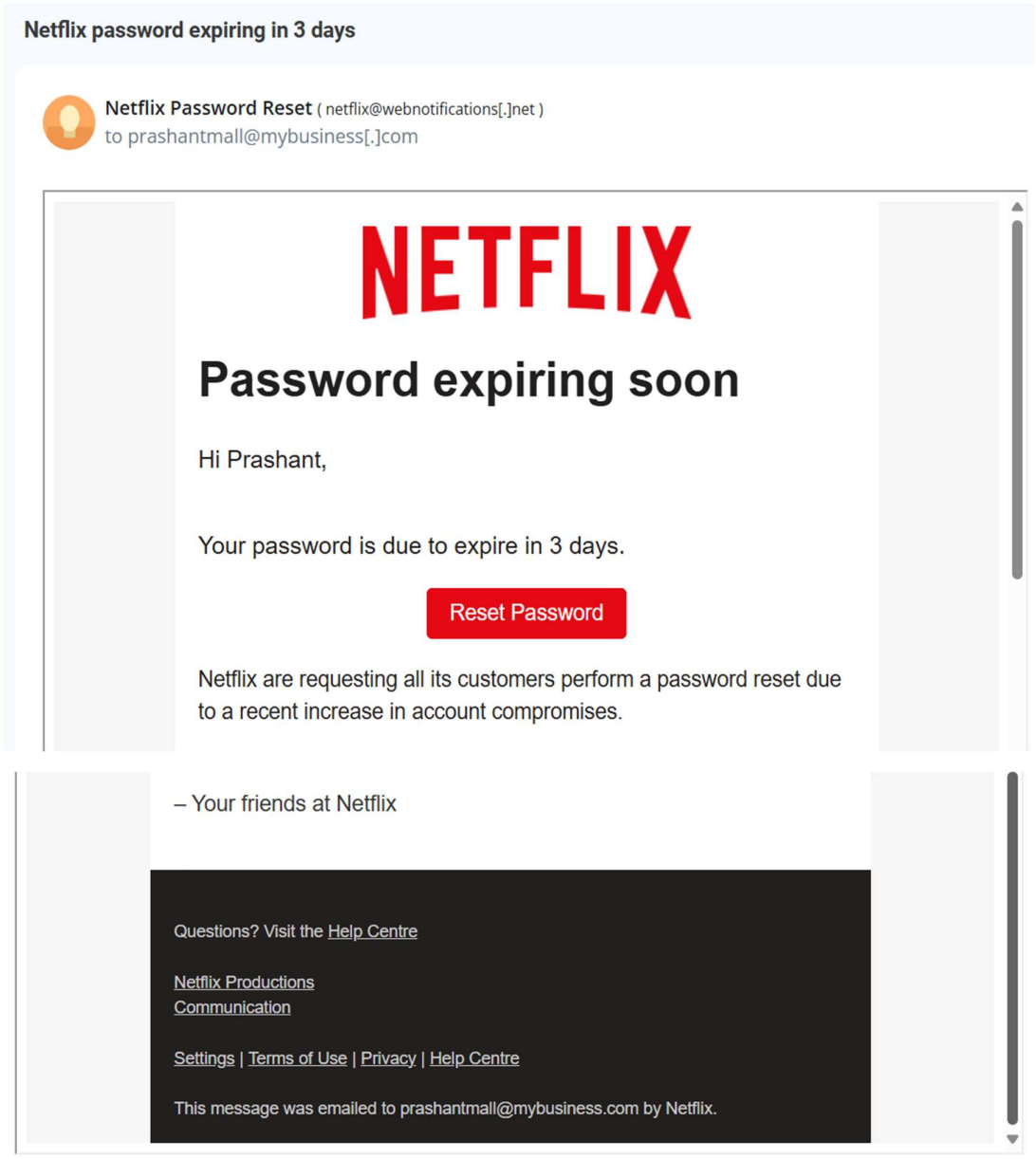
Sample Email example 1:



