# Phishing Email Detection & Awareness Report

Phishing Detection & Awareness

Prepared by:

**RASANI LAKSHMI CHARANYA**

Future Interns Project

Cybersecurity Task 2

# OBJECTIVE

The objective of this task is to analyze a phishing email sample, identify malicious indicators, classify associated risks, and provide awareness guidelines to help users recognize and prevent phishing attacks

# Phishing Email Sample

## Email Sample Evidence

A suspicious email pretending to be from PayPal was analyzed. The email requests the user to verify account information through a provided link, which is a common phishing technique used to steal user credentials.

# Email Header Analysis

The email header was analyzed using an online header analysis tool. The analysis showed authentication and domain inconsistencies, indicating that the email was not sent from an official PayPal server and may be malicious.

# Domain and Link Inspection

The email contains a hyperlink directing users to a suspicious domain that imitates PayPal but does not belong to the official PayPal website. Further investigation using Kali Linux tools revealed suspicious domain details, confirming phishing activity.

# Phishing Indicators Identified

## Phishing Indicators

Several phishing indicators were identified in the email:

- Fake sender domain
- Urgent action request
- Suspicious verification link
- Generic greeting message
- Account suspension warning

These signs indicate phishing behavior.

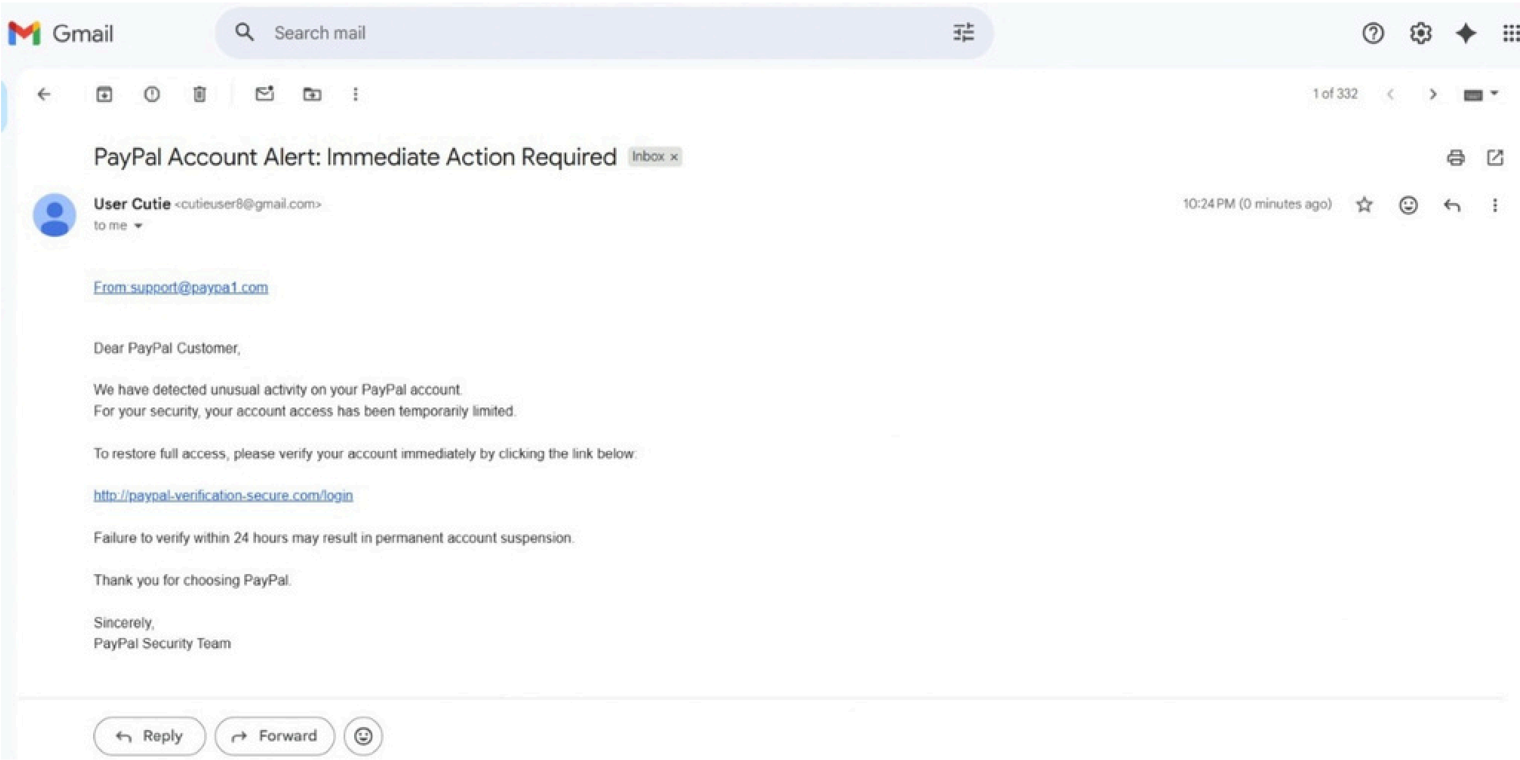
# Risk Classification

The analyzed email is classified as Phishing (High Risk) because it attempts to deceive users into providing sensitive account information through a malicious link.

# Attack Explanation

In this phishing attack, the attacker impersonates a trusted organization and sends fake emails to users. Victims are tricked into clicking malicious links and entering login credentials, which are then stolen by attackers.

# Phishing Email Sample



PayPal Account Alert: Immediate Action Required

**User Cutie** <cutieuser8@gmail.com>
to me

10:24 PM (0 minutes ago)

From: support@paypa1.com

Dear PayPal Customer,

We have detected unusual activity on your PayPal account.
For your security, your account access has been temporarily limited.

To restore full access, please verify your account immediately by clicking the link below:

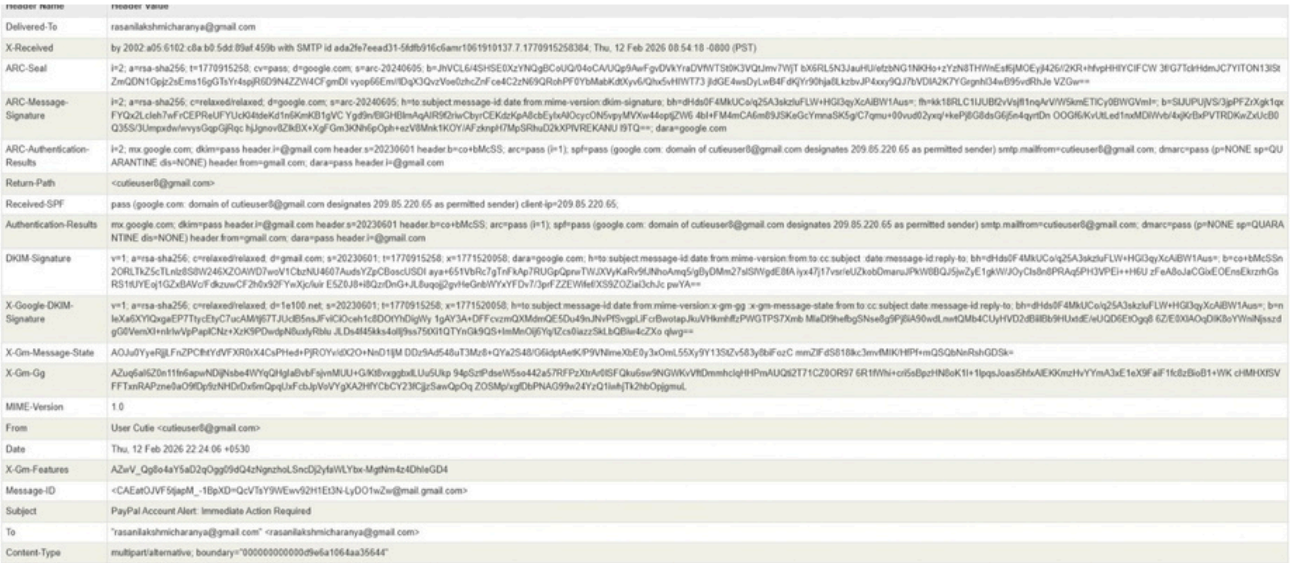
http://paypal-verification-secure.com/login

Failure to verify within 24 hours may result in permanent account suspension.

