Phishing Email Detection

What is Phishing?

Phishing is a cyberattack where attackers send deceptive emails that appear to come from legitimate sources. The primary goal is to trick users into revealing sensitive information such as usernames, passwords, or financial data.

Phishing emails may contain:

- Fake sender addresses (spoofed domains).
- Malicious links that redirect to look-alike websites.
- Urgent messages to trick users into acting quickly.
- Malicious attachment

Why Do We Check Emails for Phishing?

1. Verify Authenticity
   - To confirm that the email actually came from the claimed sender.
2. Detect Malicious Links or Attachments
   - To ensure links do not redirect to credential harvesting sites.
3. Check IP and Domain Reputation
   - To identify if the sender's infrastructure is blacklisted or malicious.
4. Prevent Data Theft
   - Stops attackers from stealing login details or personal information.
5. Build Security Awareness
   - Helps users learn safe practices for identifying phishing attempts.

Tools Used

1. MxToolbox

MxToolbox is an online tool that provides DNS lookups, mail server checks, and blacklist monitoring.

Why it is used:

- To analyze DNS records such as MX (Mail Exchange), SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication).
- To check whether the sending domain or IP address is blacklisted.

How it helps:
If a sender’s domain or IP is blacklisted or lacks valid SPF/DKIM/DMARC records, it could be a sign of phishing.

2. VirusTotal

VirusTotal is a free online service that scans files, domains, IP addresses, and URLs using multiple antivirus engines and reputation databases.

Why it is used:

- To analyze domains, IPs, and URLs against multiple security vendors.
- To see relationships (linked domains, communicating files, etc.).

How it helps:
If a link or IP inside the email shows detections across different vendors, it indicates the email may be phishing or malicious.

3. IPVoid
IPVoid is an IP reputation checking tool that uses multiple sources to determine whether an IP is safe or flagged as malicious.

Why it is used:

- To check the geographical location, ASN (Autonomous System Number), and blacklists for an IP address.
- To validate if the sender IP belongs to a trusted provider.

How it helps:
If the sending IP is reported as suspicious or is not registered to the expected company (e.g., Google), it indicates a potential phishing attempt.

4. urlscan.io
urlscan.io is a web-based scanning service that crawls URLs and shows all the requests, redirects, and final rendered page.

Why it is used:

- To view how a suspicious link behaves without clicking it in your own browser.
- To capture screenshots of the page and check the SSL/TLS certificate.

How it helps:
If the link redirects outside the expected domain (e.g., accounts.google.com → randomsite.net), it’s a phishing indicator.

Hybrid Analysis is a free malware analysis sandbox environment. It executes suspicious files or URLs in a virtual machine and observes their behavior.

Why it is used:

- To analyze if a URL or file tries to perform malicious activities (e.g., contacting suspicious IPs, dropping malware).
- To generate detailed reports of behavior.

How it helps:
Legitimate URLs (like Google's) will show no malicious activity, while phishing sites may attempt credential theft or redirection to unsafe servers.

6. Gmail "Show Original"

A built-in Gmail feature that displays the full raw email headers.

Why it is used:

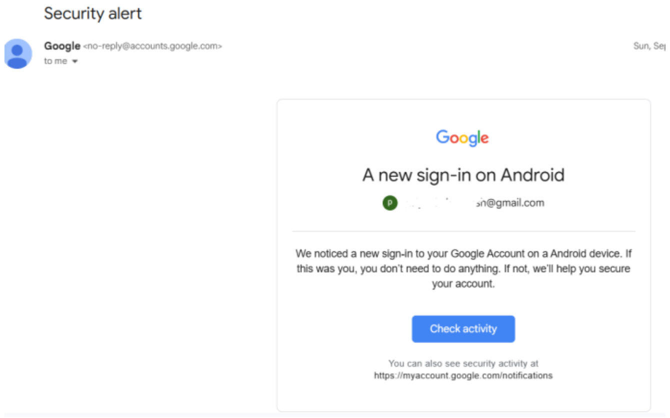
- To verify SPF, DKIM, and DMARC authentication results.
- To extract the real sending IP address.
- To check the email's routing path.

How it helps:
If SPF/DKIM/DMARC fail, the email could be spoofed. A mismatch between the displayed sender (Google) and the authenticated domain is a strong sign of phishing.

