



---

# TASK -2

---

Analyze a Phishing Email Sample



MAY 27, 2025

PRADEEP U S

Pradeep.ustd@gmail.com

# Phishing Email Analysis Report

{Phishing Mail}

From: security-update@paypa1.com

To: you@example.com

Subject: Urgent Action Required – Your Account is Locked

Dear Customer,

We have detected suspicious activity in your PayPal account. For your safety, your account has been temporarily locked.

Please verify your account by clicking the link below:

<https://www.paypal.com/login>

You must complete this verification within 24 hours to avoid permanent suspension.

Best regards,

PayPal Security Team

Attachment: Account\_Update\_Form.zip

-----

## Sender Address Analysis

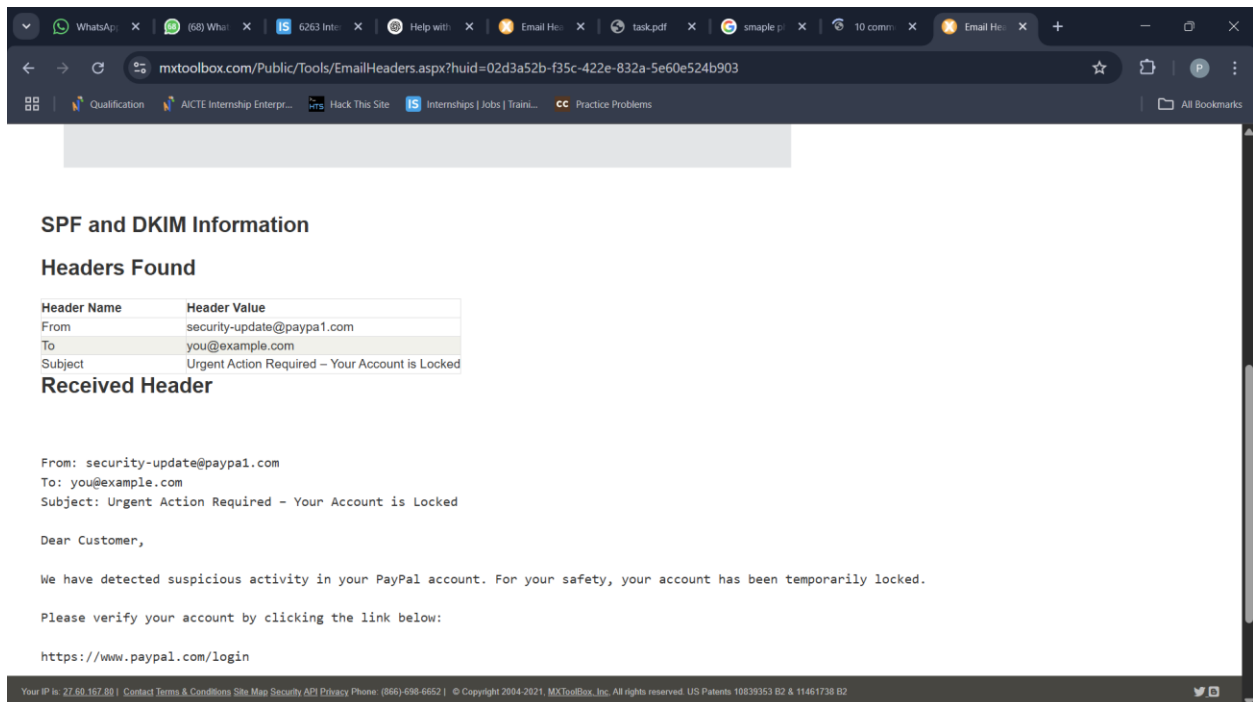
**From Address:** security-update@paypa1.com

### Spoofted Domain

- “paypa1.com” uses a numeral "1" instead of the letter "l" in "paypal.com"

## Email Header Analysis

**Tool Used:** { MxToolbox Email Header Analyzer }



The screenshot shows the MxToolbox Email Header Analyzer interface. The browser address bar displays the URL: `mxttoolbox.com/Public/Tools/EmailHeaders.aspx?huid=02d3a52b-f35c-422e-832a-5e60e524b903`. The page title is "SPF and DKIM Information". Under the "Headers Found" section, a table lists the email headers:

Header Name	Header Value
From	security-update@paypa1.com
To	you@example.com
Subject	Urgent Action Required – Your Account is Locked

Below the table, the "Received Header" section displays the raw email header information:

```
From: security-update@paypa1.com
To: you@example.com
Subject: Urgent Action Required – Your Account is Locked

Dear Customer,

We have detected suspicious activity in your PayPal account. For your safety, your account has been temporarily locked.

Please verify your account by clicking the link below:

https://www.paypal.com/login
```

The footer of the page contains the following text: "Your IP is: 27.68.167.80 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866) 498-6652 | © Copyright 2004-2021, MxToolBox, Inc. All rights reserved. US Patents: 10838353 B2 & 11461738 B2".

### Key Findings:

- **SPF:** Failed
- **DKIM:** Missing
- **Originating IP:** From a country where PayPal has no servers
- **Received headers:** Show inconsistent mail path

## Suspicious Links/Attachments

**Displayed Link:** <https://www.paypal.com/login>

**Actual Link** (hovered): <http://verify-paypal-login.com/auth>

- Fake login page used for credential harvesting

**Attachment:** Account\_Update\_Form.zip

## Urgency & Threatening

Phrases used:

- "Urgent Action Required"
- "Your account is locked"
- "Complete this verification within 24 hours"

These are **manipulative psychological triggers** to cause panic and force quick action

Grammar & Spelling Errors

"Please verify your account by clicking the link below." (*Too generic and unprofessional*)

"You must complete this verification" (*sounds forced, lacks personalization*)

## Summary

Indicator	Description
Spoofed Email Address	paypa1.com instead of paypal.com
SPF/DKIM Failures	Header check shows authentication failure
Mismatched Links	Displayed vs actual URL do not match
Suspicious Attachment	.zip file – potential malware
Urgent Language	Threatens account suspension
Generic Greeting	"Dear Customer" instead of name
Grammar Issues	Slightly awkward tone, lacks brand professionalism

## Conclusion

This email clearly displays multiple phishing characteristics