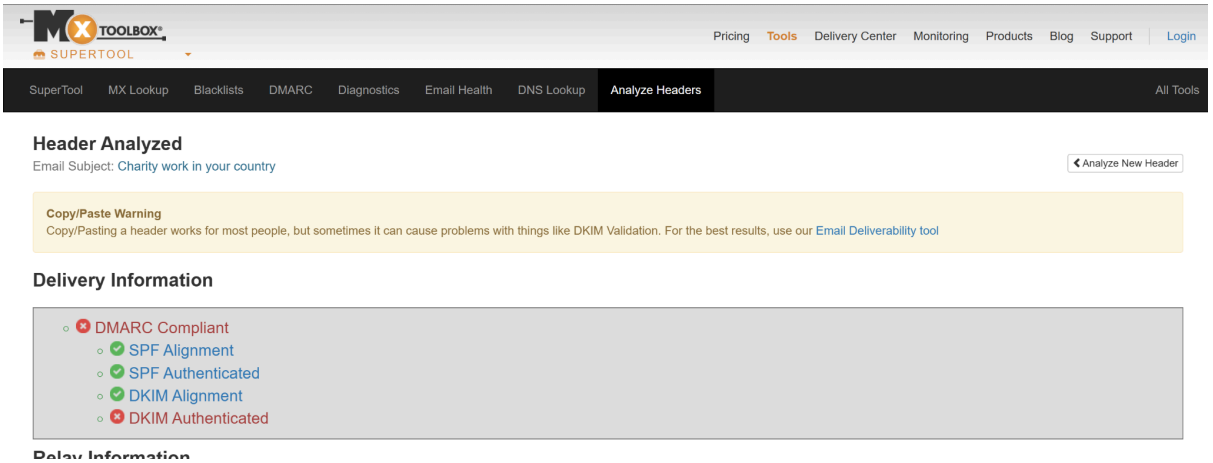
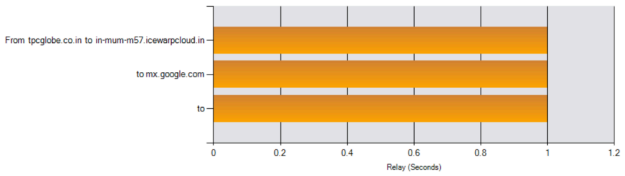
Analyzing a Phishing Email:



Relay Information

Received Delay:	**0 seconds**



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	tpcglobe.co.in 139.135.41.32	in-mum-m57.icewarpcloud.in	ASMTP (SSL)	8/22/2024 5:58:31 AM	✖
2	*	in-mum-m57.icewarpcloud.in 103.161.42.41	mx.google.com	ESMTPS	8/22/2024 5:36:09 AM	✔
3	0 seconds		2002:ab3:312:0:b0:277:e77f:cd11	SMTP	8/22/2024 5:36:09 AM	

