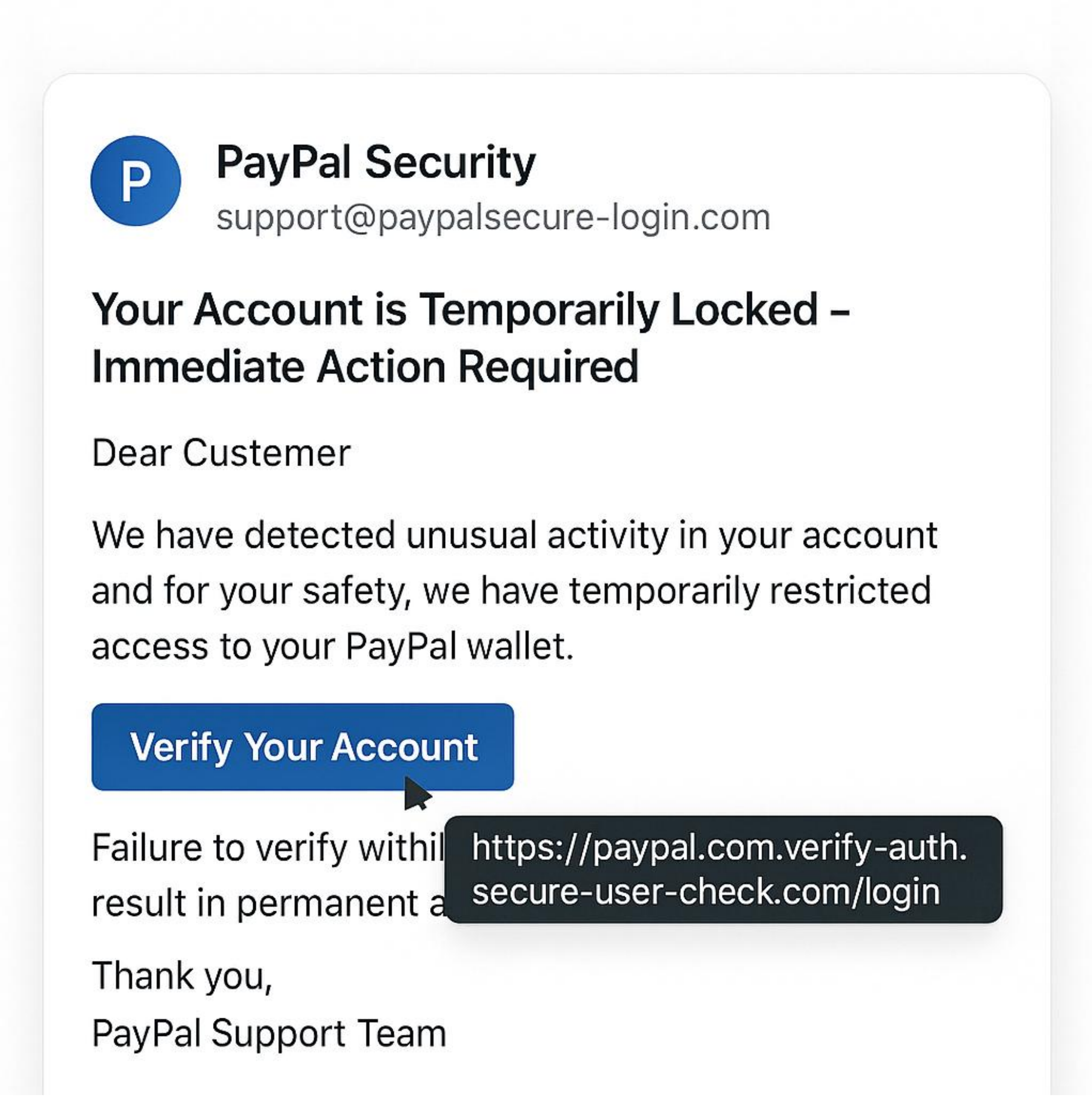
Cyber Security Internship

Task2: Analyzing a Phishing email sample

Scenario: Your account is temporarily locked – immediate action required received from "PayPal Security" <support@paypalsecure-login.com>



PayPal Security
support@paypalsecure-login.com

Your Account is Temporarily Locked – Immediate Action Required

Dear Custemer

We have detected unusual activity in your account and for your safety, we have temporarily restricted access to your PayPal wallet.