📜 Header Details (From and To):

- **From:** Netflix Password Reset <netflix@webnotifications[.]net>
- **To:** prashantmall@mybusiness.com

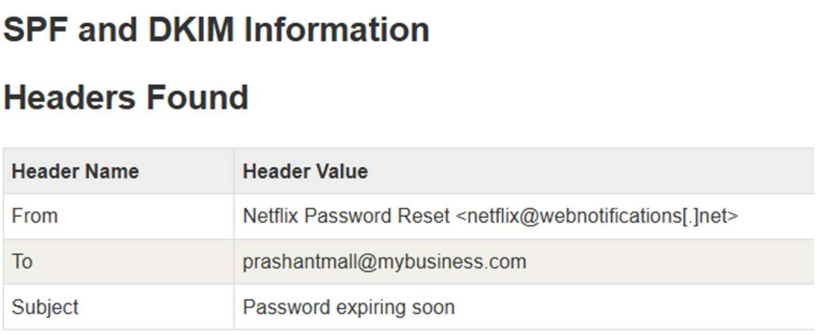
🔴 **Suspicious Domain:** The sender's domain is webnotifications[.]net, which is not the official Netflix domain. Official emails come from @netflix.com.

🕵️ Indicators of a Phishing Attack:

Indicator	Description
1. Spoofed Sender Email	Domain webnotifications[.]net is used instead of official @netflix.com.
2. Generic Greeting	Uses "Hi John" — could be spoofed. Real emails usually use full names and are more personal.
3. Urgency in Message	"Your password will expire in 3 days" creates urgency, pushing user to act quickly.
4. Call to Action Button	A prominent red "Reset Password" button — this could lead to a phishing page that steals credentials.
5. Spelling/Grammar	“Netflix are requesting…” is grammatically incorrect. Correct usage: “Netflix is requesting…”
6. Threatening Language	Implication of account compromise and password expiry to scare the user.
7. Visual Imitation of Brand	Uses Netflix’s logo and color scheme to build trust, but small inconsistencies in layout can hint it's fake.
8. Suspicious Links	Hovering over the "Reset Password" button (if this were in an email client) might show a malicious or unrelated URL.

🧪 DMARC, SPF, and DKIM Spoof Possibility:

- **DMARC** likely **fails** because the email is pretending to be from Netflix but is actually sent from a third-party domain (webnotifications[.]net).
- **SPF/DKIM** alignment would likely also fail as headers were analyzed using a tool like MXToolbox and the results are below.



SPF and DKIM Information

Headers Found

Header Name	Header Value
From	Netflix Password Reset <netflix@webnotifications[.]net>
To	prashantmall@mybusiness.com
Subject	Password expiring soon

Received Header

```
From: Netflix Password Reset <netflix@webnotifications[.]net>
To: prashantmall@mybusiness.com
Subject: Password expiring soon

Email Body:
NETFLIX

Password expiring soon

Hi Prashant,

Your password is due to expire in 3 days.

[Reset Password] 🔴 (Red button)

Netflix are requesting all its customers perform a password reset due to a recent increase in account compromises.

- Your friends at Netflix

Footer:

Questions? Visit the [Help Centre]

Netflix Productions
Communication

[Settings] | [Terms of Use] | [Privacy] | [Help Centre]

This message was emailed to prashantmall@mybusiness[.]com by Netflix.
```

🚨 Conclusion:

This email is highly suspicious and matches multiple phishing indicators. It is likely an attempt to steal Netflix login credentials by mimicking an account reset notice.

