Phishing Email Analysis Guide

Phishing emails are designed to trick users into **clicking malicious links**, **downloading harmful files**, or **giving away sensitive information**.

Below are the common **red flags** to look for and how to analyse an email header for deeper inspection.

Spotting Red Flags in an Email

1. **Unfamiliar Sender or Email Address**
   - Attackers often use random or look-alike email addresses.
   - **Example:** An email from `paypa1-support@payments.com` instead of the official `support@paypal.com`.
2. **Urgent or Alarming Language**
   - Phishers create urgency to make you act quickly.
   - **Example:** *"Your account will be suspended in 24 hours. Click here to verify!"*
3. **Suspicious Attachments or Links**
   - Attachments may contain malware, and links may lead to phishing sites.
   - **Example:** A file named `Invoice_12345.zip` from an unknown sender.
4. **Generic Greetings**
   - Instead of addressing you by name, they use vague terms.
   - **Example:** *"Dear Customer"* instead of *"Dear Haroon Zaman"*.
5. **Spelling and Grammar Mistakes**
   - Many phishing emails have poor language quality.
   - **Example:** *"We suspend you acount. Please update imediately."*
6. **Request for Personal or Financial Information**
   - Legitimate companies rarely ask for sensitive data by email.
   - **Example:** *"Please send your credit card details to confirm payment."*
7. **Unexpected Request for Payment**
   - Asking you to pay for something you didn't order.
   - **Example:** *"Your parcel delivery fee of $50 is pending. Pay now to receive it."*
8. **Too Good to Be True Offers**
   - Unrealistic promises are a common bait.
   - **Example:** *"Congratulations! You've won $1,000,000. Claim now."*
9. **Unfamiliar or Odd Attachments**
   - Files with strange extensions or unexpected format.
   - **Example:** A `.scr` or `.exe` file sent as a "document."
10. **Lack of Company Branding**

    - Real companies use consistent logos, fonts, and signatures.
    - **Example:** A "Microsoft" email with plain text and no logo.

11. **Unusual Sender's Email Domain**

    - Domains slightly altered to look genuine.

    - **Example:** `support@micros0ft.com` instead of `support@microsoft.com`.

12. **No Signature or Contact Information**

    - Professional emails usually end with proper contact details.
    - **Example:** Phishing email ends with just *“Thanks”* and nothing else.

13. **Failure of SPF, DKIM, or DMARC**

    - These email security checks ensure authenticity.
    - **Example:** Header shows `SPF=Fail` → sender is not authorized to use that domain.

Analysis of Email Header

Email headers contain hidden technical details that help verify authenticity.

1. **“From” Address**
    - Check if the displayed name matches the actual email address.
    - **Example:** *From: PayPal Support random@unknown.com* → suspicious.
2. **“Reply-To” Address**
    - Sometimes different from the “From” address.
    - **Example:** *From: bank@secure.com* but *Reply-To: hacker@gmail.com*.
3. **“Received” Fields**
    - Shows the path the email took. Look for strange or unknown servers.
    - **Example:** Email claiming from Google but “Received” from a server in Russia.
4. **IP Address and Domain Reputation**
    - Use tools like **MXToolBox** or **IPVoid** to check sender’s IP/domain.
    - **Example:** IP traced back to a server flagged for spam.
5. **External Links and Attachments**
    - Scan links/files with **VirusTotal** or **PhishTank**.
    - **Example:** URL leads to a fake login page flagged as phishing.
6. **DKIM Signature (DomainKeys Identified Mail)**
    - Confirms the email wasn’t altered in transit.
    - **Example:** *DKIM=Fail* → message may be forged.
7. **SPF Record (Sender Policy Framework)**
    - Verifies if sender is allowed to send emails from that domain.
    - **Example:** *SPF=Pass* → valid, *SPF=Fail* → forged.
8. **DMARC Authentication**
    - Aligns SPF & DKIM to confirm authenticity.
    - **Example:** *DMARC=Fail* → domain doesn’t authorize this email.
9. **Message ID**
    - Every real email has a unique ID. Fake ones may look odd or missing.
    - **Example:** A Gmail message without `@mail.gmail.com` in the ID → suspicious.
10. **Subject Encoding and Language**

- Strange characters or unusual encoding may indicate spam.
- **Example:** Subject shows as `=?UTF-8?B?V2luIGEgUFJJWkU=?=` instead of plain text.

11. **MIME Versions**

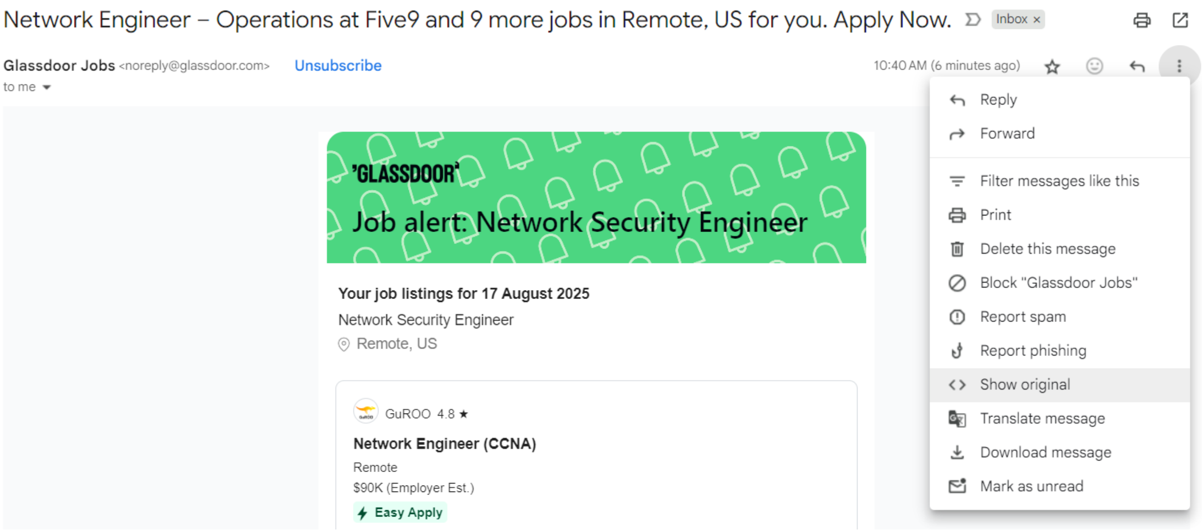
- Shows how the email is formatted. Strange or missing values can mean tampering.
- **Example:** MIME-Version is missing or altered in phishing attempts.

Example Email Phishing Analysis

Note: If the text of the Screen shots are small please zoom in.

The first step in conducting a phishing email analysis is to obtain the email's original message (including full headers) for detailed examination.

Click on the upper right three dots and the select "Show original".



Network Engineer – Operations at Five9 and 9 more jobs in Remote, US for you. Apply Now.