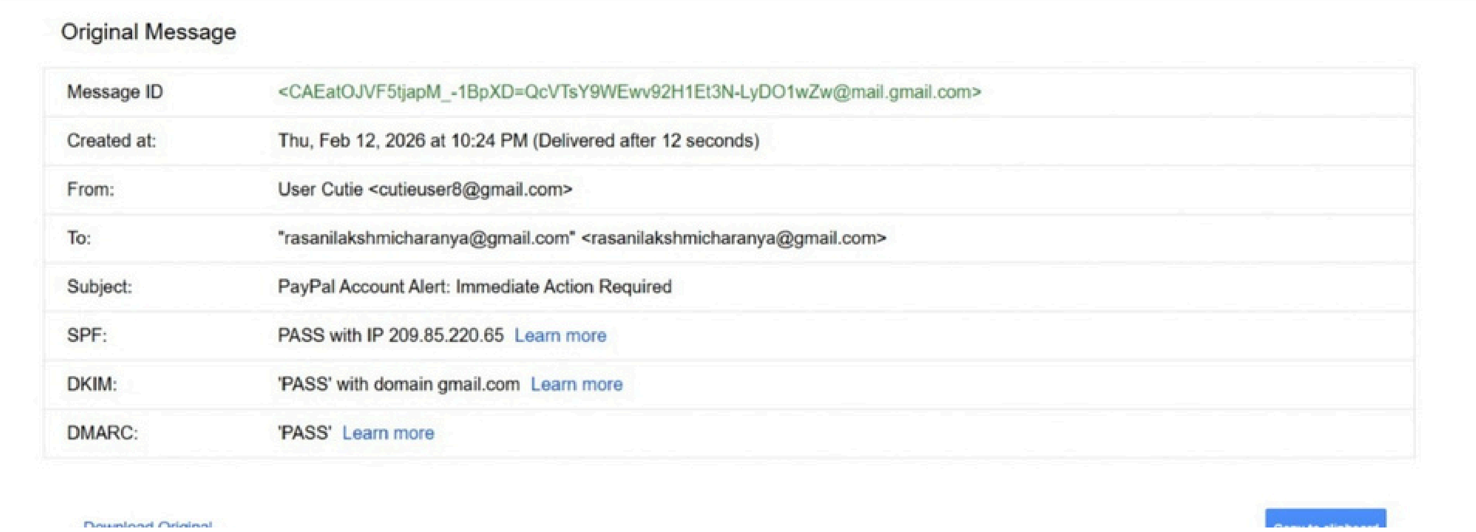
Thank you for choosing PayPal.

