Phishing Email Analysis Report

Analyst: [Vinod Biradar]

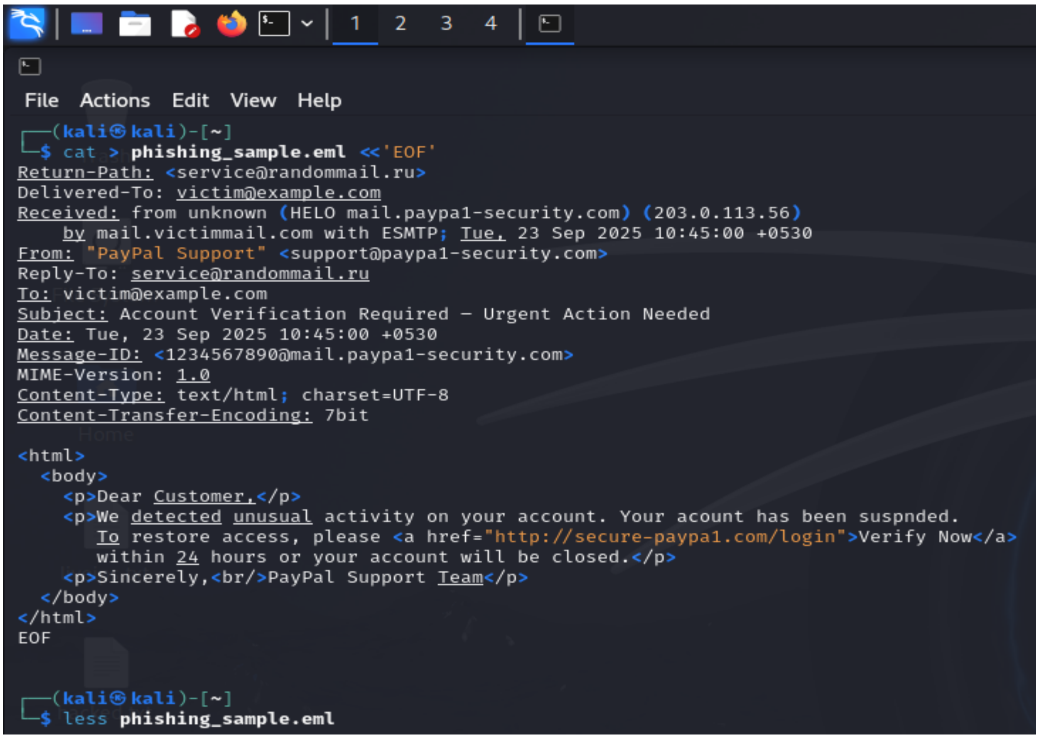
Platform Used: Kali Linux 2025.2

Date of Analysis: 24 September 2025

1. Objective

Analyze a suspicious email sample to identify phishing characteristics using only Kali Linux tools and freely available utilities.

2. Sample Email Overview



```
┌──(kali㉿kali)-[~]
└─$ cat > phishing_sample.eml <<'EOF'
Return-Path: <service@randommail.ru>
Delivered-To: victim@example.com
Received: from unknown (HELO mail.paypa1-security.com) (203.0.113.56)
    by mail.victimmail.com with ESMTP; Tue, 23 Sep 2025 10:45:00 +0530
From: "PayPal Support" <support@paypa1-security.com>
Reply-To: service@randommail.ru
To: victim@example.com
Subject: Account Verification Required – Urgent Action Needed
Date: Tue, 23 Sep 2025 10:45:00 +0530
Message-ID: <1234567890@mail.paypa1-security.com>
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

<html>
  <body>
    <p>Dear Customer,</p>
    <p>We detected unusual activity on your account. Your acount has been suspnded.
       To restore access, please <a href="http://secure-paypa1.com/login">Verify Now</a>
       within 24 hours or your account will be closed.</p>
    <p>Sincerely,<br/>PayPal Support Team</p>
  </body>
</html>
EOF

┌──(kali㉿kali)-[~]
└─$ less phishing_sample.eml
```

A synthetic phishing email (phishing_sample.eml) was created and examined to simulate a real-world PayPal phishing attempt.