Glassdoor Jobs <noreply@glassdoor.com> Unsubscribe
to me

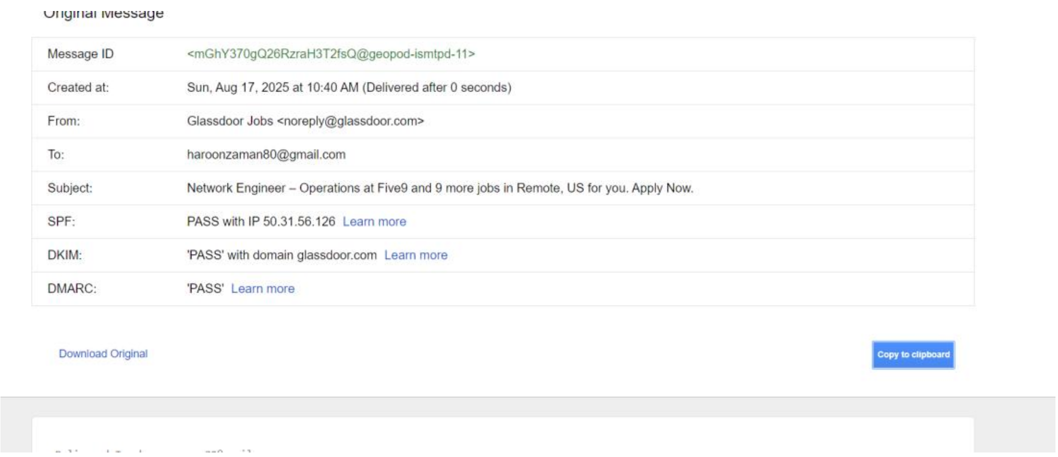
10:40 AM (6 minutes ago)

'GLASSDOOR'
Job alert: Network Security Engineer

Your job listings for 17 August 2025
Network Security Engineer
Remote, US

GuROO 4.8 ★
Network Engineer (CCNA)
Remote
$90K (Employer Est.)
Easy Apply

It will redirect you to this page



Original Message

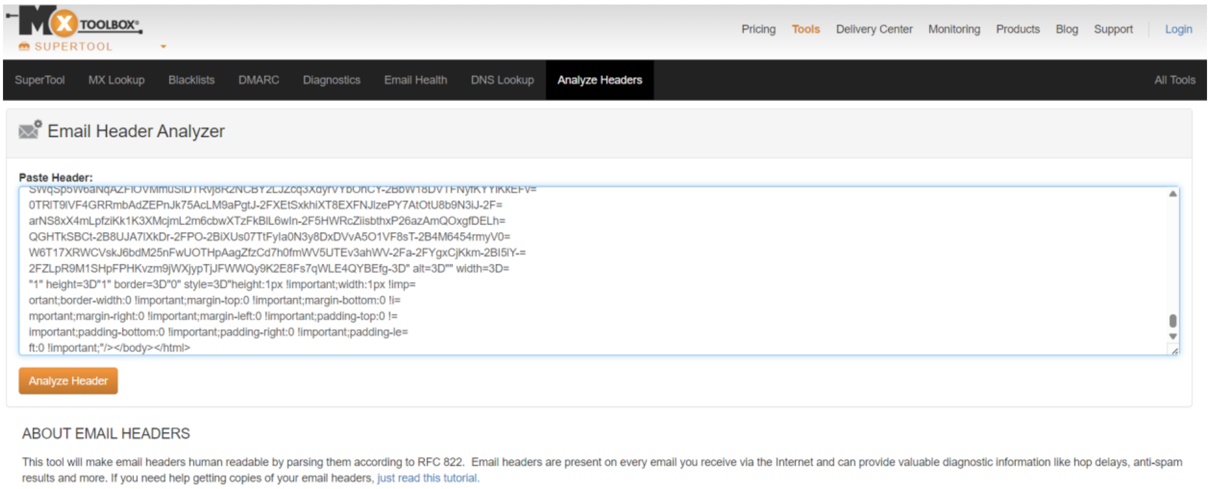
Message ID	<mGhY370gQ26RzraH3T2fsQ@geopod-ismtpd-11>
Created at:	Sun, Aug 17, 2025 at 10:40 AM (Delivered after 0 seconds)
From:	Glassdoor Jobs <noreply@glassdoor.com>
To:	haroonzaman80@gmail.com
Subject:	Network Engineer – Operations at Five9 and 9 more jobs in Remote, US for you. Apply Now.
SPF:	PASS with IP 50.31.56.126 Learn more
DKIM:	'PASS' with domain glassdoor.com Learn more
DMARC:	'PASS' Learn more

Next simply click on the “Copy to clipboard”

And open **MXToolBox**.

Then head to Analyze Header and copy the original message here.

Next click on the “Analyze Header”.



Email Header Analyzer

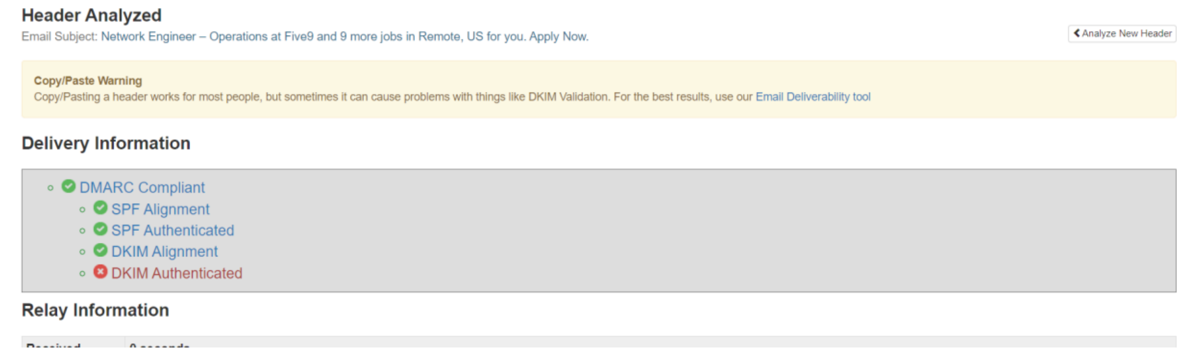
Paste Header:

```
SWqSp5W6aNqAZFIOVMmuSlDTRVj8R2NCBY2LJZcq3XdyrVYbOnCY-2BbW18DVTFNyfKYYIKKEFV=
0TRIT9lVF4GRRmbAdZEPnJk75AcLM9aPgtJ-2FXEtSxkhiXT8EXFNJlzePY7AtOtU8b9N3iJ-2F=
arNS8xX4mLpfziKk1K3XMcjmL2m6cbwXTzFkBIL6wIn-2F5HWRcZiisbthxP26azAmQOxgfDELh=
QGHTkSBCt-2B8UJA7IXkDr-2FPO-2BiXUs07TtFyla0N3y8DxDVvA5O1VF8sT-2B4M6454rmyV0=
W6T17XRWCVskJ6bdM25nFwUOTHpAagZfzCd7h0fmWV5UTEv3ahWV-2Fa-2FYgxCjKkm-2BI5lY-=
2FZLpR9M1SHpFPHKvzm9jWXjypTjJFWWQy9K2E8Fs7qWLE4QYBEfg-3D" alt=3D"" width=3D=
"1" height=3D"1" border=3D"0" style=3D"height:1px !important;width:1px !imp=
ortant;border-width:0 !important;margin-top:0 !important;margin-bottom:0 !i=
mportant;margin-right:0 !important;margin-left:0 !important;padding-top:0 !=
important;padding-bottom:0 !important;padding-right:0 !important;padding-le=
ft:0 !important;"/></body></html>
```

ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, just read this tutorial.