Sincerely,
PayPal Security Team

# Email Header Analysis



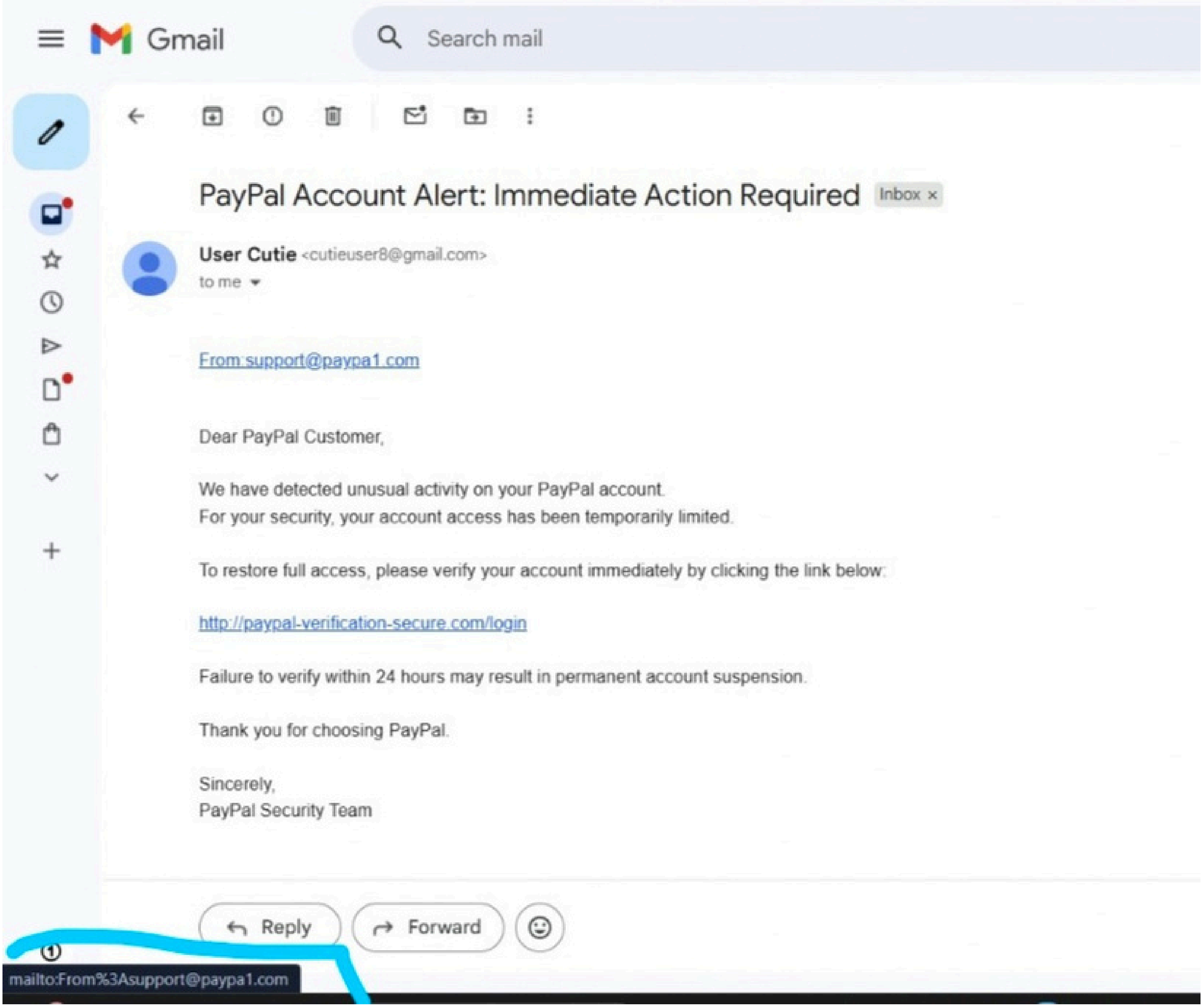
| Header Name | Header Value |
|---|---|
| Delivered-To | rasanilakshmicharanya@gmail.com |
| X-Received | by 2002:a05:6102:c8a:b0:5dd:89af:459b with SMTP id ada2fe7eead31-5fdfb916c6amr1061910137.7.1770915258384; Thu, 12 Feb 2026 08:54:18 -0800 (PST) |
| ARC-Seal | i=2; a=rsa-sha256; t=1770915258; cv=pass; d=google.com; s=arc-20240605; b=JhVCL6/4SHSE0XzYNQgBCoUQ/04oCA/UQp9AwFgvDVkYraDVfWTSt0K3VQtJmv7WjT bX6RL5N3JauHU/efzbNG1NKHo+zYzN8THWnEsf6jMOEyjl426//2KR+hfvpHHIYCIFCW 3fG7TclrHdmJC7YITON13lSt ZmQDN1Gpjz2sEms16gGTsYr4spjR6D9N4ZZW4CFgmDI vyop66Em/lDqX3QvzVoe0zhcZnFce4C2zN69QRohPF0YbMabKdtXyv6/Qhx5vHIWT73 jldGE4wsDyLwB4FdKjYr90hja8LkzbvJP4xxy9QJ7bVDIA2K7YGrgnhl34wB95vdRhJe VZGw== |
| ARC-Message-Signature | i=2; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=to:subject:message-id:date:from:mime-version:dkim-signature; bh=dHds0F4MkUCo/q25A3skzluFLW+HGl3qyXcAlBW1Aus=; fh=kk18RLC1lJUBf2vVsjfl1nqArV/W5kmETlCy0BWGVml=; b=SlJUPUjVS/3jpPFZrXgk1qx FYQx2Lcleh7wFrCEPReUFYUcK04tdeKd1n6KmKB1gVC Ygd9n/BlGHBlmAqAIR9f2riwCbyrCEKdzKpA8cbEylxAlOcycON5vpyMVXw44optjZW6 4bl+FM4mCA6m89JSKeGcYmnaSK5g/C7qmu+00vud02yxq/+kePj8G8dsG6j5n4qyrtDn OOGf6/KvUtLed1nxMDiWvb/4xjKrBxPVTRDKwZxUcB0 Q35S/3UmpxdwlwvysGqpGjRqc hJJgnov8ZlkBX+XgFGm3KNh6pOph+ezV8Mnk1KOY/AFzknpH7MpSRhuD2kXPlVREKANU I9TQ==; dara=google.com |
| ARC-Authentication-Results | i=2; mx.google.com; dkim=pass header.i=@gmail.com header.s=20230601 header.b=co+bMcSS; arc=pass (i=1); spf=pass (google.com: domain of cutieuser8@gmail.com designates 209.85.220.65 as permitted sender) smtp.mailfrom=cutieuser8@gmail.com; dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com; dara=pass header.i=@gmail.com |
| Return-Path | <cutieuser8@gmail.com> |
| Received-SPF | pass (google.com: domain of cutieuser8@gmail.com designates 209.85.220.65 as permitted sender) client-ip=209.85.220.65; |
| Authentication-Results | mx.google.com; dkim=pass header.i=@gmail.com header.s=20230601 header.b=co+bMcSS; arc=pass (i=1); spf=pass (google.com: domain of cutieuser8@gmail.com designates 209.85.220.65 as permitted sender) smtp.mailfrom=cutieuser8@gmail.com; dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com; dara=pass header.i=@gmail.com |
