome.exe -type=renderer -field-trial-handle=1032:146056...

Any.run

- Another tool with impressive features - joesecurity

The screenshot shows the JoeSecurity website with the URL joesecurity.org/why-joe-sandbox. The page title is "Why Joe Sandbox?". The main content highlights three key features:

- Rapidly detect and analyze threats across multiple operating systems**: This section includes a note about modern adversaries using multiple OSes and icons for Windows, macOS, Linux, and Android.
- Gain access to very detailed and comprehensive analysis reports**: This section notes Joe Sandbox's detailed reports for both advanced and beginner analysts, accompanied by a magnifying glass icon over a document.
- Access one of the most complete and features rich sandbox solution on the market**: This section lists features like Live Interaction & Results, URL Analysis & AI based Phishing, with a small icon of a browser tab.

- 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 name	display 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., “detected,” “accout,” “suspencion,” “permanenlly”
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)