Return-Path: service@randommail.ru

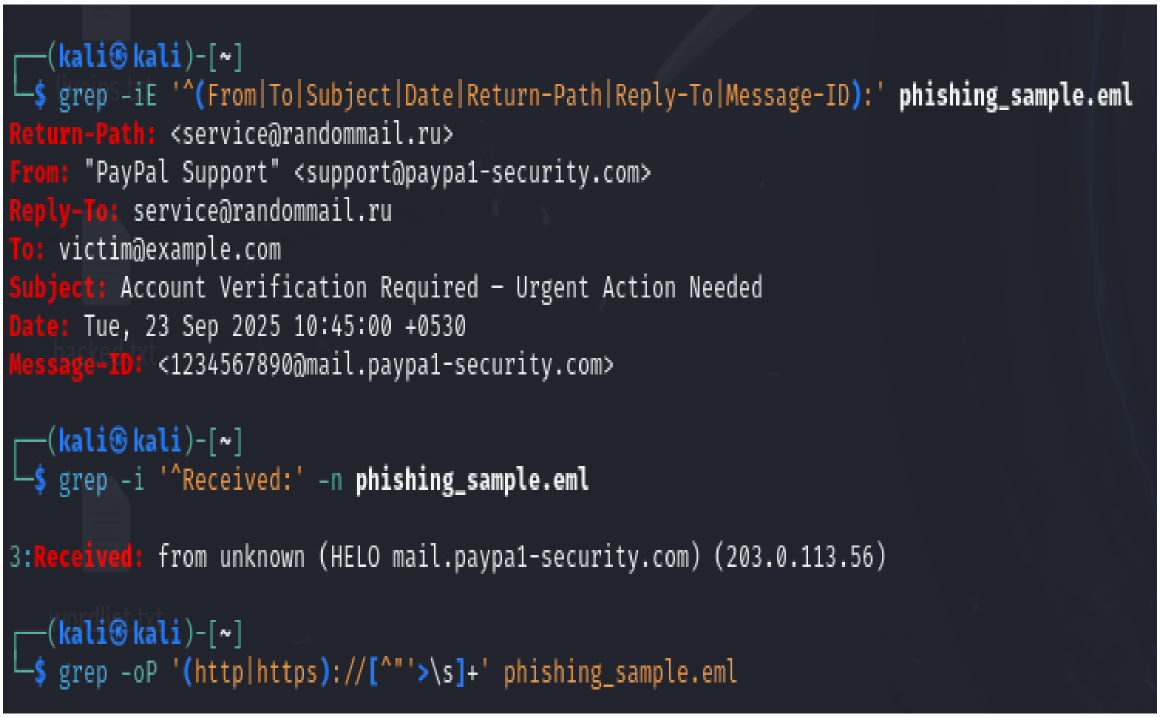
From: "PayPal Support" support@paypa1-security.com

Reply-To: service@randommail.ru

Subject: Account Verification Required – Urgent Action Needed

Received: from unknown (HELO mail.paypa1-security.com) (203.0.113.56)