Step-by-Step Procedure

Step 1: Identify Suspicious Email

- Selected email subject: "Security alert".
- Sender: Google no-reply@accounts.google.com



Security alert

Google <no-reply@accounts.google.com>
to me

Sun, Se

Google

A new sign-in on Android

P n@gmail.com

We noticed a new sign-in to your Google Account on a Android device. If this was you, you don't need to do anything. If not, we'll help you secure your account.

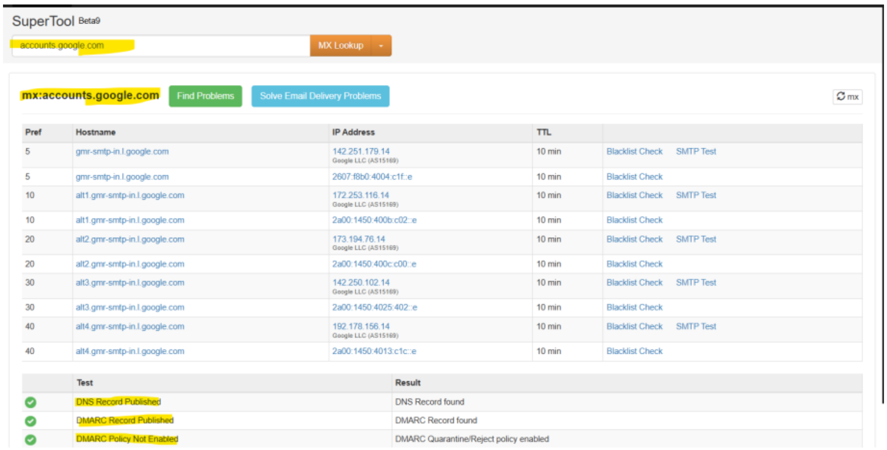
Check activity

You can also see security activity at
https://myaccount.google.com/notifications

Step 2: Domain Analysis Using MxToolbox

- Domain checked: accounts.google.com.

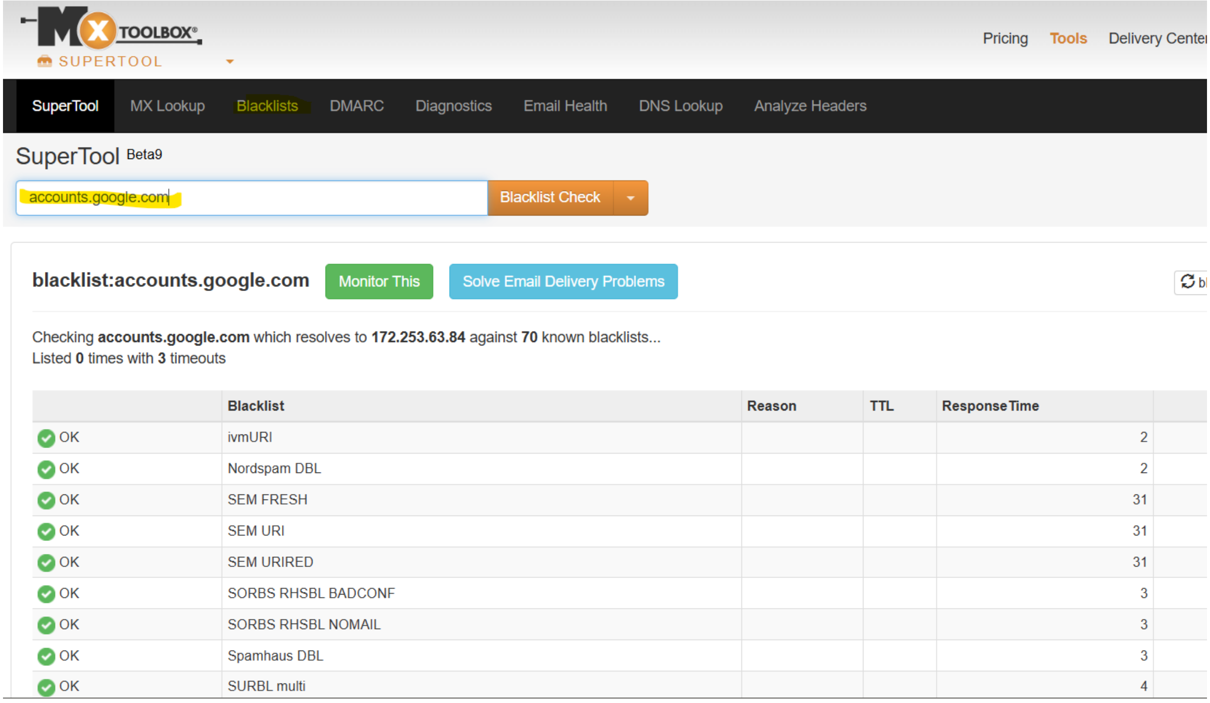
- Verified DNS, DMARC and MX records.