It will show this in result.



Header Analyzed

Email Subject: Network Engineer – Operations at Five9 and 9 more jobs in Remote, US for you. Apply Now.

Copy/Paste Warning

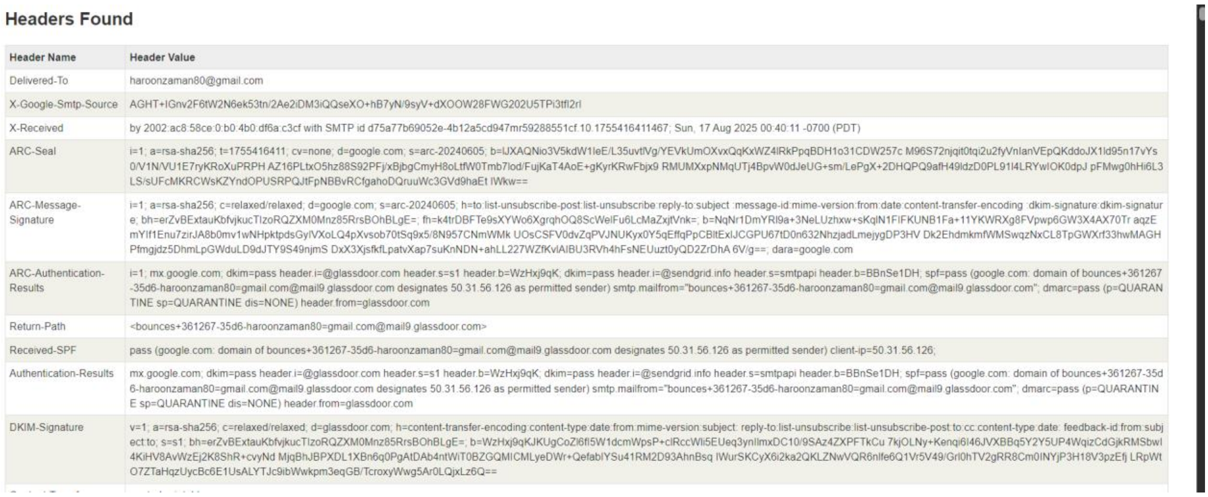
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our Email Deliverability tool

Delivery Information

- ✓ DMARC Compliant
  - ✓ SPF Alignment
  - ✓ SPF Authenticated
  - ✓ DKIM Alignment
  - ✗ DKIM Authenticated

Relay Information

If you have still any doubts just scroll down and the MXToolbox organized the email header.



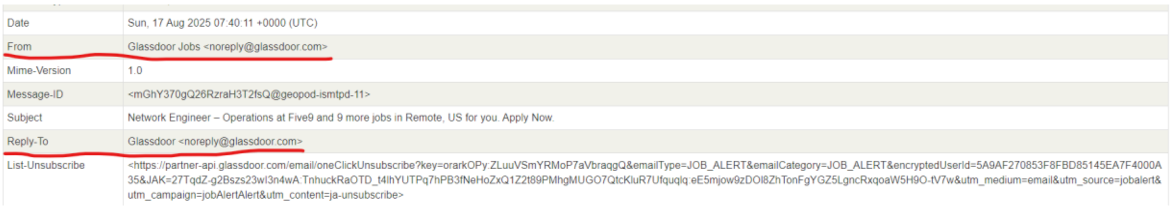
Headers Found

Header Name	Header Value
Delivered-To	haroonzaman80@gmail.com
X-Google-Smtp-Source	AGHT+IGnv2F6tW2N6ek53tn/2Ae2iDM3iQQseXO+hB7yN/9syV+dXOOW28FWG202U5TPi3tfl2rl
X-Received	by 2002:ac8:58ce:0:b0:4b0:df6a:c3cf with SMTP id d75a77b69052e-4b12a5cd947mr59288551cf.10.1755416411467; Sun, 17 Aug 2025 00:40:11 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1755416411; cv=none; d=google.com; s=arc-20240605; b=lJXAQNio3V5kdW1leE/L35uvtlVg/YEVkUmOXvxQqKxWZ4lRkPpqBDH1o31CDW257c M96S72njqit0tqi2u2fyVnIanVEpQKddoJX1ld95n17vYs0/V1N/VU1E7ryKRoXuPRPH AZ16PLtxO5hz88S92PFj/xBjbgCmyH8oLtfW0Tmb7lod/FujKaT4AoE+gKyrKRwFbjx9 RMUMXxpNMqUTj4BpvW0dJeUG+sm/LePgX+2DHQPQ9afH49ldzD0PL91l4LRYwIOK0dpJ pFMwg0hHi6L3LS/sUFcMKRCWsKZYndOPUSRPQJtFpNBBvRCfgahoDQruuWc3GVd9haEt lWkw==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=to:list-unsubscribe-post:list-unsubscribe:reply-to:subject :message-id:mime-version:from:date:content-transfer-encoding :dkim-signature:dkim-signature; bh=erZvBExtauKbfvjkucTlzoRQZXM0Mnz85RrsBOhBLgE=; fh=k4trDBFTe9sXYWo6XgrqhOQ8ScWelFu6LcMaZxjtVnk=; b=NqNr1DmYRl9a+3NeLUzhxw+sKqlN1FIFKUNB1Fa+11YKWRXg8FVpwp6GW3X4AX70Tr aqzEmYIf1Enu7zirJA8b0mv1wNHpktpdsGyIVXoLQ4pXvsob70tSq9x5/8N957CNmWMk UOsCSFV0dvZqPVJNUKyx0Y5qEffqPpCBltExlJCGPU67tD0n632NhzjadLmejygDP3HV Dk2EhdmkmfWMSwqzNxCL8TpGWXrf33hwMAGHPfmgjdz5DhmLpGWduLD9dJTY9S49njmS DxX3XjsfkfLpatvXap7suKnNDN+ahLL227WZfKvlAIBU3RVh4hFsNEUuzt0yQD2ZrDhA 6V/g==; dara=google.com
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@glassdoor.com header.s=s1 header.b=WzHxj9qK; dkim=pass header.i=@sendgrid.info header.s=smtpapi header.b=BBnSe1DH; spf=pass (google.com: domain of bounces+361267-35d6-haroonzaman80=gmail.com@mail9.glassdoor.com designates 50.31.56.126 as permitted sender) smtp.mailfrom="bounces+361267-35d6-haroonzaman80=gmail.com@mail9.glassdoor.com"; dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=glassdoor.com
Return-Path	<bounces+361267-35d6-haroonzaman80=gmail.com@mail9.glassdoor.com>
Received-SPF	pass (google.com: domain of bounces+361267-35d6-haroonzaman80=gmail.com@mail9.glassdoor.com designates 50.31.56.126 as permitted sender) client-ip=50.31.56.126;
Authentication-Results	mx.google.com; dkim=pass header.i=@glassdoor.com header.s=s1 header.b=WzHxj9qK; dkim=pass header.i=@sendgrid.info header.s=smtpapi header.b=BBnSe1DH; spf=pass (google.com: domain of bounces+361267-35d6-haroonzaman80=gmail.com@mail9.glassdoor.com designates 50.31.56.126 as permitted sender) smtp.mailfrom="bounces+361267-35d6-haroonzaman80=gmail.com@mail9.glassdoor.com"; dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=glassdoor.com
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=glassdoor.com; h=content-transfer-encoding:content-type:date:from:mime-version:subject: reply-to:list-unsubscribe:list-unsubscribe-post:to:cc:content-type:date: feedback-id:from:subject:to; s=s1; bh=erZvBExtauKbfvjkucTlzoRQZXM0Mnz85RrsBOhBLgE=; b=WzHxj9qKJKUgCoZl6fI5W1dcmWpsP+clRccWIi5EUeq3ynIlmxDC10/9SAz4ZXPFTkCu 7kjOLNy+Kenqi6l46JVXBBq5Y2Y5UP4WqizCdGjkRMSbwl4KiHV8AvWzEj2K8ShR+cvyNd MjqBhJBPXDL1XBn6q0PgAtDAb4ntWiT0BZGQMICMLyeDWr+QefablYSu41RM2D93AhnBsq lWurSKCyX6i2ka2QKLZNwVQR6nlfe6Q1Vr5V49/Grl0hTV2gRR8Cm0INYjP3H18V3pzEfj LRpWtO7ZTaHqzUycBc6E1UsALYTJc9ibWwkpm3eqGB/TcroxyWwg5Ar0LQjxLz6Q==

