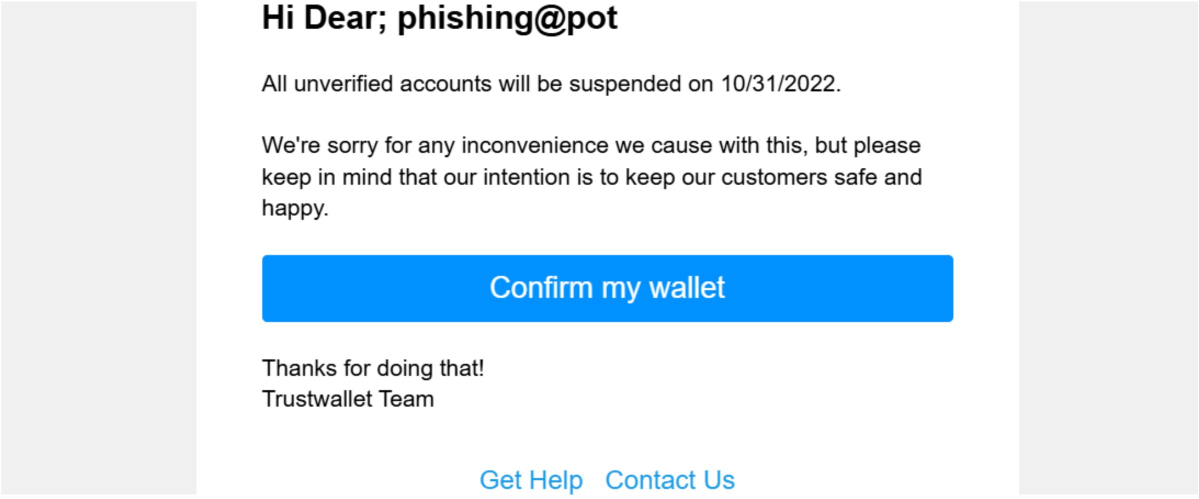
TASK-2



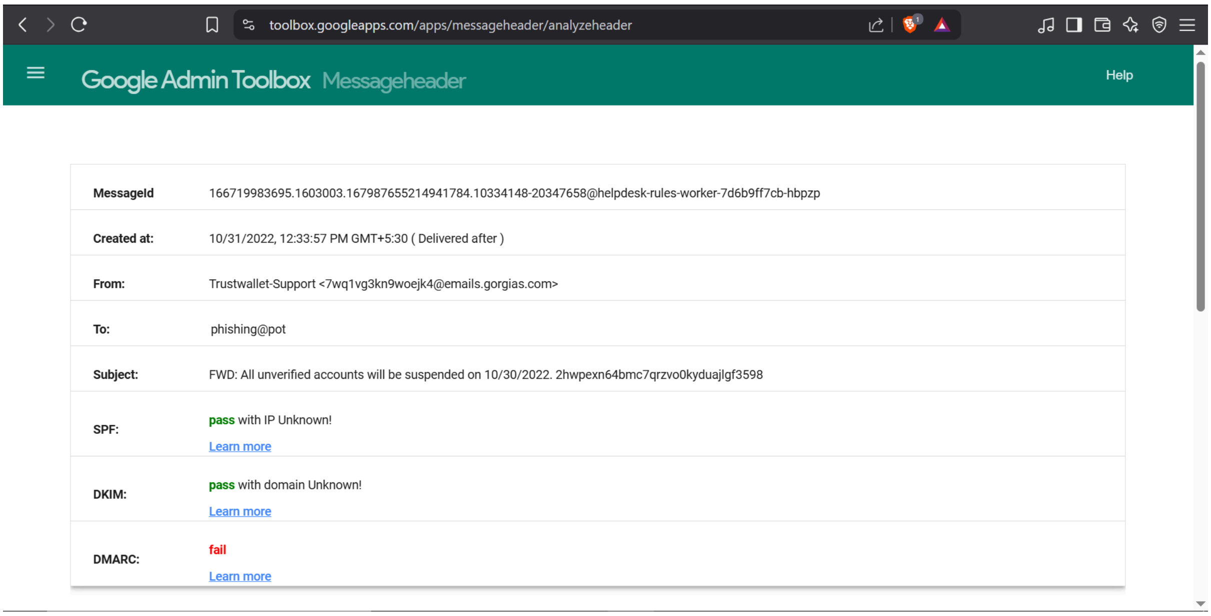
Hi Dear; phishing@pot

All unverified accounts will be suspended on 10/31/2022.