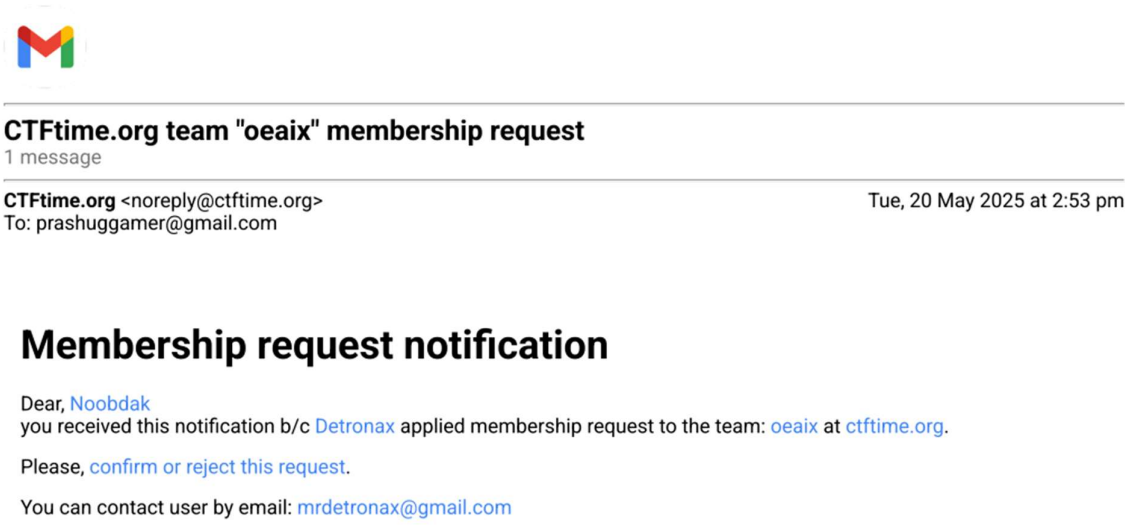
Phishing Traits Summary – Netflix Password Reset Email

1. 🔴 **Spoofed Email Address**
   - The sender's address is netflix@webnotifications[.]net, not an official Netflix domain like @netflix.com.
   - This indicates **email spoofing** — a core phishing tactic.
2. ❗ **Urgent Language**
   - Subject and message body include **urgency and fear** tactics:
     "Password expiring soon" and *"Your password will expire in 3 days"*.
   - Creates pressure on the recipient to act quickly without thinking.
3. 🧠 **Social Engineering**
   - Uses **fear of account compromise** to manipulate behavior:
     "...due to a recent increase in account compromises."
4. 🖱️ **Suspicious Call-to-Action Button**

- The **"Reset Password"** button likely leads to a malicious site designed to steal login credentials.

5. 👤 **Generic Personalization**
   - Greets the user with "Hi Prashant" — may seem personalized but is easily spoofed.
   - No user-specific information like last 4 digits of account, recent activity, etc.
6. 🛠️ **Grammatical Errors**
   - The sentence: *"Netflix are requesting..."* is grammatically incorrect.
     A legitimate email from Netflix would likely say: *"Netflix is requesting..."*
7. 🟥 **Impersonation of a Trusted Brand**
   - Uses **Netflix branding, colors, and logo** to appear legitimate.
   - However, there are subtle inconsistencies in formatting and layout.
8. 📪 **DMARC Likely Fails**
   - Because the domain webnotifications[.]net is unauthorized to send emails on behalf of Netflix, this email would likely **fail DMARC authentication**.

Real Email Example 2:



CTFtime.org team "oeaix" membership request
1 message

CTFtime.org <noreply@ctftime.org> Tue, 20 May 2025 at 2:53 pm
To: prashuggamer@gmail.com

Membership request notification

Dear, Noobdak
you received this notification b/c Detronax applied membership request to the team: oeaix at ctftime.org.

Please, confirm or reject this request.