You can start verifying each header from the topic in this document **Analysis of Email Header.**

1. Start from “from” sender and “Reply-to”.

They should be the same.



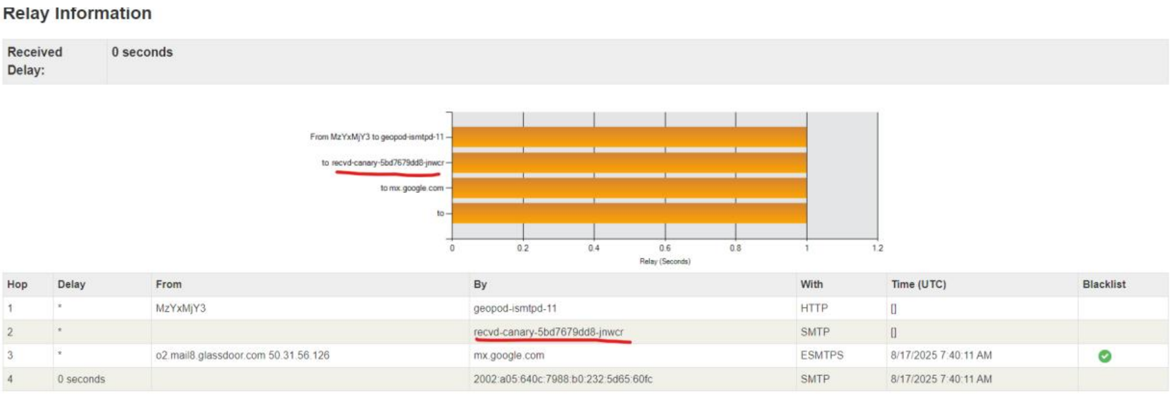
Date	Sun, 17 Aug 2025 07:40:11 +0000 (UTC)
From	Glassdoor Jobs <noreply@glassdoor.com>
Mime-Version	1.0
Message-ID	<mGhY370gQ26RzraH3T2fsQ@geopod-ismtpd-11>
Subject	Network Engineer – Operations at Five9 and 9 more jobs in Remote, US for you. Apply Now.
Reply-To	Glassdoor <noreply@glassdoor.com>
List-Unsubscribe	<https://partner-api.glassdoor.com/email/oneClickUnsubscribe?key=orarkOPy:ZLuuVSmYRMoP7aVbraqgQ&emailType=JOB_ALERT&emailCategory=JOB_ALERT&encryptedUserId=5A9AF270853F8FBD85145EA7F4000A35&JAK=27TqdZ-g2Bszs23wl3n4wA:TnhuckRaOTD_t4lhYUTPq7hPB3fNeHoZxQ1Z2t89PMhgMUGO7QtcKluR7Ufquqlq:eE5mjow9zDOl8ZhTonFgYGZ5LgncRxqoaW5H9O-tV7w&utm_medium=email&utm_source=jobalert&utm_campaign=jobAlertAlert&utm_content=ja-unsubscribe>

If that’s not enough we go further to Received.

2. “Received” Fields

If we can scroll up and go to “**Relay Information**”

We should match the received information to see if they match, if not then it is phishing



Relay Information

Received Delay:	0 seconds

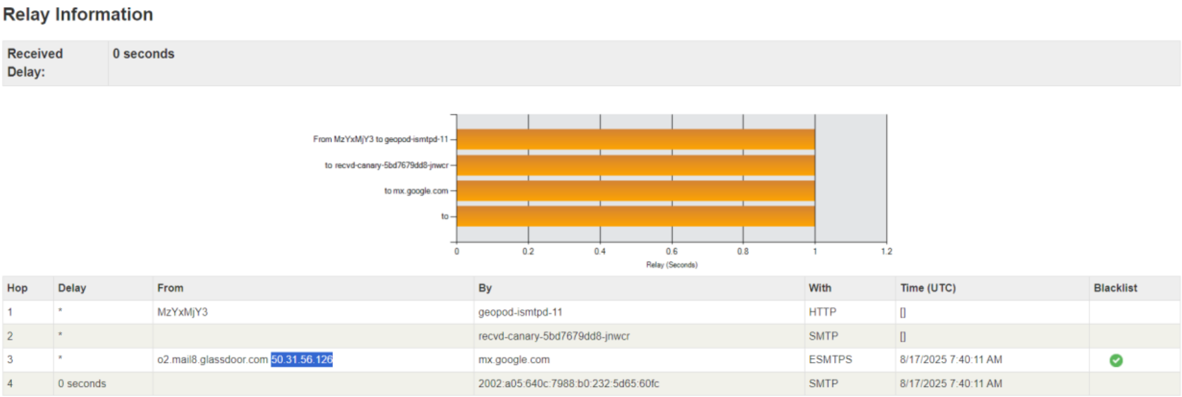
From MzYxMjY3 to geopod-ismtpd-11
to recvd-canary-5bd7679dd8-jnwcr
to mx.google.com
to
0
0.2
0.4
0.6
0.8
1
1.2
Relay (Seconds)

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	MzYxMjY3	geopod-ismtpd-11	HTTP	[]	
2	*		recvd-canary-5bd7679dd8-jnwcr	SMTP	[]	
3	*	o2.mail8.glassdoor.com 50.31.56.126	mx.google.com	ESMTPS	8/17/2025 7:40:11 AM	✓
4	0 seconds		2002:a05:640c:7988:b0:232:5d65:60fc	SMTP	8/17/2025 7:40:11 AM	

If that does not satisfy you then.