| DKIM-Signature | v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=20230601; t=1770915258; x=1771520058; dara=google.com; h=to:subject:message-id:date:from:mime-version:from:to:cc:subject :date:message-id:reply-to; bh=dHds0F4MkUCo/q25A3skzluFLW+HGl3qyXcAlBW1Aus=; b=co+bMcSSn 2ORLTkZ5cTLnlz8S8W246XZOAWD7woV1CbzNU4607AudsYZpCBoscUSDI aya+651VbRc7gTnFkAp7RUGpQprwTWJXVyKaRv9fJNhoAmq5/gByDMm27slSlWgdE8fA iyx47j17vsr/eUZkobDmaruJPkW8BQJ5jwZyE1gkW/JOyCls8n8PRAq5PH3VPEi++H6U zFeA8oJaCGixEOEnsEkrzrhGs RS1tUYEoj1GZxBAVc/FdkzuwCF2h0x92FYwXjc/luir E5Z0J8+i8QzrDnG+JL8uqojj2gvHeGnbWYxYFDv7/3prFZZEWifel/XS9ZOZiai3chJc pwYA== |
| X-Google-DKIM-Signature | v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20230601; t=1770915258; x=1771520058; h=to:subject:message-id:date:from:mime-version:x-gm-gg :x-gm-message-state:from:to:cc:subject:date:message-id:reply-to; bh=dHds0F4MkUCo/q25A3skzluFLW+HGl3qyXcAlBW1Aus=; b=n leXa6XYlQxgaEP7TtycEtyC7ucAM/tj67TJUclB5nsJFvlCiOceh1c8DOtYhDigWy 1gAY3A+DFFcvzmQXMdmQE5Du49nJNvPfSvgpLiFcrBwotapJkuVHkmhffzPWGTPS7Xmb MlaDf9hefbgSNse8g9Pj8iA90wdLnwtQMb4CUyHVD2dBilBb9HUxtdE/eUQD6EtOgq8 6Z/E0XlAOqDlK8oYWniNjsszd gG0VemXl+nlrlwVpPaplCNz+XzK9PDwdpN8uxlyRblu JLDs4f45kks4olIj9ss750Xl1QTYnGk9QS+lmMnOlj6Yq/lZcs0iazzSkLbQBiw4cZXo qlwg== |
| X-Gm-Message-State | AOJu0YyeRjjLFnZPCfhtYdVFXR0rX4CsPHed+PjROYv/dX2O+NnD1ljM DDz9Ad548uT3Mz8+QYa2S48/G6ldptAetK/P9VNlmeXbE0y3xOmL55Xy9Y13StZv583y8biFozC mmZlFdS818lkc3mvfMIK/HfPf+mQSQbNnRshGDSk= |
| X-Gm-Gg | AZuq6al6Z0n11fn6apwNDijNsbe4WYqQHglaBvbFsjvnMUU+G/Kt8vxggbxlLUu5Ukp 94pSztPdseW5so442a57RFPzXtrAr0lSFQku6sw9NGWKvVftDmmhclqHHPmAUQti2T71CZ0OR97 6R1fWhi+cri5sBpzHN8oK1l+1lpqsJoasi5hfxAlEKKmzHvYYmA3xE1eX9FaiF1fc8zBioB1+WK cHMHXfSV FFTxnRAPzne0aO9fDp9zNHDrDx6mQpqUxFcbJpVoVYgXA2HfYCbCY23fCjjzSawQpOq ZOSMp/xgfDbPNAG99w24YzQ1iwhjTk2hbOpjgmuL |
| MIME-Version | 1.0 |
| From | User Cutie <cutieuser8@gmail.com> |
| Date | Thu, 12 Feb 2026 22:24:06 +0530 |
| X-Gm-Features | AZwV_Qg8o4aY5aD2qOgg09dQ4zNgnzhoLSncDj2yfaWLYbx-MgtNm4z4DhleGD4 |
| Message-ID | <CAEatOJVF5tjapM_-1BpXD=QcVTsY9WEwv92H1Et3N-LyDO1wZw@mail.gmail.com> |
| Subject | PayPal Account Alert: Immediate Action Required |
| To | "rasanilakshmicharanya@gmail.com" <rasanilakshmicharanya@gmail.com> |
| Content-Type | multipart/alternative; boundary="000000000000d9e6a1064aa35644" |