Pref	Hostname	IP Address	TTL	
5	gmr-smtp-in.l.google.com	142.251.179.14 Google LLC (AS15169)	10 min	Blacklist Check SMTP Test
5	gmr-smtp-in.l.google.com	2607:f8b0:4004:c1f::e	10 min	Blacklist Check
10	alt1.gmr-smtp-in.l.google.com	172.253.116.14 Google LLC (AS15169)	10 min	Blacklist Check SMTP Test
10	alt1.gmr-smtp-in.l.google.com	2a00:1450:400b:c02::e	10 min	Blacklist Check
20	alt2.gmr-smtp-in.l.google.com	173.194.76.14 Google LLC (AS15169)	10 min	Blacklist Check SMTP Test
20	alt2.gmr-smtp-in.l.google.com	2a00:1450:400c:c00::e	10 min	Blacklist Check
30	alt3.gmr-smtp-in.l.google.com	142.250.102.14 Google LLC (AS15169)	10 min	Blacklist Check SMTP Test
30	alt3.gmr-smtp-in.l.google.com	2a00:1450:4025:402::e	10 min	Blacklist Check
40	alt4.gmr-smtp-in.l.google.com	192.178.156.14 Google LLC (AS15169)	10 min	Blacklist Check SMTP Test
40	alt4.gmr-smtp-in.l.google.com	2a00:1450:4013:c1c::e	10 min	Blacklist Check

	Test	Result
✓	DNS Record Published	DNS Record found
✓	DMARC Record Published	DMARC Record found
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled

- Blacklist check shows domain is not blacklisted.



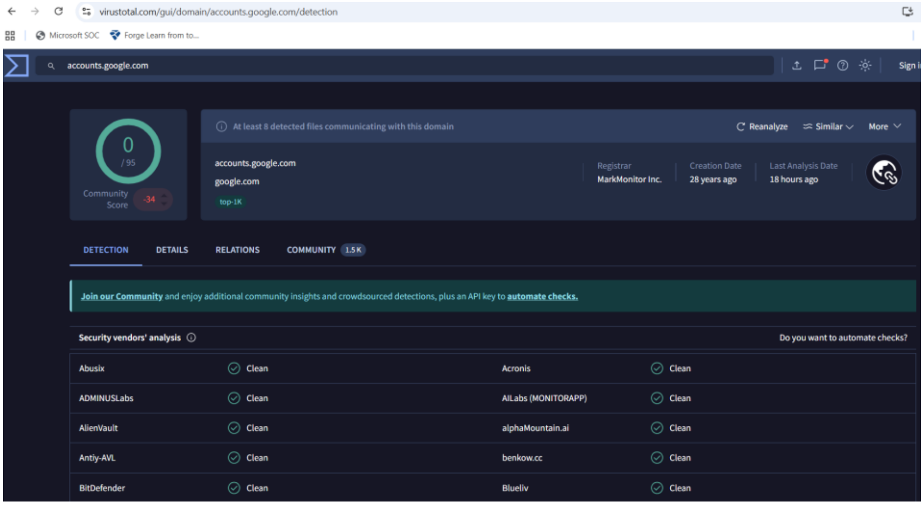
blacklist:accounts.google.com

Checking **accounts.google.com** which resolves to **172.253.63.84** against **70** known blacklists...
Listed **0** times with **3** timeouts

	Blacklist	Reason	TTL	Response Time
✓ OK	ivmURI			2
✓ OK	Nordspam DBL			2
✓ OK	SEM FRESH			31
✓ OK	SEM URI			31
✓ OK	SEM URIRED			31
✓ OK	SORBS RHSBL BADCONF			3
✓ OK	SORBS RHSBL NOMAIL			3
✓ OK	Spamhaus DBL			3
✓ OK	SURBL multi			4

Step 3: Domain Reputation Check with Virustotal

Domain: accounts.google.com.VirusTotal shows no malicious detections.