Failure to verify withi
result in permanent a

https://paypal.com.verify-auth.secure-user-check.com/login

Thank you,
PayPal Support Team

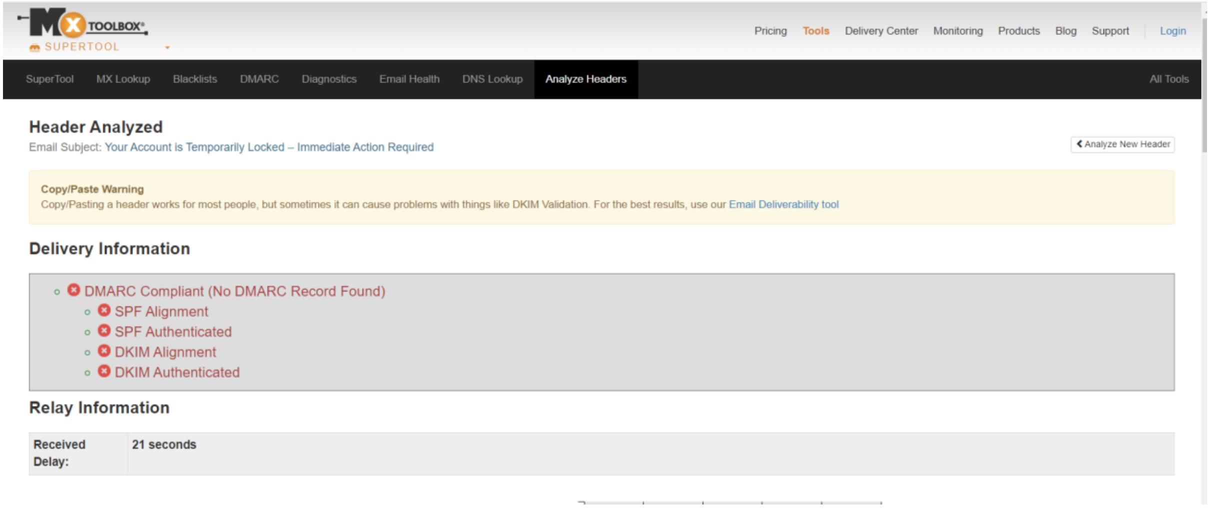
- User received email impersonating PayPal with authentication failures. Contains credential harvesting URL
- Type: Malicious/ confirmed phishing mail

- Sender domain is Typosquatting/ brand impersonation
- I first ran the header code in MXTOOL Box and Message Header Analyzer for detailed analysis.
- I got a reputation of failed SPF, DMARC and DKIM.
- I later checked the reputation of IP address - 185.244.25.91 in apivoid and whois.
- Action taken: Blocked IP address at email gateway and web proxy, initiated end-user notification and end point scan

Extracted IOCs:

- Sender domains: paypalsecure-login.com, secure-paypalhelpdesk.com
- URLs (from email body): https://paypal.com.verify-auth.secure-user-check.com/login
- Message-ID domain: mail.paypalsecure-login.com
- IP addresses: 185.244.25.91, 192.0.2.55 (example)
- User-Agent / Mailer: PHPMailer 6.5.1

Below are the attached screenshots:



Header Analyzed

Email Subject: Your Account is Temporarily Locked – Immediate Action Required

Copy/Paste Warning

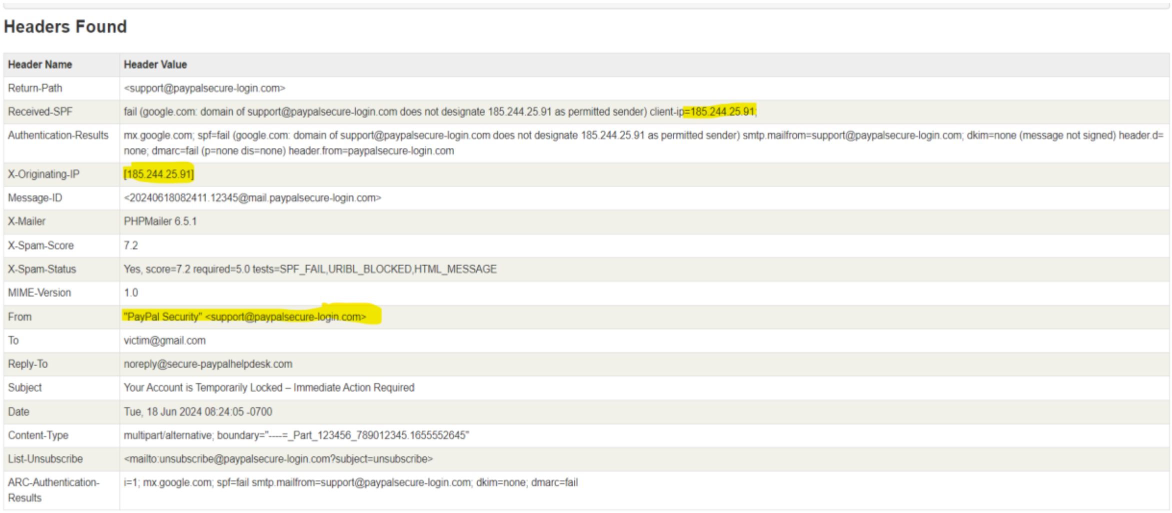
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our Email Deliverability tool