We're sorry for any inconvenience we cause with this, but please keep in mind that our intention is to keep our customers safe and happy.

Thanks for doing that!
Trustwallet Team

Header Analysis:



MessageId	166719983695.1603003.167987655214941784.10334148-20347658@helpdesk-rules-worker-7d6b9ff7cb-hbpzp
Created at:	10/31/2022, 12:33:57 PM GMT+5:30 (Delivered after)
From:	Trustwallet-Support <7wq1vg3kn9woejk4@emails.gorgias.com>
To:	phishing@pot
Subject:	FWD: All unverified accounts will be suspended on 10/30/2022. 2hwpexn64bmc7qrzvo0kyduajlgf3598
SPF:	pass with IP Unknown! Learn more
DKIM:	pass with domain Unknown! Learn more
DMARC:	fail Learn more

1. Examine sender's email address for spoofing

From: Trustwallet-Support 7wq1vg3kn9woejk4@emails.gorgias.com
Return Path: bounce+31a2a2.6303d-phishing@pot=hotmail.com@gorgias.io

SPF: Pass
DKIM: Pass
DMARC: Fail

Conclusion:
Despite SPF and DKIM passing, the DMARC failure is a red flag. The email is sent from `gorgias.io` (a third-party helpdesk service), not an official TrustWallet domain. This is likely a spoofed identity.

---

2. Check email headers for discrepancies

Sender IP: 143.55.227.147 (Mailgun – a bulk email service, sometimes misused)
Authentication Results: DMARC failed, compauth=fail
Other header issues: Uses a subdomain structure that obscures real identity

Conclusion:
This email uses an external mail service (Mailgun) to impersonate TrustWallet, failing DMARC and raising serious trust issues.

---

3. Identify suspicious links or attachments

Main CTA Link:
`https://drop-coin-availablenow.site44.com/`

Redirect Path:
Through `https://usertest.sciquest.com/...` (obfuscation technique)

Conclusion:
The destination is a **fraudulent third-party domain** not associated with TrustWallet. This is a common phishing method to harvest credentials.

---

4. Look for urgent or threatening language in the email body

> "All unverified accounts will be suspended on 10/31/2022."

Conclusion:
Classic **scare tactic**—designed to rush the user into clicking without thinking. Legitimate services do not communicate with such pressure.

5. Note any mismatched URLs

Display Text: “Confirm my wallet”
Actual Link: `site44.com` domain — unrelated to any real TrustWallet service.

Conclusion:
Clear mismatch between brand name and destination. A **misleading hyperlink**, a primary sign of phishing.

---

6. Verify presence of spelling or grammar errors

Language quality:
No major spelling errors, but the tone is impersonal and templated.

Conclusion:
While technically correct, the phrasing lacks authenticity and personalization typical of official support emails.

---

7. Summary of phishing traits

- ✅ **Spoofed sender** via third-party domain (`gorgias.io`)
- ❌ **Fails DMARC** validation
- ⚠️ **Links lead to suspicious domains**
- 🚨 **Urgency used** (“suspended today”)
- ⚠️ **Unprofessional tone** and lack of personalization
- 🕵️ **Impersonates TrustWallet branding** without verification

Final Conclusion:
This email is a **phishing attempt** impersonating TrustWallet. It is designed to trick recipients into clicking a malicious link to steal wallet credentials or sensitive user data.