0
/ 95
Community Score -34

At least 8 detected files communicating with this domain

accounts.google.com
google.com
top-1K

Registrar: MarkMonitor Inc.
Creation Date: 28 years ago
Last Analysis Date: 18 hours ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

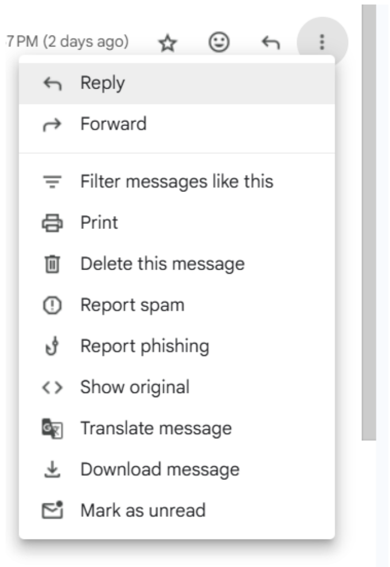
Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	Blueliv	✓ Clean

Step 4: Email Header Verification (Gmail Show Original)

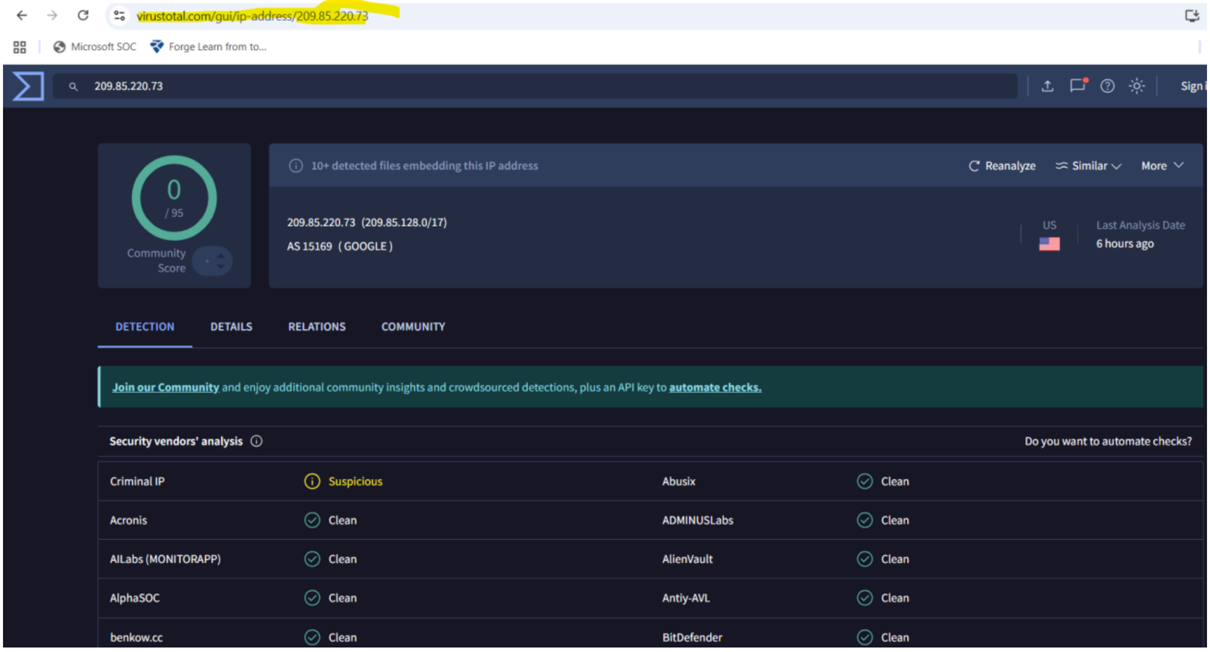
- SPF: PASS with IP 209.85.220.73.
- DKIM: PASS with domain accounts.google.com.
- DMARC: PASS.



Message ID	<igiga26NxFYvWcFwFADaZg@notifications.google.com>
Created at:	Sun, Sep 7, 2025 at 7:57 PM (Delivered after 3 seconds)
From:	Google <no-reply@accounts.google.com>
To:	
Subject:	Security alert
SPF:	PASS with IP 209.85.220.73 Learn more
DKIM:	'PASS' with domain accounts.google.com Learn more
DMARC:	'PASS' Learn more

Step 5: IP Reputation Check

- IP extracted: 209.85.220.73.
- VirusTotal IP analysis shows clean reputation.



virustotal.com/gui/ip-address/209.85.220.73

10+ detected files embedding this IP address

209.85.220.73 (209.85.128.0/17)
AS 15169 (GOOGLE)