SPF and DKIM Information

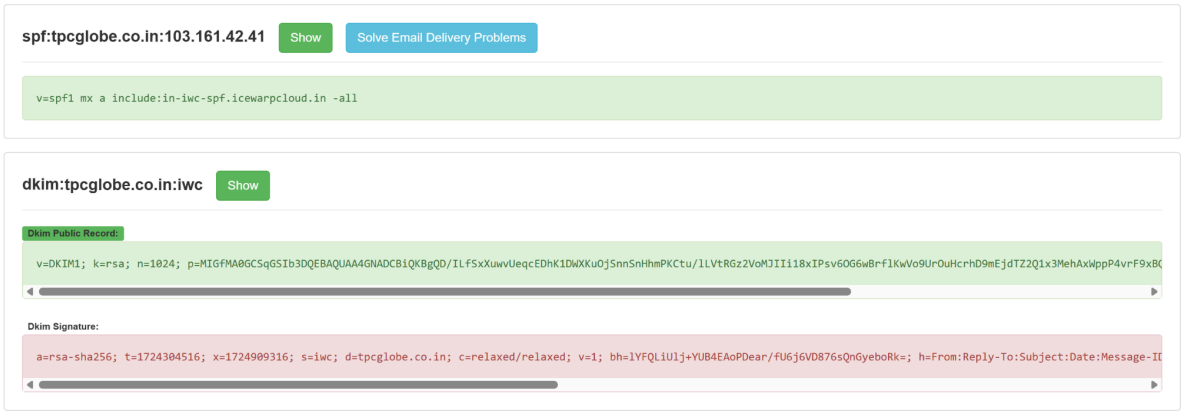
dmarc:tpcglobe.co.in Hide | Solve Email Delivery Problems

```
v=DMARC1; p=none; rua=mailto:dmarc@tpcglobe.co.in;
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	none	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
rua	mailto:dmarc@tpcglobe.co.in	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.

	Test	Result	
✖	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✔	DMARC Record Published	DMARC Record found	
✔	DMARC Syntax Check	The record is valid	
✔	DMARC Multiple Records	Multiple DMARC records corrected to a single record.	
✔	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.	

Reported by **ns6.centumtech.net** on 10/29/2025 at **1:02:07 PM (UTC 0)**, just for you. Transcript



Headers Found

Header Name	Header Value
Delivered-To	jagannadhulapalli@gmail.com
X-Forwarded-Encrypted	i=2; AJvYcCXDcnGVxGYldZoWpyCc5VvXRdpsekayeJtnc65fzzRth7zK8e22N//FqARNuEo5pCAjhGoNJkkN8Vs07rDA84zATg==@gmail.com
X-Google-Smtp-Source	AGHT+IGxauA7vwlJbZCuvMLlWSL1A1ImDfOb6Gysr1TrYZBxhl2PCuMjFwusF7pfwLJ/1Lke7DQ8
X-Received	by 2002:a17:90b:1b48:b0:2c9:8c34:9754 with SMTP id 98e67ed59e1d1-2d5e9a66838mr4848952a91.21.1724304969219; Wed, 21 Aug 2024 22:36:09 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1724304969; cv=none; d=google.com; s=arc-20240605; b=XTYxzu0hYqggR2gZNN6MwoO819sufgZpcj901NafMly5duqUtE2tAjOvuI50+ZMe68 3lnKsEGIMx0gW/jJfi2cJlRoxvvhhxB4iSAb4IljnGtgU1g7g9budplukCdvqDOlg4TZ G+mjpKDW08LCbqCyK0ZT4HiGP/PoPhcZlcIV8eRk7uW3oXEpqzp7s3s6ASXqhcZMqZ3G 9YxGwI4TEPExHgiQKSSdk3MS2f3kXvgFYFgv8QiloIMeWtJe5jI8IY1TWpXY VPGbsN7Y e3Vk5NuZ7LuF7K4Qz5x/odnmaVSR/f5pJJtvemXOvNqVHp/0j5CgTa2FGPhu47nWSQEO GBVQ==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=mime-version:reply-to:message-id:subject:from:date:dkim-signature; bh=lYFQLiUlj+YUB4EAoPDear/fU6j6VD876sQnGyeboRk=; fh=47DEQpj8HBSa+/TlmW+5JCeuQeRkm5NMpJWZG3hSuFU=; b=baanf8GwESN6OgUQwLILUHw8MSEJ1/dDLSc6e0uvaP84vAHBcuk8uy5N2uxWTGj7Rn qHMaipgOIOlvgLgr0unW30u8Pogrpu96jFauk4R07 vFlFJP4HB8nodPQ/VNSko3kv7s+ 7ERHeKkcKC/JQhN/3RuQ0UkZjaCj1JNzOZ/FPo6siNL7HqImeFilQvJYrXO/USczl+i0 Ab7o8BS3wuDbk7RCrhrJ5SE/NyVG3A10Xpj5F8MmWYCt2z5U8Sy3S0fYUA5IGuhoz 9WR p0FFv4lgDKhh7YE4XV3F0z+PTnF0n0p7klF///QL9wRVH+0i5PipTd5HwfXhCl+28MeT gFUA==; dara=google.com
ARC-Authentication-Results	i=1; mx.google.com; dkim=temperror (no key for signature) header.i=@tpcglobe.co.in header.s=iwc header.b=STtTl+Tz; spf=pass (google.com: domain of pmd@tpcglobe.co.in designates 103.161.42.41 as permitted sender) smtp.mailfrom=pmd@tpcglobe.co.in; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=tpcglobe.co.in
Return-Path	<pmd@tpcglobe.co.in>
Received-SPF	pass (google.com: domain of pmd@tpcglobe.co.in designates 103.161.42.41 as permitted sender) client-ip=103.161.42.41;
Authentication-Results	mx.google.com; dkim=temperror (no key for signature) header.i=@tpcglobe.co.in header.s=iwc header.b=STtTl+Tz; spf=pass (google.com: domain of pmd@tpcglobe.co.in designates 103.161.42.41 as permitted sender) smtp.mailfrom=pmd@tpcglobe.co.in; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=tpcglobe.co.in
DKIM-Signature	a=rsa-sha256; t=1724304516; x=1724909316; s=iwc; d=tpcglobe.co.in; c=relaxed/relaxed; v=1; bh=lYFQLiUlj+YUB4EAoPDear/fU6j6VD876sQnGyeboRk=; h=From:Reply-To:Subject:Date:Message-ID:MIME-Version:Content-Type; b=STtTl+TzuEnWV6lg0QqwxUho2pnPzK3O6JCnLMBgO/Q2lSh6Wna0FxhYqroZMSTRU/a3AxzptNOV2kzlqaGPafY384Txz1aTO3OJmFSCG2cRGOwzcXCje797g4+LyD7B7rCB53ay2IhWs/sq+zi8RLhEI2GQlwzB+lpYjEUzd2o=