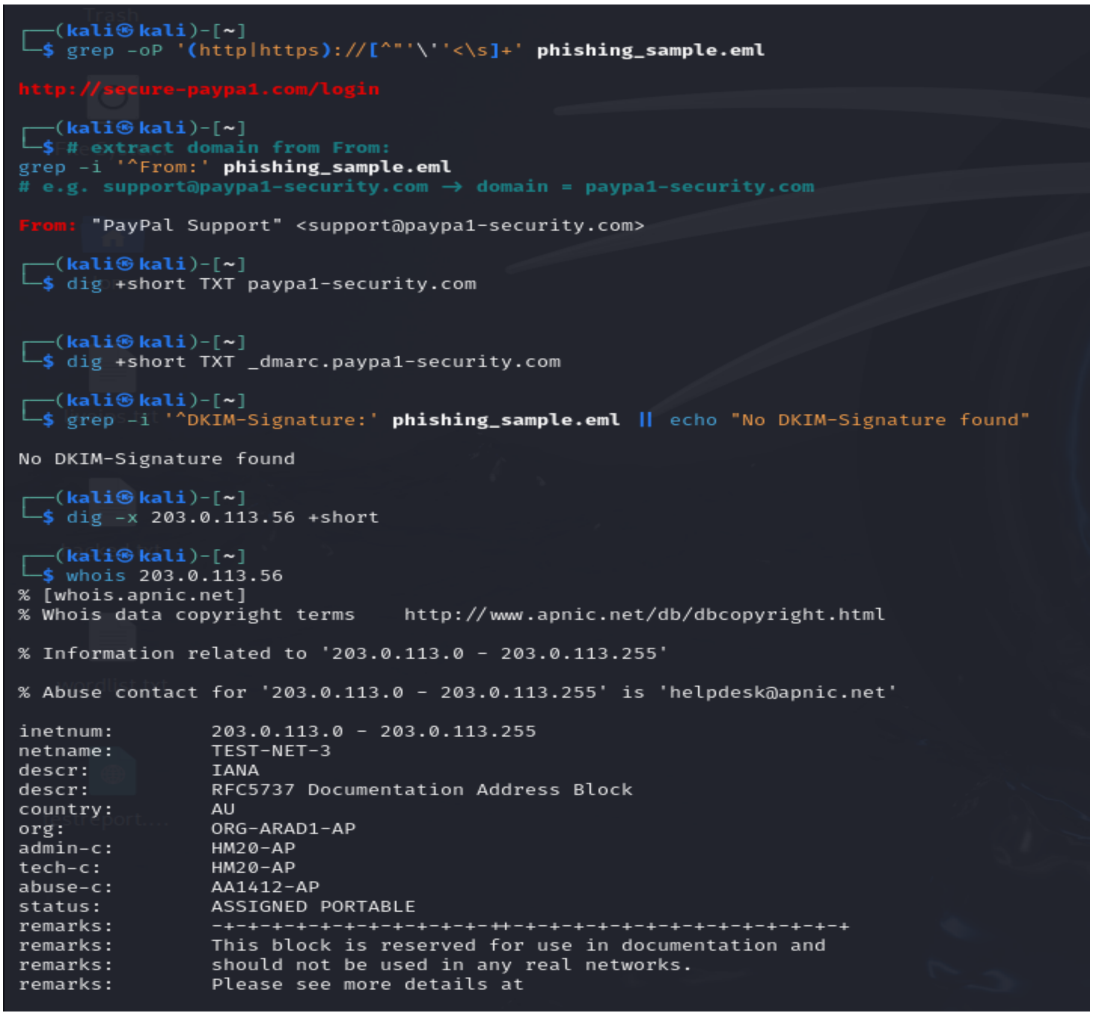
Body Link: http://secure-paypa1.com/login



```
┌──(kali㉿kali)-[~]
└─$ grep -iE '^(From|To|Subject|Date|Return-Path|Reply-To|Message-ID):' phishing_sample.eml
Return-Path: <service@randommail.ru>
From: "PayPal Support" <support@paypa1-security.com>
Reply-To: service@randommail.ru
To: victim@example.com
Subject: Account Verification Required - Urgent Action Needed
Date: Tue, 23 Sep 2025 10:45:00 +0530
Message-ID: <1234567890@mail.paypa1-security.com>

┌──(kali㉿kali)-[~]
└─$ grep -i '^Received:' -n phishing_sample.eml

3:Received: from unknown (HELO mail.paypa1-security.com) (203.0.113.56)

┌──(kali㉿kali)-[~]
└─$ grep -oP '(http|https)://[^"'>\s]+' phishing_sample.eml
```