Original Message

| | |
|---|---|
| Message ID | <CAEatOJVF5tjapM_-1BpXD=QcVTsY9WEwv92H1Et3N-LyDO1wZw@mail.gmail.com> |
| Created at: | Thu, Feb 12, 2026 at 10:24 PM (Delivered after 12 seconds) |
| From: | User Cutie <cutieuser8@gmail.com> |
| To: | "rasanilakshmicharanya@gmail.com" <rasanilakshmicharanya@gmail.com> |
| Subject: | PayPal Account Alert: Immediate Action Required |
| SPF: | PASS with IP 209.85.220.65 Learn more |
| DKIM: | 'PASS' with domain gmail.com Learn more |
| DMARC: | 'PASS' Learn more |

# Domain and Link Inspection



PayPal Account Alert: Immediate Action Required

**User Cutie** <cutieuser8@gmail.com>
to me

From:support@paypa1.com

Dear PayPal Customer,

We have detected unusual activity on your PayPal account.
For your security, your account access has been temporarily limited.

To restore full access, please verify your account immediately by clicking the link below:

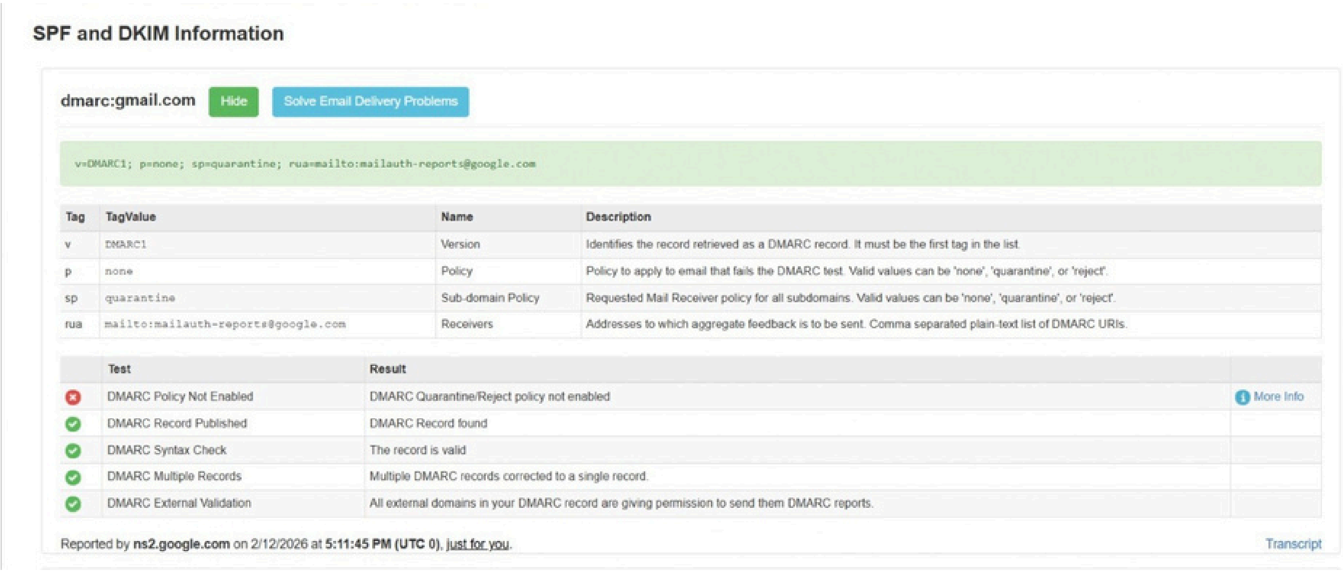
http://paypal-verification-secure.com/login

Failure to verify within 24 hours may result in permanent account suspension.

Thank you for choosing PayPal.