Date	Wed, 21 Aug 2024 22:28:27 -0700
From	pmd <pmd@tpcglobe.co.in>
Subject	Charity work in your country
Message-ID	<32ffd09c6cee6e7962d2d746950ae454@tpcglobe.co.in>

🧾 Step 1: Email Header Analysis

- **Tool Used:** MXToolbox Header Analyzer
- **Email Subject:** *Charity work in your country*

- **Observation:**
  The email header was analyzed to check the sender's authenticity and mail routing path. The results indicated:

  - **DMARC:** ❌ Not Compliant
  - **SPF Alignment:** ✅ Passed
  - **SPF Authentication:** ✅ Passed
  - **DKIM Alignment:** ✅ Passed

    - **DKIM Authentication:** ❌ Failed

- **Interpretation:**
  The failure of DMARC and DKIM authentication suggests that the message may not be from a legitimate or authorized sender. SPF alone is not enough to ensure message trustworthiness.

Step 2: Relay Information (Mail Path Tracking)

- The mail passed through the following servers:

    1. **tpcglobe.co.in (139.135.41.32) → icewarpcloud.in**
    2. **icewarpcloud.in (103.161.42.41) → mx.google.com**
    3. **mx.google.com** → recipient mailbox

- **Blacklist Check:**
  The IP address **139.135.41.32** was found on a **blacklist**, indicating previous suspicious activity or spam-related behavior.

- **Observation:**
  Although the delivery delay was 0 seconds (indicating quick delivery), the blacklist status and relay through external mail servers raise concerns about legitimacy.

Step 3: SPF and DKIM Record Validation

SPF Record (Sender Policy Framework)

v=spf1 mx a include:in-iwc-spf.icewarpcloud.in -all

Result: SPF is correctly configured and passes validation.

Purpose: SPF confirms that the sending mail server is authorized to send emails for the domain `tpcglobe.co.in`.

DKIM Record (DomainKeys Identified Mail)

v=DKIM1; k=rsa; n=1024; p=MIGfMA0GCSqGSIb3DQEBAQUAA4...

Result: DKIM signature verification failed (`DKIM Authenticated: No`)

Reason: Signature mismatch or modification in message content during transmission.

Impact: The email's integrity cannot be verified.

Step 4: DMARC Record Analysis

v=DMARC1; p=none; rua=mailto:dmarc@tpcglobe.co.in;

Policy (p): `none` → No action is taken even if SPF/DKIM fail.

Result: DMARC record published but not enforced.

Interpretation:
This weak policy (`p=none`) allows potentially spoofed or phishing emails to bypass filters.

Step 5: Header Details Verification

- **Return-Path:** `pmd@tpcglobe.co.in`
- **Received-SPF:** pass (Google confirms SPF validation)
- **ARC Authentication Results:** DKIM temporary failure
- **Authentication Results (Summary):**
    - SPF: pass
    - DKIM: fail
    - DMARC: pass (because of `p=none`, not actual compliance)
- **Observation:**
  Despite passing SPF, the failure of DKIM and a non-enforced DMARC make the email **suspect**. The sender's domain (`tpcglobe.co.in`) might be spoofed or misused.

Final Assessment:

The analyzed email shows multiple red flags such as:

- Failed DKIM authentication
- Weak DMARC policy (`p=none`)

- Sender IP found on blacklist

These factors strongly indicate that the email could be a **phishing or spoofed message** sent from an unauthorized mail server.

Conclusion:

Security Mechanism	Result	Status	Risk
SPF	**Passed**	✅	**Low**
DKIM	**Failed**	❌	**High**
DMARC	**Not Enforced**	⚠️	**High**
Blacklist Status	**Blacklisted IP**	❌	**Critical**