3. ”IP Address”

You can copy the IP address.



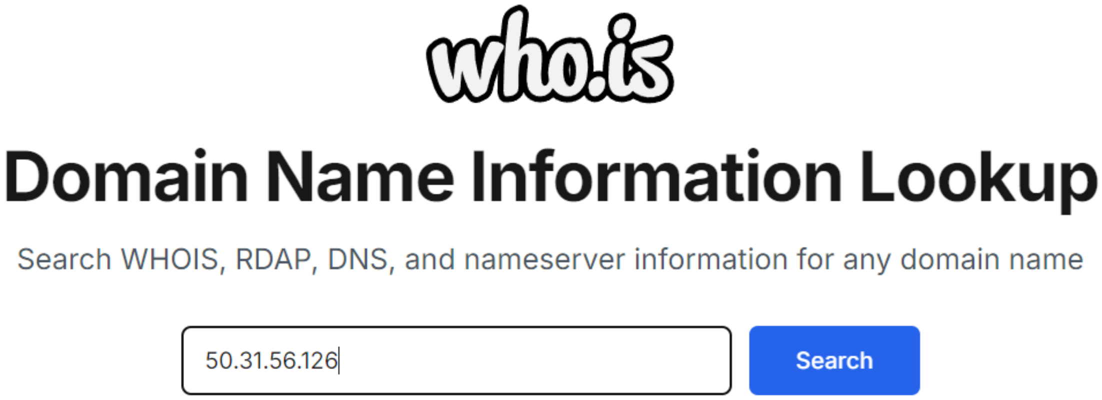
Relay Information

Received Delay:	0 seconds

From MzYxMjY3 to geopod-ismtpd-11
to recvd-canary-5bd7679dd8-jnwcr
to mx.google.com
to
0
0.2
0.4
0.6
0.8
1
1.2
Relay (Seconds)

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	MzYxMjY3	geopod-ismtpd-11	HTTP	[]	
2	*		recvd-canary-5bd7679dd8-jnwcr	SMTP	[]	
3	*	o2.mail8.glassdoor.com 50.31.56.126	mx.google.com	ESMTPS	8/17/2025 7:40:11 AM	✓
4	0 seconds		2002:a05:640c:7988:b0:232:5d65:60fc	SMTP	8/17/2025 7:40:11 AM	

You can go to Whois (https://who.is/). Paste the IP address here.



Domain Name Information Lookup

Search WHOIS, RDAP, DNS, and nameserver information for any domain name

50.31.56.126

And it will show you, **who this IP address resolve into**.

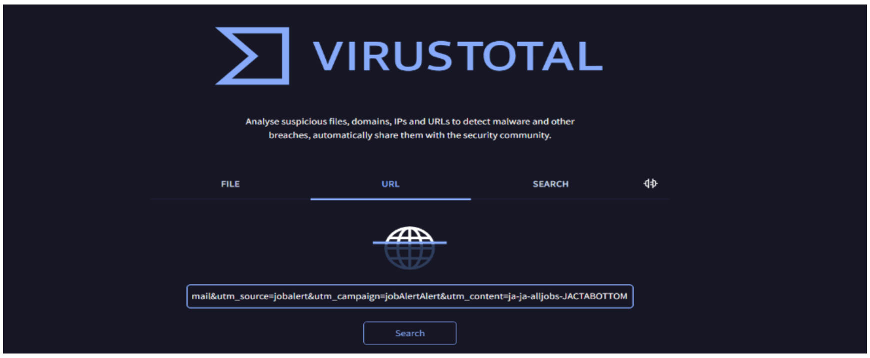
If that leave you in doubt you go further into then next.

4. External Links and Attachments

Note: DONOT open the link just copy the link from the email.

When the link is copied head to the URL scanning tool like **VirusTotal.**

https://www.virustotal.com/gui/home/

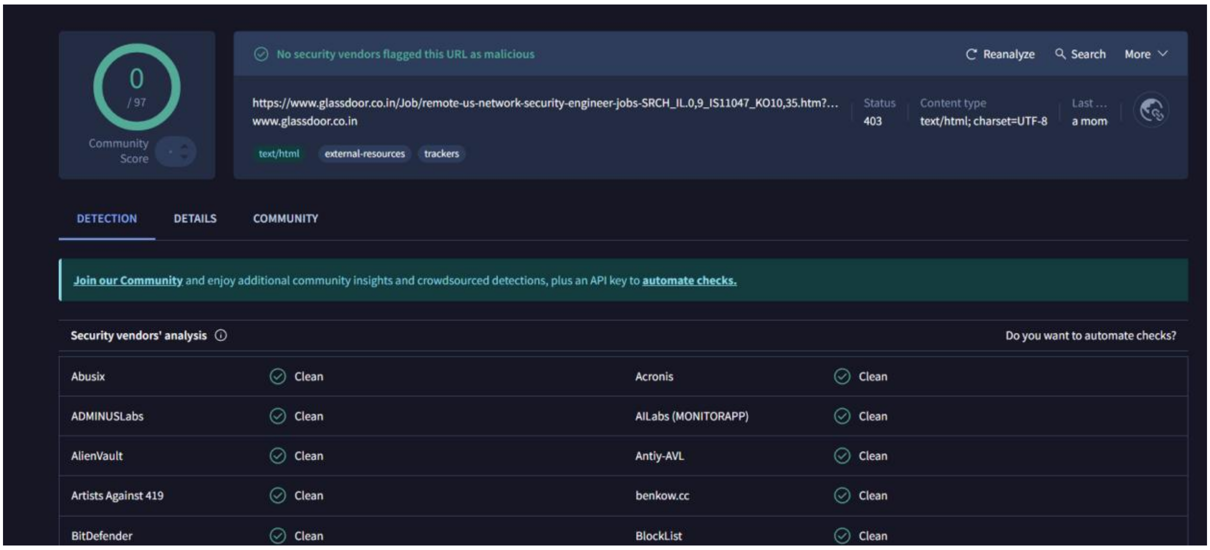


Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

mail&utm_source=jobalert&utm_campaign=jobAlertAlert&utm_content=ja-ja-alljobs-JACTABOTTOM

When you click Search it will show the result if it is clean or not.