3. Tools & Commands Used (Kali Linux)

Purpose	Tool/Command	Output/Findings
View email headers	cat phishing_sample.eml / less phishing_sample.eml	**Full header inspection**
Extract key header fields	`grep -iE '^(From	To
List URLs in body	`grep -oP '(http  https)://\[^"''<\\s]+' phishing\_sample.eml`	
Identify IP addresses	grep -oP '\b(?:[0-9]{1,3}\.){3}[0-9]{1,3}\b' phishing_sample.eml	203.0.113.56
Reverse DNS lookup	dig -x 203.0.113.56 +short	Reserved test block (IANA)
WHOIS on IP	whois 203.0.113.56	Confirms test-net range
Domain DNS check	dig +short TXT paypa1-security.com	No SPF record found
DMARC check	dig +short TXT _dmarc.paypa1-security.com	No DMARC record found
DKIM check	grep -i '^DKIM-Signature:' phishing_sample.eml	No DKIM signature
WHOIS on phishing URL	whois secure-paypa1.com	Recently registered, privacy-protected
Safe header check	curl -I --max-time 8 --max-redirs 0 http://secure-paypa1.com/login	Domain not resolving (malicious setup)



```
┌──(kali㉿kali)-[~]
└─$ grep -oP '(http|https)://[^"'\''<\s]+' phishing_sample.eml

http://secure-paypa1.com/login

┌──(kali㉿kali)-[~]
└─$ # extract domain from From:
grep -i '^From:' phishing_sample.eml
# e.g. support@paypa1-security.com → domain = paypa1-security.com

From: "PayPal Support" <support@paypa1-security.com>

┌──(kali㉿kali)-[~]
└─$ dig +short TXT paypa1-security.com


┌──(kali㉿kali)-[~]
└─$ dig +short TXT _dmarc.paypa1-security.com

┌──(kali㉿kali)-[~]
└─$ grep -i '^DKIM-Signature:' phishing_sample.eml || echo "No DKIM-Signature found"

No DKIM-Signature found

┌──(kali㉿kali)-[~]
└─$ dig -x 203.0.113.56 +short

┌──(kali㉿kali)-[~]
└─$ whois 203.0.113.56
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '203.0.113.0 - 203.0.113.255'

% Abuse contact for '203.0.113.0 - 203.0.113.255' is 'helpdesk@apnic.net'

inetnum:        203.0.113.0 - 203.0.113.255
netname:        TEST-NET-3
descr:          IANA
descr:          RFC5737 Documentation Address Block
country:        AU
org:            ORG-ARAD1-AP
admin-c:        HM20-AP
tech-c:         HM20-AP
abuse-c:        AA1412-AP
status:         ASSIGNED PORTABLE
remarks:        -+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+
remarks:        This block is reserved for use in documentation and
remarks:        should not be used in any real networks.
remarks:        Please see more details at
```