Last Analysis Date
6 hours ago

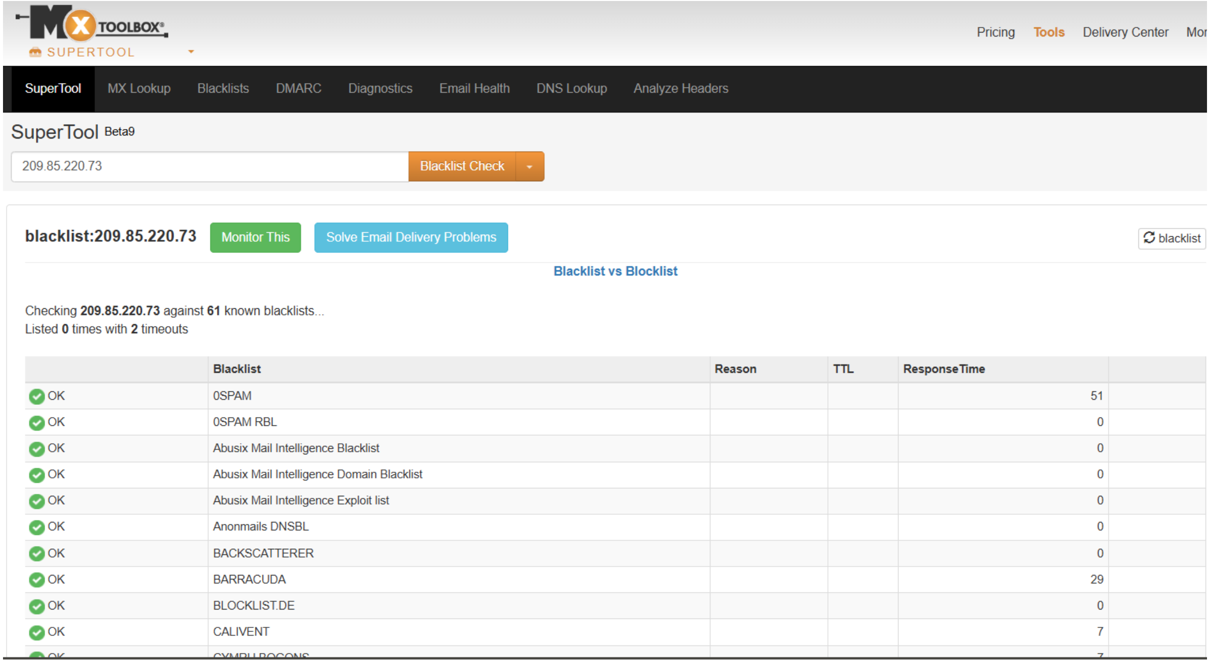
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Criminal IP	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
AlphaSOC	Clean	Antiy-AVL	Clean
benkow.cc	Clean	BitDefender	Clean

MxToolbox IP Lookup confirms IP belongs to Google infrastructure.

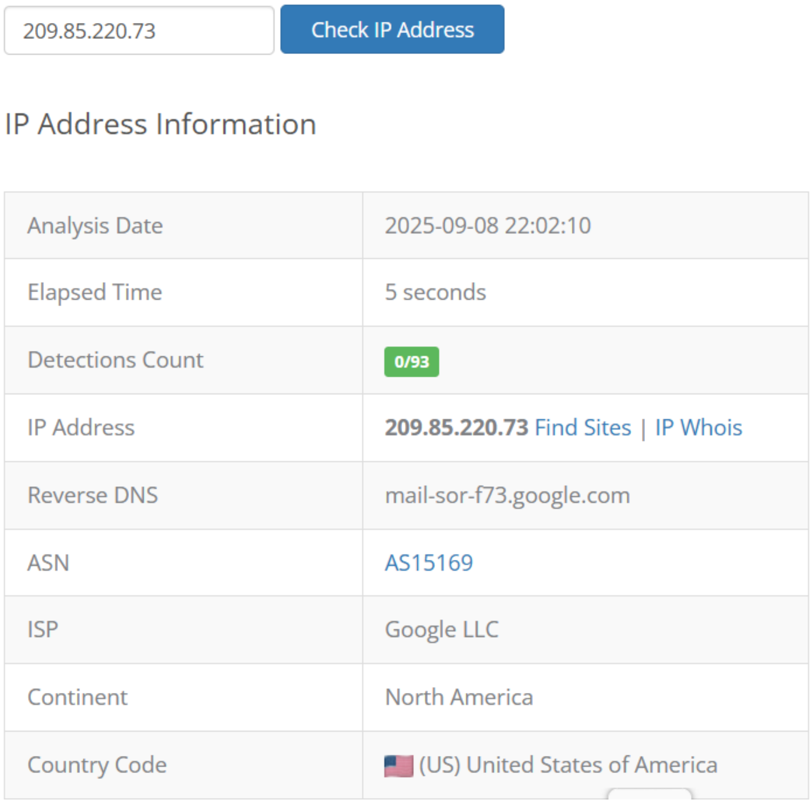


blacklist:209.85.220.73

Checking **209.85.220.73** against **61** known blacklists...
Listed **0** times with **2** timeouts