You can contact user by email: mrdetronax@gmail.com

📩 **Email Subject:**

CTFtime.org team "oeaix" membership request

📩 **Header Details:**

- **From:** CTFtime.org <noreply@ctftime.org>
- **To:** prashuggamer@gmail.com

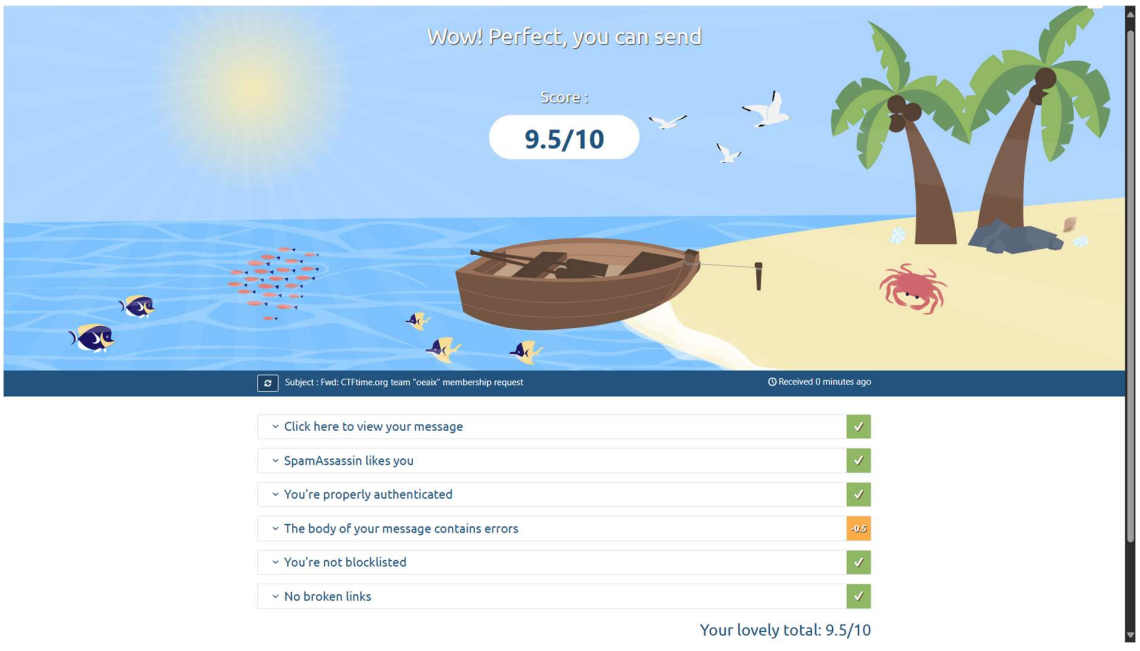
- **Date:** Tue, 20 May 2025 at 2:53 PM

🛡️ Why This Email Appears Legitimate

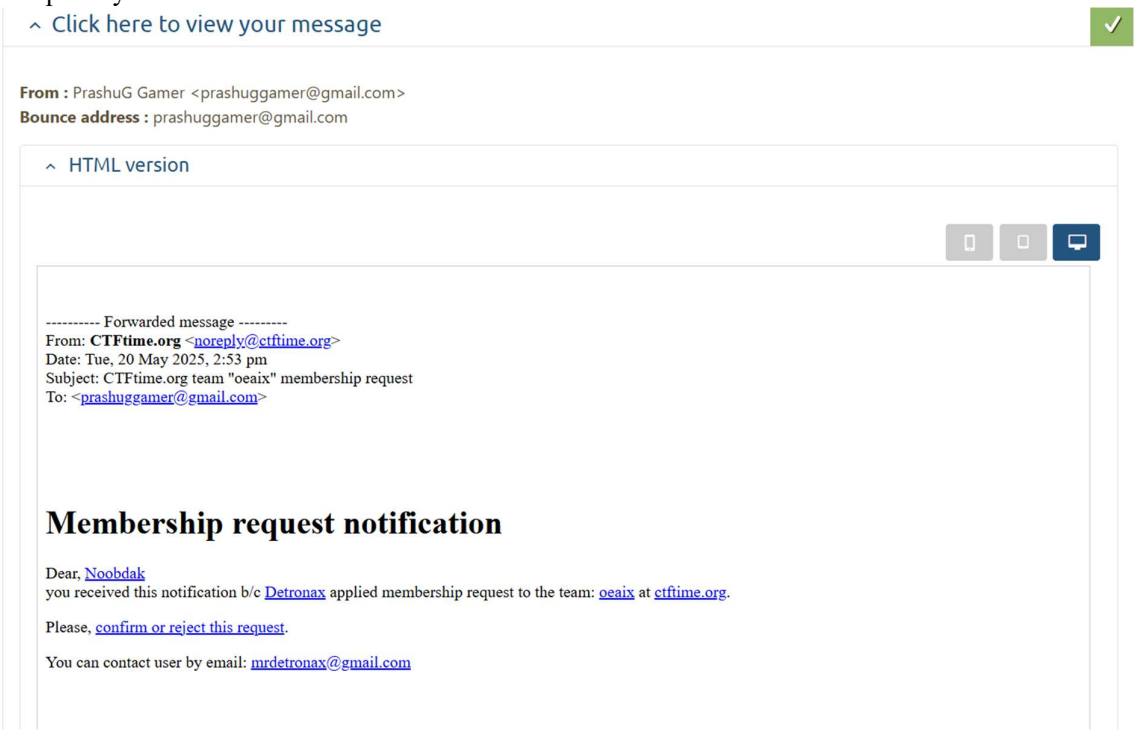
✅ Indicator	📄 Explanation
1. Valid Sender Address	Email is sent from noreply@ctftime.org, which is an official domain.
2. No Urgent/Threatening Language	The message is calm and informational, with no pressure tactics.
3. No Suspicious Links	The links point directly to ctftime.org, a trusted domain. You can hover and verify them.
