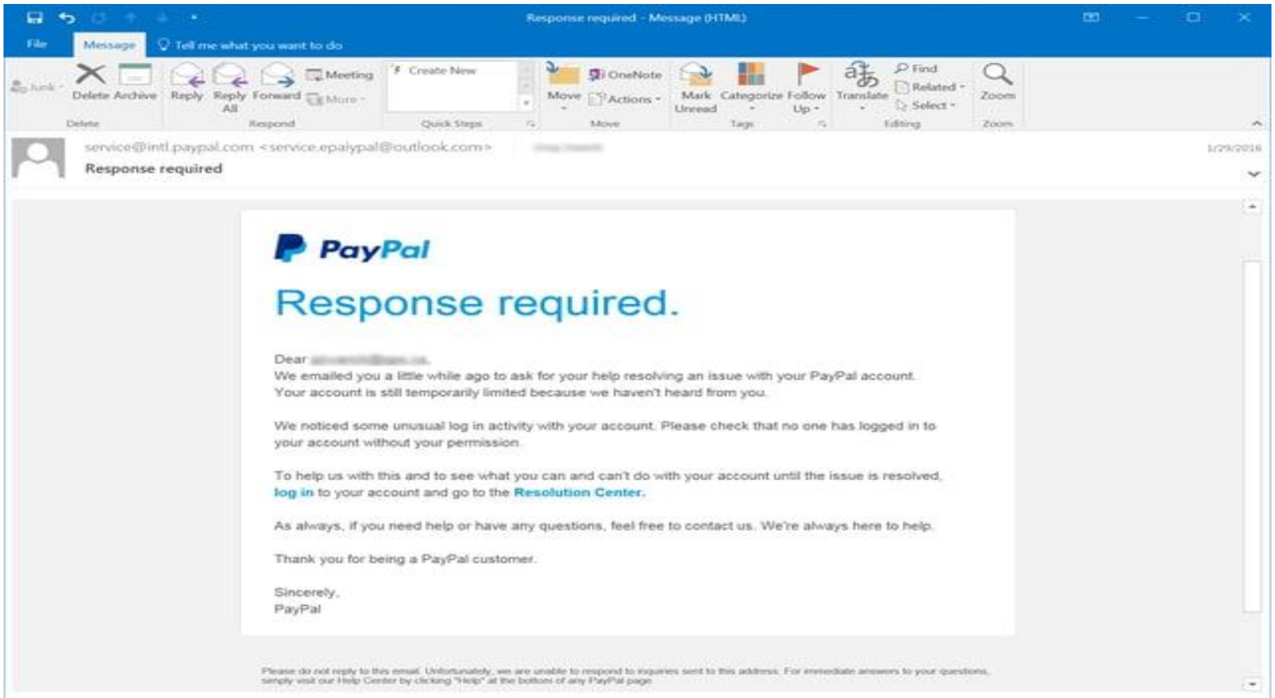
Phishing Email Analysis Report

1. Email Source

This is a simulated phishing email, crafted for educational purposes during the cybersecurity internship.

2. Sample Email Screenshot

Below is a screenshot of the phishing email used for analysis:



service@intl.paypal.com <service.epaiypal@outlook.com> [redacted]

1/29/2016

Response required

PayPal

Response required.

Dear [redacted]