	Blacklist	Reason	TTL	ResponseTime
✓ OK	0SPAM			51
✓ OK	0SPAM RBL			0
✓ OK	Abusix Mail Intelligence Blacklist			0
✓ OK	Abusix Mail Intelligence Domain Blacklist			0
✓ OK	Abusix Mail Intelligence Exploit list			0
✓ OK	Anonmails DNSBL			0
✓ OK	BACKSCATTERER			0
✓ OK	BARRACUDA			29
✓ OK	BLOCKLIST.DE			0
✓ OK	CALIVENT			7
✓ OK	CYMRU BOGONS			7

- IPVoid reputation check confirms no malicious activity.



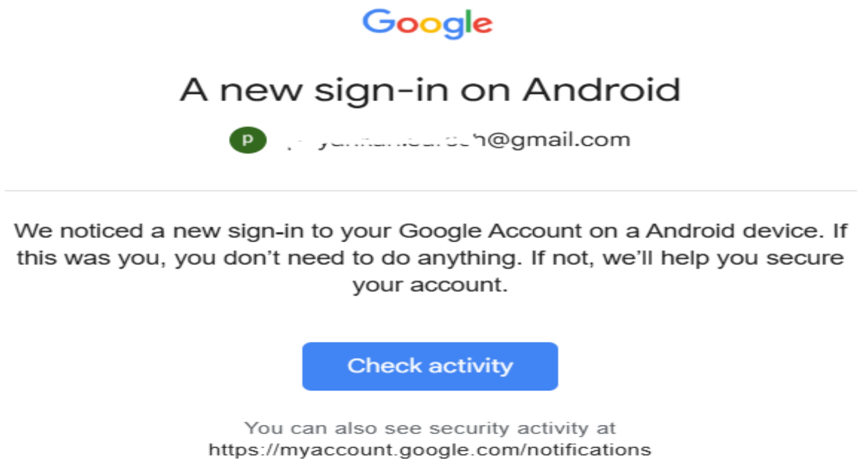
IP Address Information

Analysis Date	2025-09-08 22:02:10
Elapsed Time	5 seconds
Detections Count	0/93
IP Address	209.85.220.73 Find Sites | IP Whois
Reverse DNS	mail-sor-f73.google.com
ASN	AS15169
ISP	Google LLC
Continent	North America
Country Code	(US) United States of America

Step 6: URL Link Verification

- URL extracted from “Check Activity” button:

https://accounts.google.com/AccountChooser?Email= @gmail.com&continue=https://myaccount.google.com/alert/nt/1757255270830?rfn%3D325%26rfnc%3D1%26eid%3D-7424189988990015393%26et%3D0

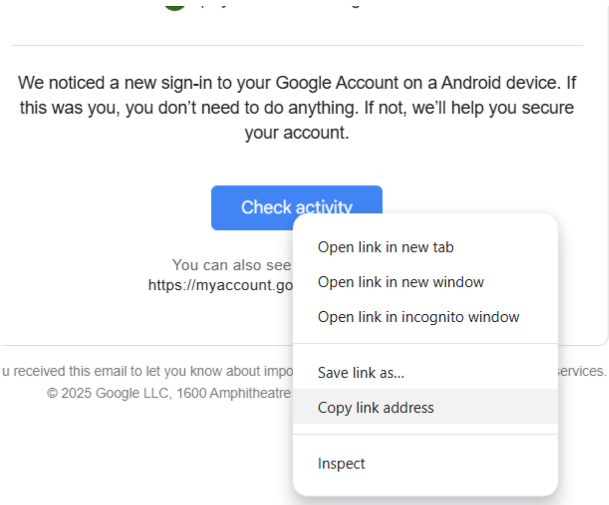


A new sign-in on Android

[illegible]h@gmail.com

We noticed a new sign-in to your Google Account on a Android device. If this was you, you don’t need to do anything. If not, we’ll help you secure your account.