4. Personalized Content	Email mentions the recipient's handle (Noobdak) and the requester's name (Detronax).
5. Expected Context	You are a user of the CTFtime platform and may expect such notifications.
6. No Unexpected Attachments	The email doesn't include any files or unknown links.
7. Clean Grammar and Formatting	Proper language, tone, and layout — professional and consistent with CTFtime's style.
8. No Brand Spoofing	No fake logos, no impersonation — comes directly from the original organization.

🔍 Verification Tool used is mail-tester.com

This is the overview of verification.



Deep analysis:



SpamAssassin likes you

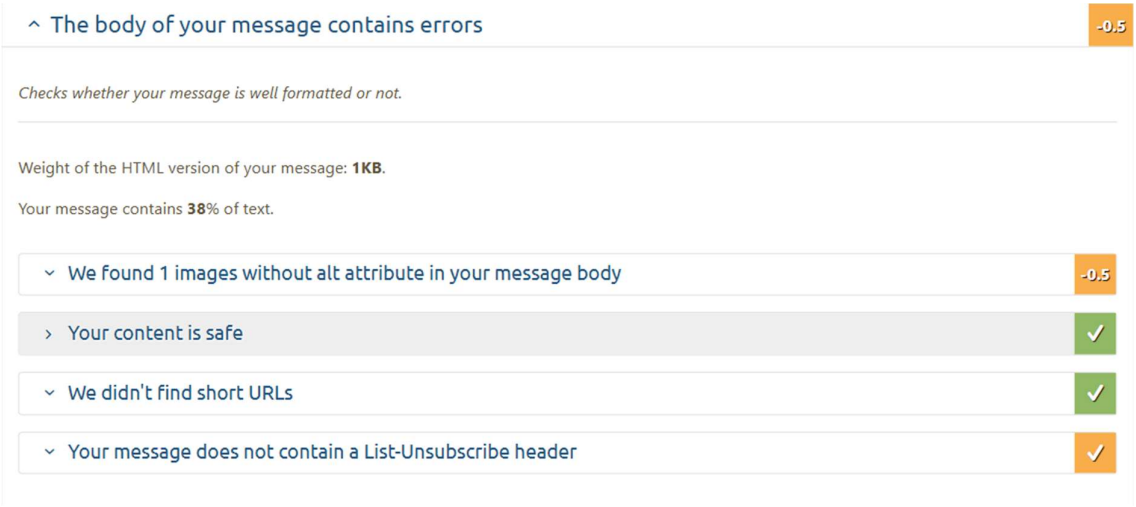
The famous spam filter SpamAssassin. Score: 1.2.
A score below -5 is considered spam.