Sincerely,
PayPal Security Team

mailto:From%3Asupport@paypa1.com



SPF and DKIM Information

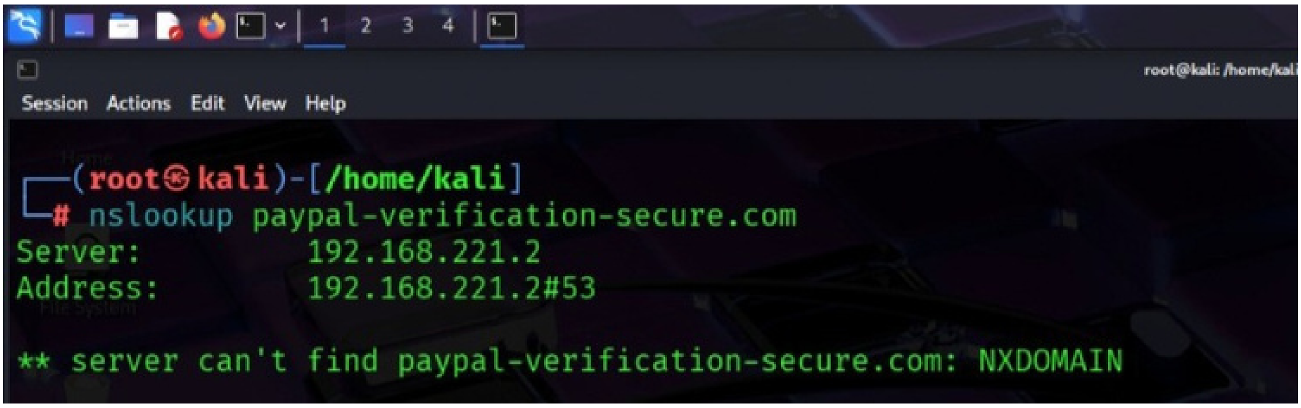
dmarc:gmail.com

```
v=DMARC1; p=none; sp=quarantine; rua=mailto:mailauth-reports@google.com
```

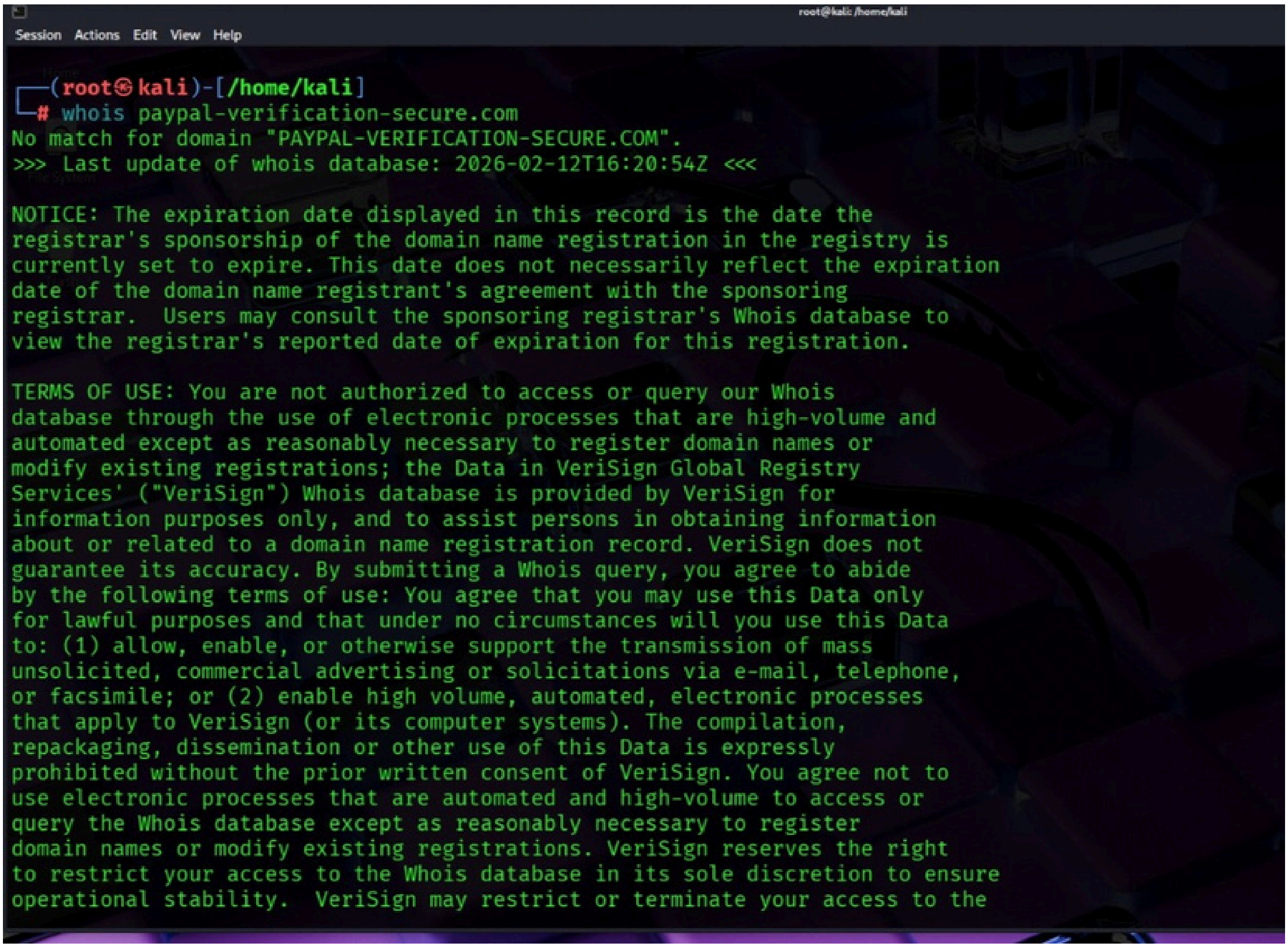
| Tag | TagValue | Name | Description |
|---|---|---|---|
| v | DMARC1 | Version | Identifies the record retrieved as a DMARC record. It must be the first tag in the list. |
| p | none | Policy | Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'. |
| sp | quarantine | Sub-domain Policy | Requested Mail Receiver policy for all subdomains. Valid values can be 'none', 'quarantine', or 'reject'. |
| rua | mailto:mailauth-reports@google.com | 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 | ℹ 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. |  |