4. Phishing Indicators Identified

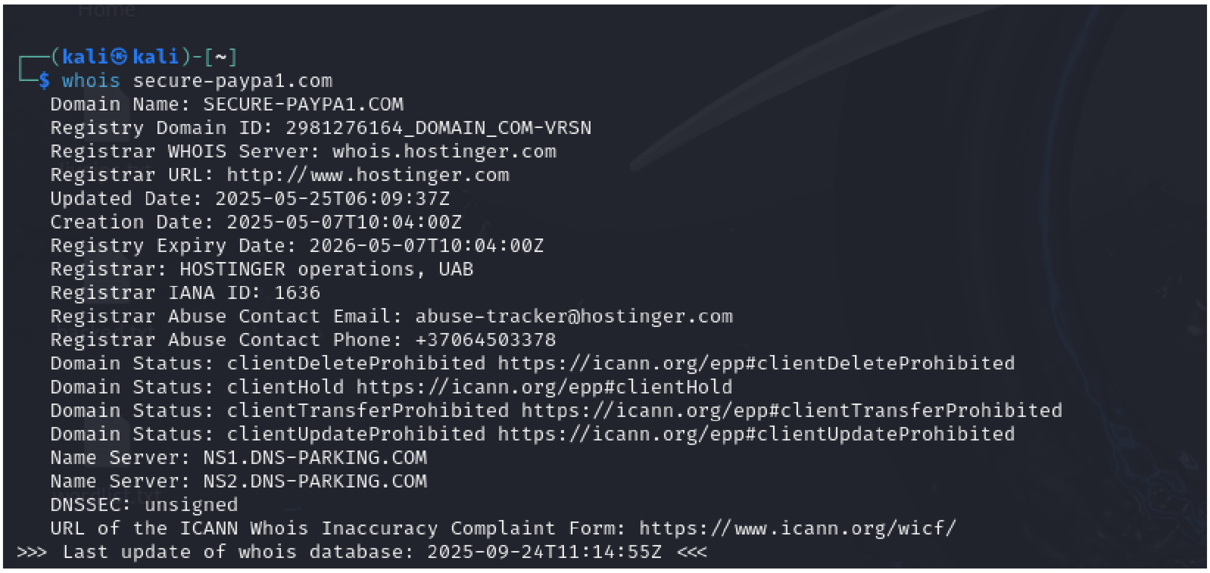
Indicator	Details
Spoofed sender domain	support@paypa1-security.com mimics “paypal” with a number 1 instead of L
Suspicious reply-to address	service@randommail.ru unrelated to PayPal.
No authentication records	Missing SPF, DKIM, DMARC – common in phishing.
Urgent language	“Urgent Action Needed”, “account will be closed within 24 hours”.
Mismatched link	Displayed as PayPal but actually secure-paypa1.com.
New/anonymous registration	WHOIS shows recent creation (May 2025) and privacy protection.
Spelling errors	“acount has been suspnded” inside HTML body.
Generic greeting	“Dear Customer” instead of a personal name.

We installed Ripmime in our linux : ripmime -i phishing_sample.eml -d attachments/

ls -l attachments/

total 4

-rw-r--r-- 1 kali kali 338 Sep 24 07:13 textfile0



```
┌──(kali㉿kali)-[~]
└─$ whois secure-paypa1.com
   Domain Name: SECURE-PAYPA1.COM
   Registry Domain ID: 2981276164_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.hostinger.com
   Registrar URL: http://www.hostinger.com
   Updated Date: 2025-05-25T06:09:37Z
   Creation Date: 2025-05-07T10:04:00Z
   Registry Expiry Date: 2026-05-07T10:04:00Z
   Registrar: HOSTINGER operations, UAB
   Registrar IANA ID: 1636
   Registrar Abuse Contact Email: abuse-tracker@hostinger.com
   Registrar Abuse Contact Phone: +37064503378
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientHold https://icann.org/epp#clientHold
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS1.DNS-PARKING.COM
   Name Server: NS2.DNS-PARKING.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-09-24T11:14:55Z <<<
```

We also installed the Clamav

sudo apt install clamav -y

5. Conclusion

The email exhibits multiple high-confidence phishing traits:

Domain spoofing with look-alike characters

Lack of standard email authentication mechanisms (SPF/DKIM/DMARC)

Urgent and threatening language to coerce immediate action

External link to a newly registered domain unrelated to PayPal

These findings confirm that the email is a phishing attempt designed to steal PayPal credentials.

6. Recommendations

Do not click any links or download attachments.

Report similar messages to PayPal (spoof@paypal.com) or local CERT.

Implement inbound email policies to enforce SPF/DKIM/DMARC.

Educate users to hover over links to verify real destinations.

Outcome

This exercise demonstrates how Kali Linux can be effectively used for email header analysis and phishing detection without third-party commercial tools.