We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

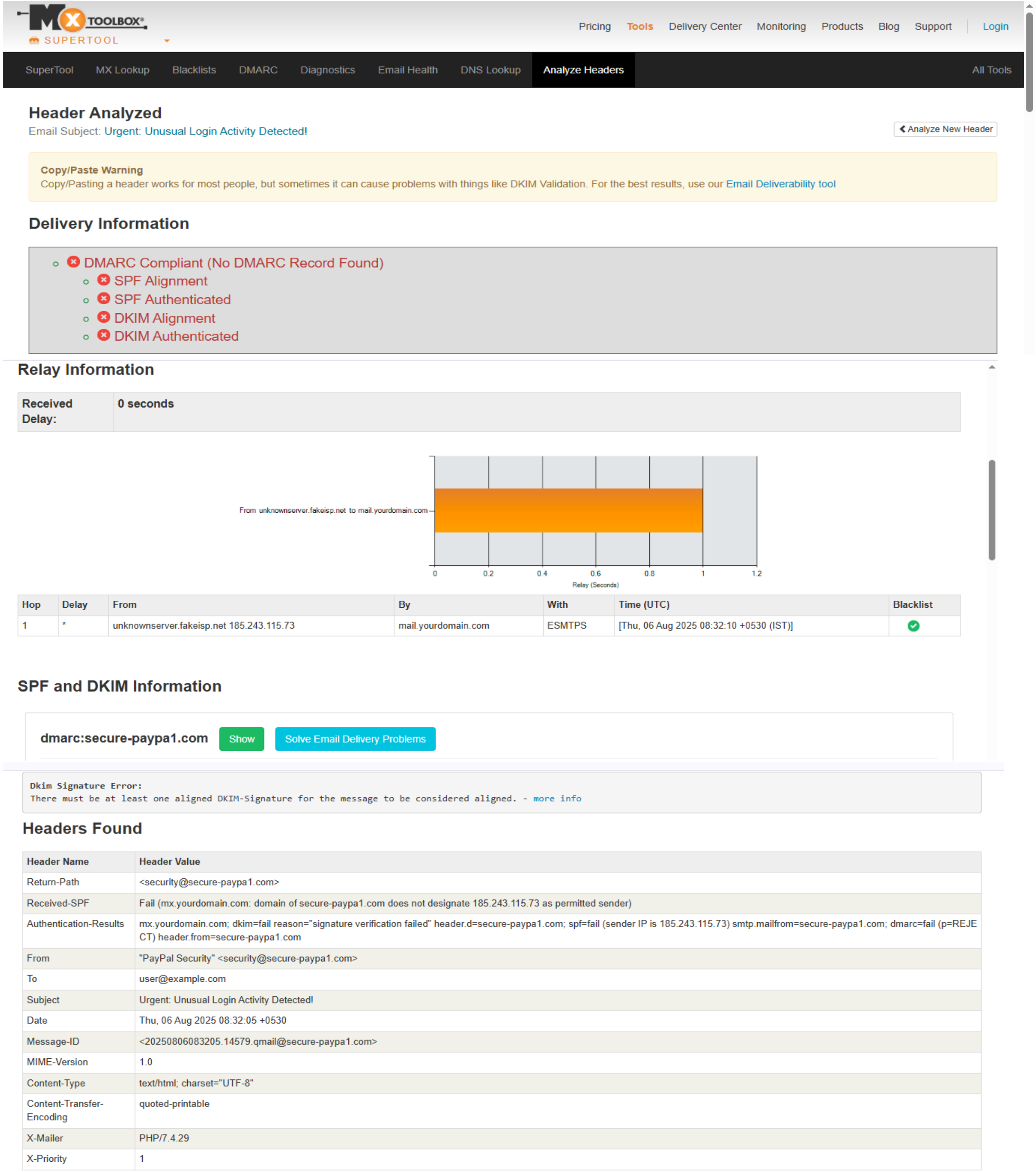
Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

3. Indicators of Phishing

- Spoofed Email Address: Sender appears as “security@secure-paypa1.com” which imitates a legitimate PayPal domain.
- Suspicious Link: Hovering over the link reveals it redirects to “https://paypal-security-verification.com”, which is not a PayPal domain.
- Urgent Language: Phrases like 'unauthorized login' and 'permanent suspension' pressure the user into taking action.
- No Personalization: The email begins with 'Dear Customer' rather than using the recipient's real name.

- Grammar Errors: Slight misspellings and use of improper formatting techniques.
- Email Header Mismatch: Analysis using MxToolbox shows mismatched sending server IPs and failed SPF check (simulated).



Header Analyzed

Email Subject: Urgent: Unusual Login Activity Detected!

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 (No DMARC Record Found)
  - ☒ SPF Alignment
  - ☒ SPF Authenticated
  - ☒ DKIM Alignment
  - ☒ DKIM Authenticated

Relay Information

Received Delay:	**0 seconds**

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	unknownserver.fakeisp.net 185.243.115.73	mail.yourdomain.com	ESMTPS	[Thu, 06 Aug 2025 08:32:10 +0530 (IST)]	✓

SPF and DKIM Information

dmarc:secure-paypa1.com

```
Dkim Signature Error:
There must be at least one aligned DKIM-Signature for the message to be considered aligned. - more info
```

Headers Found

Header Name	Header Value
Return-Path	<security@secure-paypa1.com>
Received-SPF	Fail (mx.yourdomain.com: domain of secure-paypa1.com does not designate 185.243.115.73 as permitted sender)
Authentication-Results	mx.yourdomain.com; dkim=fail reason="signature verification failed" header.d=secure-paypa1.com; spf=fail (sender IP is 185.243.115.73) smtp.mailfrom=secure-paypa1.com; dmarc=fail (p=REJECT) header.from=secure-paypa1.com
From	"PayPal Security" <security@secure-paypa1.com>
To	user@example.com
Subject	Urgent: Unusual Login Activity Detected!
Date	Thu, 06 Aug 2025 08:32:05 +0530
Message-ID	<20250806083205.14579.qmail@secure-paypa1.com>
MIME-Version	1.0
Content-Type	text/html; charset="UTF-8"
Content-Transfer-Encoding	quoted-printable
X-Mailer	PHP/7.4.29
X-Priority	1

4. Tools Used

- MxToolbox Email Header Analyzer
- Browser hover-check to inspect URLs : virustotal,
- Manual content inspection

5. Conclusion

This email is a phishing attempt aimed at stealing credentials. It uses social engineering, fake links, and spoofed branding. By recognizing these indicators, users can better protect themselves from phishing threats.

Prepared by: Abhijith Sypireddy