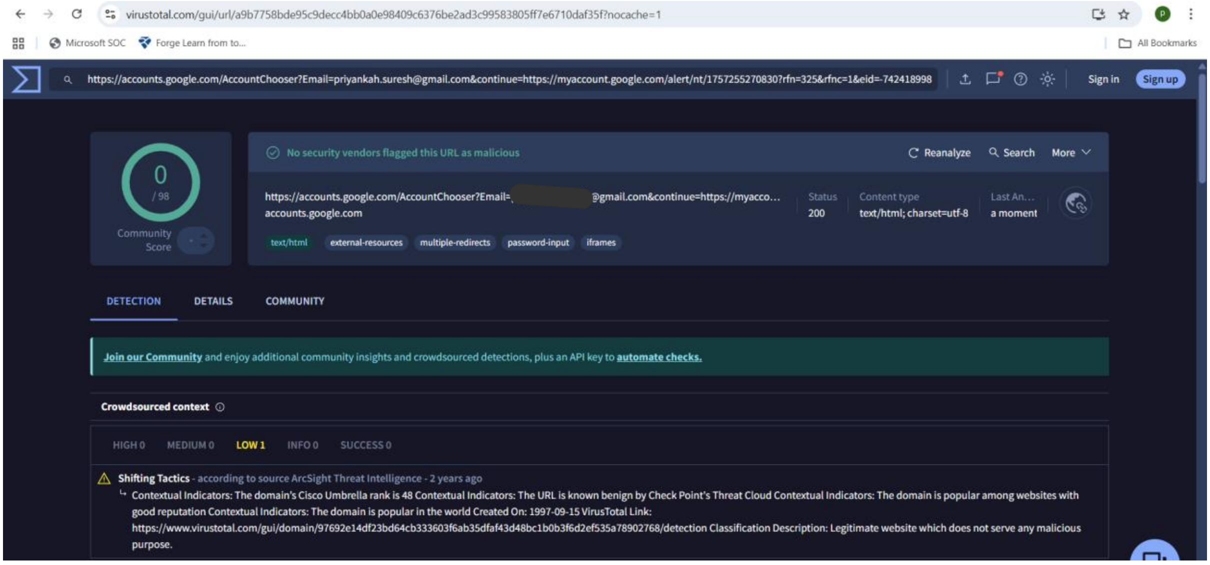
You can also see security activity at https://myaccount.google.com/notifications



We noticed a new sign-in to your Google Account on a Android device. If this was you, you don't need to do anything. If not, we'll help you secure your account.

u received this email to let you know about impo ervices.
© 2025 Google LLC, 1600 Amphitheatre

- VirusTotal URL Scan: Shows URL is safe, no malicious detections.



https://accounts.google.com/AccountChooser?Email=priyankah.suresh@gmail.com&continue=https://myaccount.google.com/alert/nt/1757255270830?rfn=325&rfnc=1&eid=-742418998

No security vendors flagged this URL as malicious

https://accounts.google.com/AccountChooser?Email=[redacted]@gmail.com&continue=https://myacco...
accounts.google.com