You can also scan a file without opening it.



No security vendors flagged this URL as malicious

https://www.glassdoor.co.in/Job/remote-us-network-security-engineer-jobs-SRCH_IL.0,9_IS11047_KO10,35.htm?...
www.glassdoor.co.in

Status: 403

Content type: text/html; charset=UTF-8

Last ...: a mom

text/html · external-resources · trackers

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?

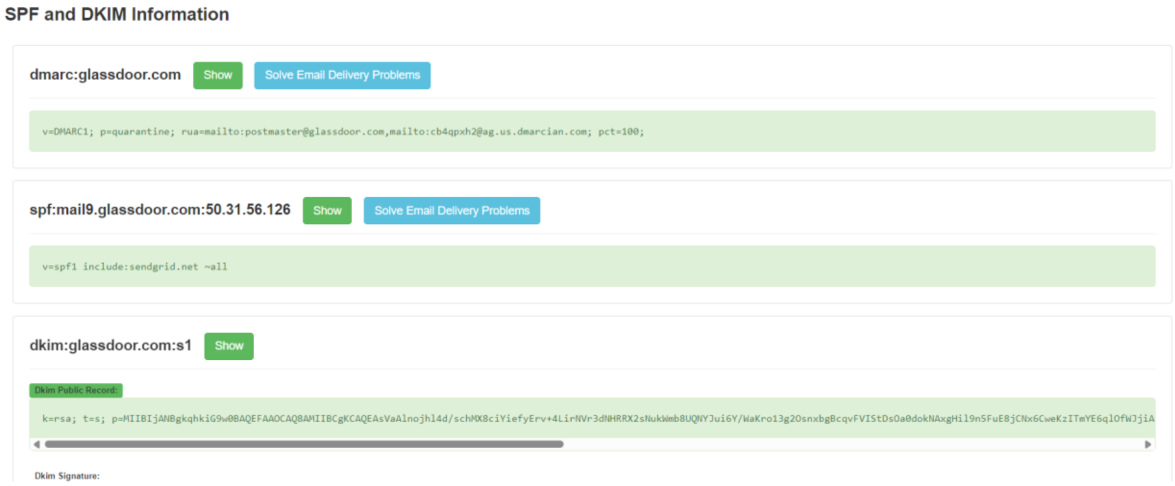
Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean
Artists Against 419	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	BlockList	✓ Clean

It will come clean or not.

If that is not enough we go further into.

5. DKIM and SPF

We can find it here in **MXToolBox**.



SPF and DKIM Information

dmarc:glassdoor.com

```
v=DMARC1; p=quarantine; rua=mailto:postmaster@glassdoor.com,mailto:cb4qpxh2@ag.us.dmarcian.com; pct=100;
```

spf:mail9.glassdoor.com:50.31.56.126

```
v=spf1 include:sendgrid.net ~all
```

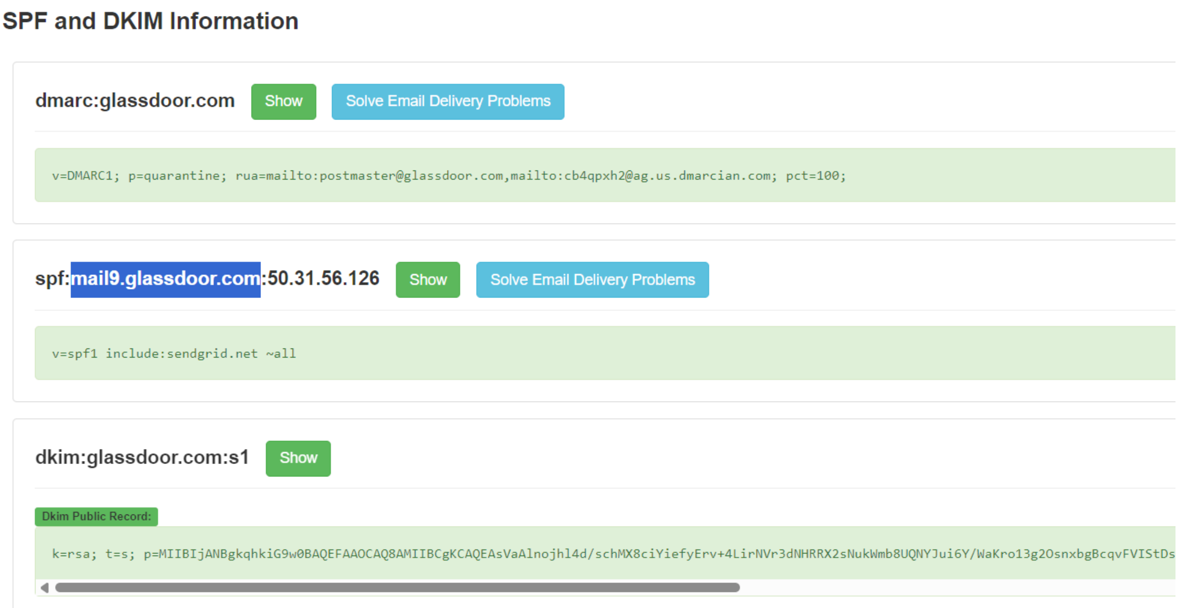
dkim:glassdoor.com:s1

Dkim Public Record:

```
k=rsa; t=s; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsVaAlnojhl4d/schMX8ciYiefyErv+4LirNVr3dNHRRX2sNukWmb8UQNYJui6Y/WaKro13g2OsnxbgBcqvFVIStDsOa0dokNAxgHil9n5FuE8jCNx6CweKzITmYE6qlOfWJjiA
```

Dkim Signature:

For confirmation, if the SPF is correct, copy the SPF link and confirm it further using the tool **SPF-Record (https://www.spf-record.com/spf-lookup/).**