Delivery Information

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

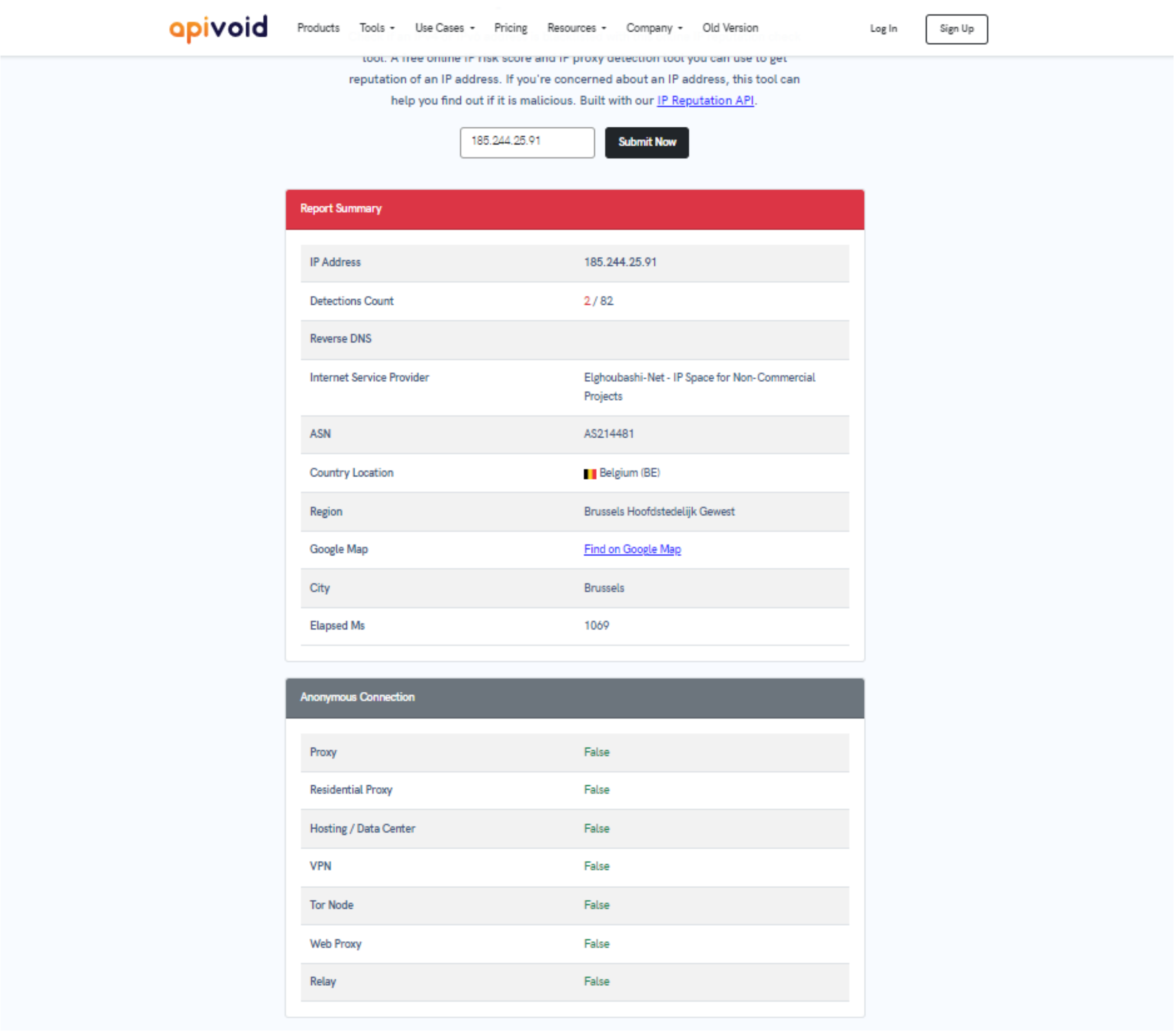
Relay Information

Received Delay:	21 seconds



Headers Found

Header Name	Header Value
Return-Path	<support@paypalsecure-login.com>
Received-SPF	fail (google.com: domain of support@paypalsecure-login.com does not designate 185.244.25.91 as permitted sender) client-ip=185.244.25.91;
Authentication-Results	mx.google.com; spf=fail (google.com: domain of support@paypalsecure-login.com does not designate 185.244.25.91 as permitted sender) smtp.mailfrom=support@paypalsecure-login.com; dkim=none (message not signed) header.d=none; dmarc=fail (p=none dis=none) header.from=paypalsecure-login.com
X-Originating-IP	[185.244.25.91]
Message-ID	<20240618082411.12345@mail.paypalsecure-login.com>
X-Mailer	PHPMailer 6.5.1
X-Spam-Score	7.2
X-Spam-Status	Yes, score=7.2 required=5.0 tests=SPF_FAIL,URIBL_BLOCKED,HTML_MESSAGE
MIME-Version	1.0
From	"PayPal Security" <support@paypalsecure-login.com>
To	victim@gmail.com
Reply-To	noreply@secure-paypalhelpdesk.com
Subject	Your Account is Temporarily Locked – Immediate Action Required
Date	Tue, 18 Jun 2024 08:24:05 -0700
Content-Type	multipart/alternative; boundary="----=_Part_123456_789012345.1655552645"
List-Unsubscribe	<mailto:unsubscribe@paypalsecure-login.com?subject=unsubscribe>
ARC-Authentication-Results	i=1; mx.google.com; spf=fail smtp.mailfrom=support@paypalsecure-login.com; dkim=none; dmarc=fail



tool. A free online IP risk score and IP proxy detection tool you can use to get reputation of an IP address. If you're concerned about an IP address, this tool can help you find out if it is malicious. Built with our IP Reputation API.

185.244.25.91

Report Summary

IP Address	185.244.25.91
Detections Count	2 / 82
Reverse DNS	
Internet Service Provider	Elghoubashi-Net - IP Space for Non-Commercial Projects
ASN	AS214481
Country Location	Belgium (BE)
Region	Brussels Hoofdstedelijk Gewest
Google Map	Find on Google Map
City	Brussels
Elapsed Ms	1069

Anonymous Connection

Proxy	False
Residential Proxy	False
Hosting / Data Center	False
VPN	False
Tor Node	False
Web Proxy	False
Relay	False