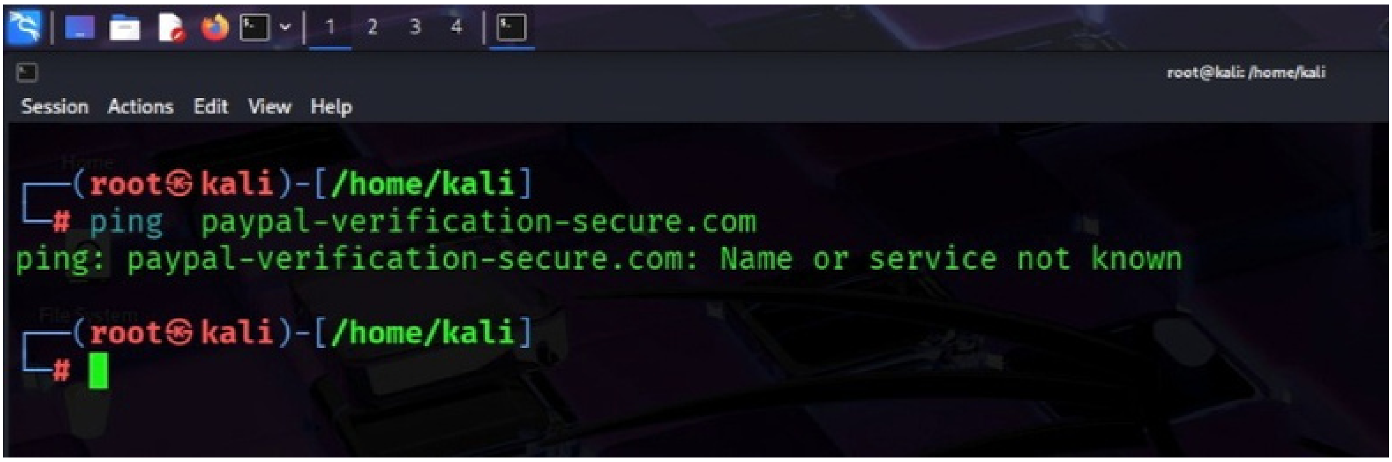
Reported by **ns2.google.com** on 2/12/2026 at **5:11:45 PM (UTC 0)**, just for you.



```
┌──(root㉿kali)-[/home/kali]
└─# nslookup paypal-verification-secure.com
Server:         192.168.221.2
Address:        192.168.221.2#53

** server can't find paypal-verification-secure.com: NXDOMAIN
```



```
┌──(root㉿kali)-[/home/kali]
└─# whois paypal-verification-secure.com
No match for domain "PAYPAL-VERIFICATION-SECURE.COM".
>>> Last update of whois database: 2026-02-12T16:20:54Z <<<

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
```



```
┌──(root㉿kali)-[/home/kali]
└─# ping  paypal-verification-secure.com
ping: paypal-verification-secure.com: Name or service not known

┌──(root㉿kali)-[/home/kali]
└─# 
```

# Prevention Guidelines

Users can protect themselves from phishing attacks by following these practices:

- Do not click links from unknown or suspicious emails.
- Verify sender email domains carefully.
- Enable Two-Factor Authentication (2FA).
- Report suspicious emails immediately.
- Never share passwords or OTP with anyone.

# Conclusion

This analysis demonstrates how phishing emails operate and highlights the importance of user awareness and cautious behavior to protect personal and organizational data from cyber threats.