SPF and DKIM Information

dmarc:glassdoor.com

```
v=DMARC1; p=quarantine; rua=mailto:postmaster@glassdoor.com,mailto:cb4qpxh2@ag.us.dmarcian.com; pct=100;
```

spf:mail9.glassdoor.com:50.31.56.126

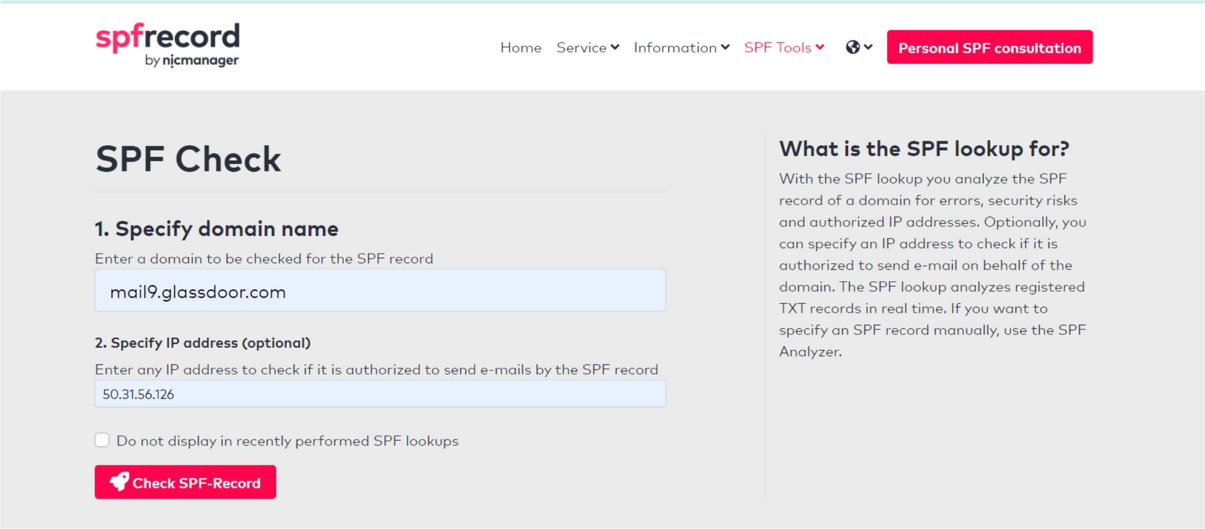
```
v=spf1 include:sendgrid.net ~all
```

dkim:glassdoor.com:s1

Dkim Public Record:

```
k=rsa; t=s; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsVaAlnojhl4d/schMX8ciYiefyErv+4LirNVr3dNHRRX2sNukWmb8UQNYJui6Y/WaKro13g2OsnxbgBcqvFVIStDs
```

The redirect yourself to SPF-Record website and paste the link and the IP Address in the next field there to search.



SPF Check

1. Specify domain name

Enter a domain to be checked for the SPF record

mail9.glassdoor.com

2. Specify IP address (optional)

Enter any IP address to check if it is authorized to send e-mails by the SPF record

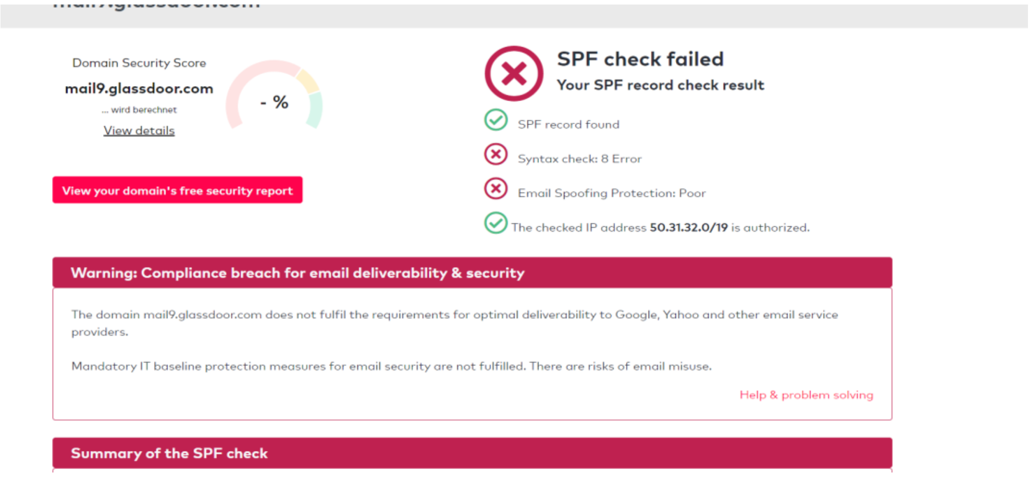
50.31.56.126

□ Do not display in recently performed SPF lookups

What is the SPF lookup for?

With the SPF lookup you analyze the SPF record of a domain for errors, security risks and authorized IP addresses. Optionally, you can specify an IP address to check if it is authorized to send e-mail on behalf of the domain. The SPF lookup analyzes registered TXT records in real time. If you want to specify an SPF record manually, use the SPF Analyzer.

Check the record to see its authentication.



Domain Security Score

mail9.glassdoor.com

... wird berechnet

SPF check failed

Your SPF record check result

- ✓ SPF record found
- ☒ Syntax check: 8 Error
- ☒ Email Spoofing Protection: Poor
- ✓ The checked IP address **50.31.32.0/19** is authorized.

Warning: Compliance breach for email deliverability & security

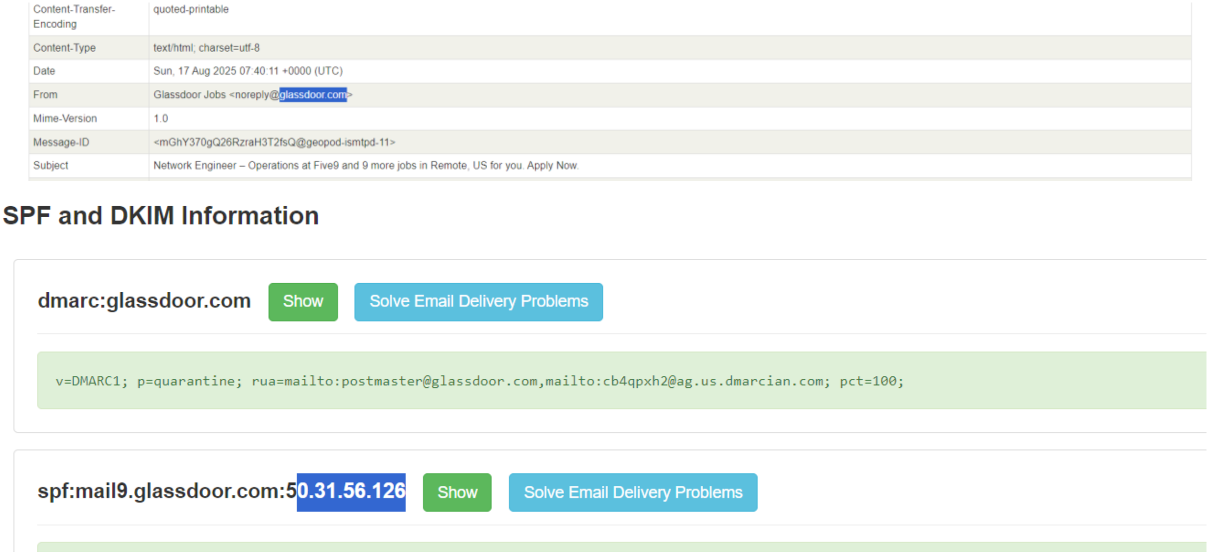
The domain mail9.glassdoor.com does not fulfil the requirements for optimal deliverability to Google, Yahoo and other email service providers.

Mandatory IT baseline protection measures for email security are not fulfilled. There are risks of email misuse.