Status: 200
Content type: text/html; charset=utf-8
Last An...: a moment

text/html external-resources multiple-redirects password-input iframes

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

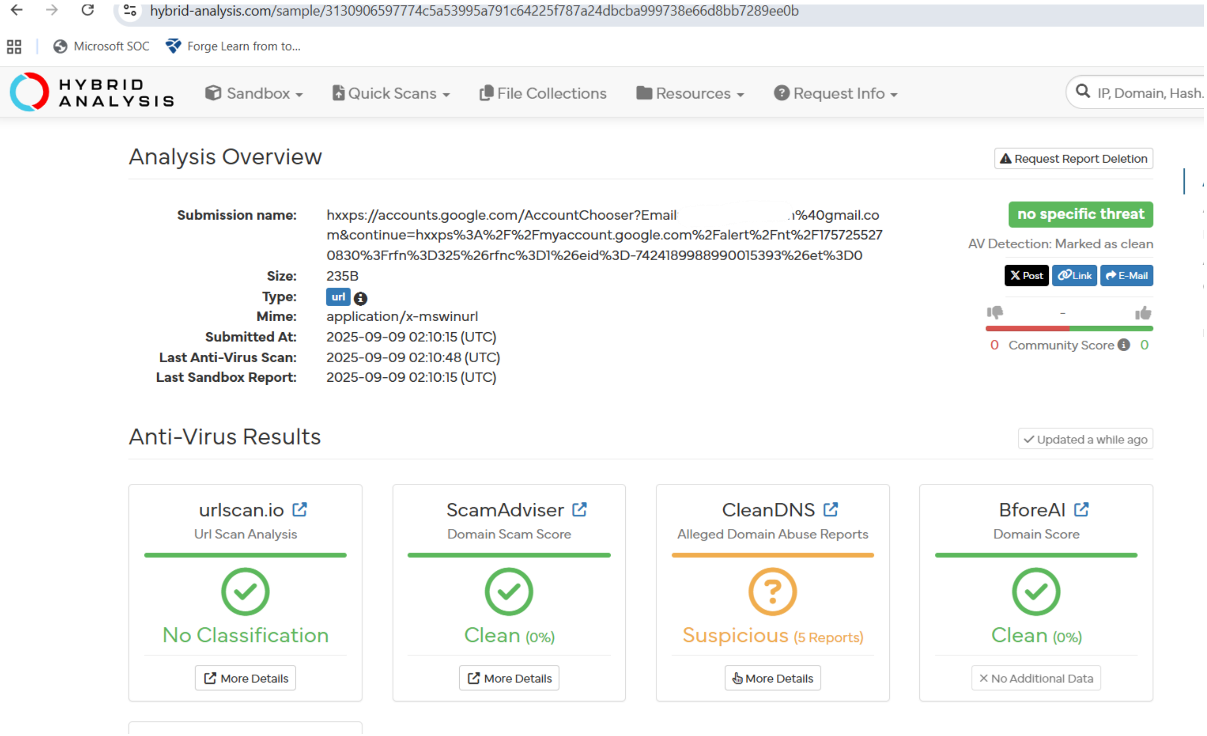
Crowdsourced context

HIGH 0 MEDIUM 0 LOW 1 INFO 0 SUCCESS 0

Shifting Tactics - according to source ArcSight Threat Intelligence - 2 years ago
Contextual Indicators: The domain's Cisco Umbrella rank is 48 Contextual Indicators: The URL is known benign by Check Point's Threat Cloud Contextual Indicators: The domain is popular among websites with good reputation Contextual Indicators: The domain is popular in the world Created On: 1997-09-15 VirusTotal Link: https://www.virustotal.com/gui/domain/97692e14df23bd64cb333603f6ab35dfaf43d48bc1b0b3f6d2ef535a78902768/detection Classification Description: Legitimate website which does not serve any malicious purpose.

- urlscan.io: Confirms redirects remain within Google domains, page screenshot matches Google login.

- Hybrid Analysis Sandbox: No suspicious activity detected.



Analysis Overview

Submission name:	hxxps://accounts.google.com/AccountChooser?Email ı%40gmail.com&continue=hxxps%3A%2F%2Fmyaccount.google.com%2Falert%2Fnt%2F1757255270830%3Frfn%3D325%26rfnc%3D1%26eid%3D-7424189988990015393%26et%3D0
Size:	235B
Type:	url
Mime:	application/x-mswinurl
Submitted At:	2025-09-09 02:10:15 (UTC)
Last Anti-Virus Scan:	2025-09-09 02:10:48 (UTC)
Last Sandbox Report:	2025-09-09 02:10:15 (UTC)

no specific threat

AV Detection: Marked as clean

0 Community Score 0

Anti-Virus Results

✓ Updated a while ago

urlscan.io	ScamAdviser	CleanDNS	BforeAI
Url Scan Analysis	Domain Scam Score	Alleged Domain Abuse Reports	Domain Score
No Classification	Clean (0%)	Suspicious (5 Reports)	Clean (0%)

Step 7: Gmail Account Activity Check

- Clicking “Check Activity” redirects to myaccount.google.com, which is an official Google property.
- Verified login details and timestamp match actual activity.

Summary

- SPF, DKIM, and DMARC all PASS, confirming email authenticity.
- IP 209.85.220.73 is a valid Google mail server with clean reputation.
- Domain accounts.google.com is legitimate and not blacklisted.
- URL link resolves to Google Account Chooser → myaccount.google.com (Google security alert page).

Final Conclusion:

The email analyzed is a legitimate Google security alert and not a phishing attempt.

Benefits of This Project

1. Practical Email Analysis – Teaches how to validate suspicious emails step by step.
2. Hands-on with Security Tools – MxToolbox, VirusTotal, IPVoid, urlscan.io, and Hybrid Analysis.
3. Improves Security Awareness – Helps detect phishing attempts in real-world scenarios.
4. Protects Users – Prevents credential theft and account compromise.

Author Details:

Author: Priyanka H S
Title: Phishing Email Detection Lab