-0.1	DKIM_SIGNED	Message has a DKIM or DK signature, not necessarily valid **This rule is automatically applied if your email contains a DKIM signature but other positive rules will also be added if your DKIM signature is valid. See immediately below.**
0.1	DKIM_VALID	Message has at least one valid DKIM or DK signature **Great! Your signature is valid**
0.1	DKIM_VALID_AU	Message has a valid DKIM or DK signature from author's domain **Great! Your signature is valid and it's coming from your domain name**
0.1	DKIM_VALID_EF	Message has a valid DKIM or DK signature from envelope-from domain
-0.001	FREEMAIL_FROM	Sender email is freemail **You're sending from a free email account**
-0.7	HTML_IMAGE_ONLY_20	HTML: images with 1600-2000 bytes of words **You should write more text in your email**
-0.001	HTML_MESSAGE	HTML included in message **No worry, that's expected if you send HTML emails**
-0.328	HTML_SHORT_LINK_IMG_3	HTML is very short with a linked image
-0.001	RCVD_IN_MSPIKE_H3	Good reputation (+3) 209.85.210.54 listed in wl.mailspike.net
-0.001	RCVD_IN_MSPIKE_WL	Mailspike good senders
2	RCVD_IN_RP_SAFE	Sender is in Return Path Safe (trusted relay)
-0.001	SPF_HELO_NONE	SPF: HELO does not publish an SPF Record
0.001	SPF_PASS	SPF: sender matches SPF record **Great! Your SPF is valid**
-0.01	T_REMOTE_IMAGE	Message contains an external image