Summary of the SPF check

It will show that the link and IP address whether it is authorize or not.

We can further check the SPF if it is malicious or not, by grabbing the link from the “From” field in MXToolBox and the IP address from the SPF field.



Content-Transfer-Encoding	quoted-printable
Content-Type	text/html; charset=utf-8
Date	Sun, 17 Aug 2025 07:40:11 +0000 (UTC)
From	Glassdoor Jobs <noreply@glassdoor.com>
Mime-Version	1.0
Message-ID	<mGhY370gQ26RzraH3T2fsQ@geopod-ismtpd-11>
Subject	Network Engineer – Operations at Five9 and 9 more jobs in Remote, US for you. Apply Now.

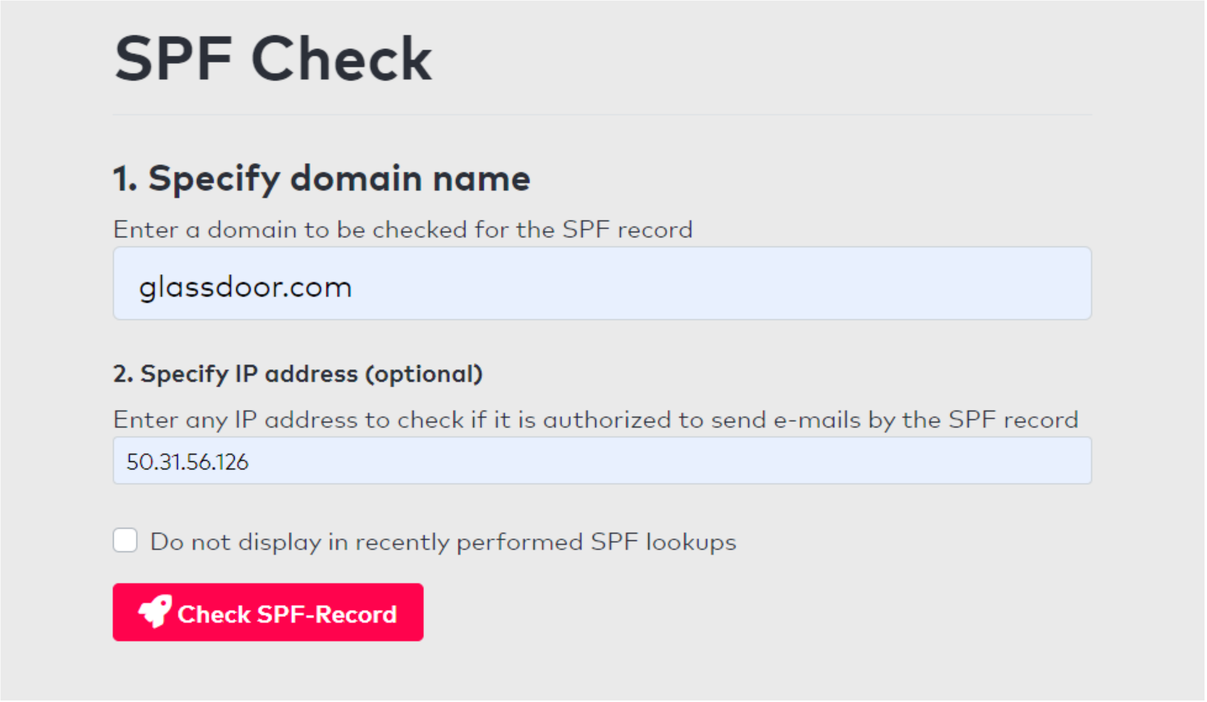
SPF and DKIM Information

dmarc:glassdoor.com

```
v=DMARC1; p=quarantine; rua=mailto:postmaster@glassdoor.com,mailto:cb4qpxh2@ag.us.dmarcian.com; pct=100;
```

spf:mail9.glassdoor.com:50.31.56.126

And paste them in SPF-records website (the link is given).



SPF Check

1. Specify domain name

Enter a domain to be checked for the SPF record

glassdoor.com

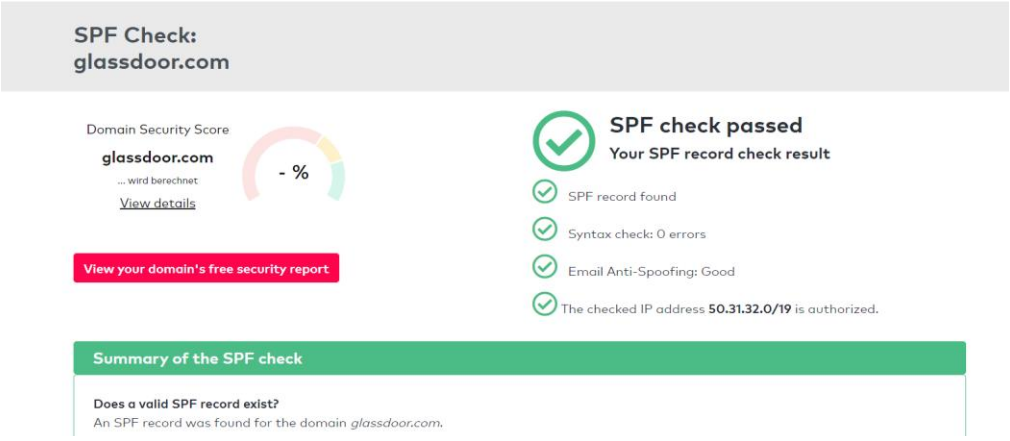
2. Specify IP address (optional)

Enter any IP address to check if it is authorized to send e-mails by the SPF record

50.31.56.126

□ Do not display in recently performed SPF lookups

It will either match or not. If not then it is an indication of being malicious.



SPF Check:
glassdoor.com

Domain Security Score
glassdoor.com
... wird berechnet
View details

SPF check passed
Your SPF record check result

- ✓ SPF record found
- ✓ Syntax check: 0 errors
- ✓ Email Anti-Spoofing: Good
- ✓ The checked IP address **50.31.32.0/19** is authorized.

Summary of the SPF check

Does a valid SPF record exist?
An SPF record was found for the domain *glassdoor.com.*

In this example, I have demonstrated a step-by-step process for analyzing a potentially malicious email. By following these steps, one can reliably identify multiple red flags that indicate the email is part of a phishing campaign.

Conclusion:

Phishing remains one of the most common and dangerous forms of cyberattack, exploiting human trust rather than technical vulnerabilities. By carefully examining both the visible content of an email and its hidden header information, suspicious indicators can be identified with a high degree of accuracy.

The step-by-step approach outlined in this document—from spotting red flags in the message body to verifying authentication mechanisms such as SPF, DKIM, and DMARC—provides a structured method to distinguish between legitimate and malicious emails.

Ultimately, consistent awareness and methodical analysis are the strongest defences against phishing campaigns. By practicing these techniques regularly, individuals and organizations can significantly reduce the risk of falling victim to email-based threats.