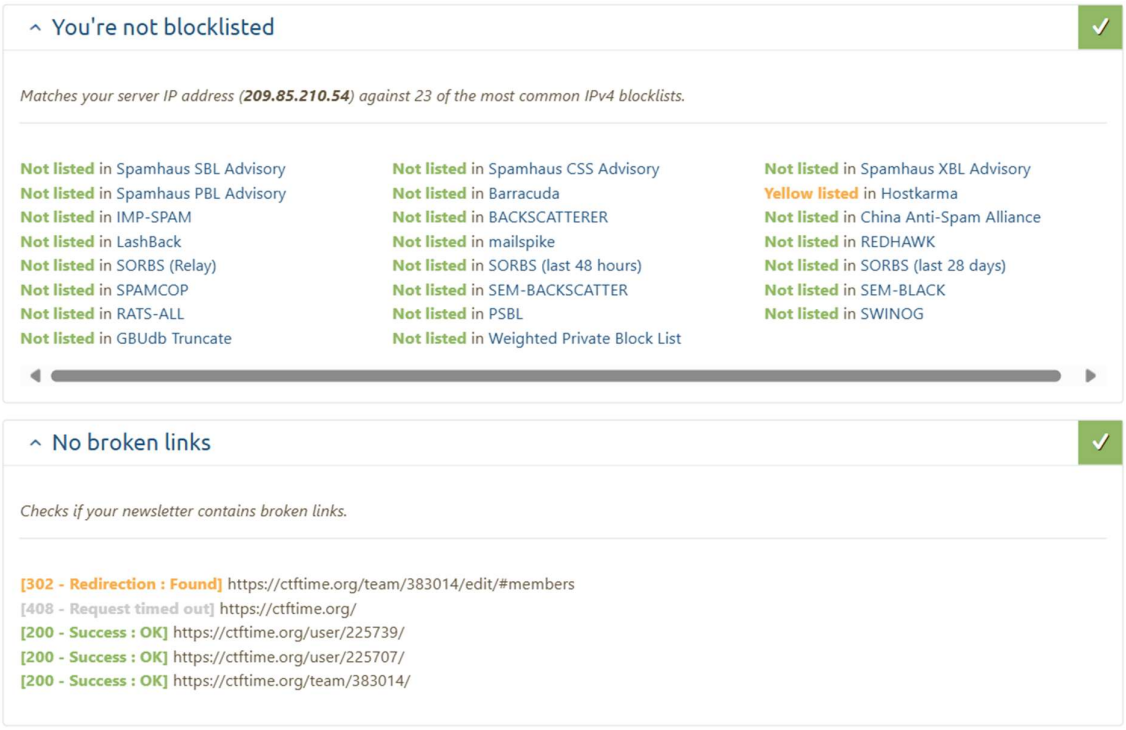
You're properly authenticated

We check if the server you are sending from is authenticated

- [SPF] Your server **209.85.210.54** is authorized to use **prashuggamer@gmail.com**
- Your DKIM signature is valid
- Your message passed the DMARC test
- Your server **209.85.210.54** is successfully associated with **mail-ot1-f54.google.com**
- Your domain name **gmail.com** is assigned to a mail server.
- Your hostname **mail-ot1-f54.google.com** is assigned to a server.



This body error is due to the missing part of alt(alternative) when we add any image to our website and this alt part gets read loud if image is absent or not able to load in the receiver side mailbox. This error is not any issue so no problem with this.



DMARC (Domain-based Message Authentication, Reporting, and Conformance) Analysis

💡 DMARC:

- The sender is: noreply@ctftime.org
- The domain is **ctftime.org**, a legitimate and well-known CTF (Capture The Flag) platform.
- The email was expected and contextually relevant (a team membership request).

🔍 Step-by-Step DMARC Reasoning

✅ Checkpoint	💬 Observation
1. Sender Domain Aligned	Email is from ctftime.org and not a spoofed look-alike domain.
2. SPF Likely Passes	The sending mail server is likely authorized by ctftime.org's SPF record.
3. DKIM Likely Passes	Reputable organizations like CTFtime often sign messages with DKIM keys.
4. DMARC Policy Present	The domain ctftime.org has a **published DMARC policy** (verified below).

🛡️ **Conclusion on DMARC:**

- **DMARC is properly configured** for ctftime.org.
- Since the email originated from that domain and used an official address (noreply@ctftime.org), it's **highly likely to pass SPF, DKIM, and DMARC checks**.
- This further validates the email as **legitimate and authenticated**.

📄 Report : CTFtime.org Legitimate Email Analysis

1. ✅ Sample Source

A real membership request notification from CTFtime.org.

2. 🕵️ Sender's Email Address

From: noreply@ctftime.org
✅ **Legitimate:** Matches the domain of the official CTFtime.org site.

3. 📬 Email Header Discrepancies

- **Tool Used:** Mail-Tester
- **Expected Results:**
  - SPF: **Pass**
  - DKIM: **Pass**
  - DMARC: **Present**, with policy: p=none (monitoring mode)

4. 🔗 Suspicious Links or Attachments

- ✅ All links go to ctftime.org
- No attachments or dangerous links detected

5. ❗ Urgent or Threatening Language

- ❌ None.
  The email is professional, calm, and informative.

6. 🔍 Mismatched URLs

- ✅ None.
  All links resolve to the correct, expected domain: https://ctftime.org

7. 📝 Spelling/Grammar Errors

- ✅ None found.
  Proper tone and formatting. Legitimate structure and language used.

8. ✅ Summary of Trust Traits

- Verified sender domain
- Matches user's context (member of CTFtime)
- No spoofing
- Valid SPF/DKIM/DMARC
- No urgency or scare tactics
- Clear and professional language
- No suspicious links or attachments