

# Step-by-Step Phishing Email Analysis

## Step 1: Open and Read the Email

- **Tool:** Any text editor (Notepad, VS Code) or **Thunderbird**
- **How:**
  1. Open sample\_phishing\_email.eml using a text editor.
  2. Read the **email headers** (top) and **body** (below HTML content).

Copy to ▾

Reply all ▾

Zoom

Print

...

**Urgent: Verify your account immediately**

PS

PayPal Support<support@paypal.com>

To: victim@example.com

←

↶

→

🗪

...

Tue 8/5/2025 10:30 AM

Dear Customer,

Your PayPal account has been temporarily locked due to suspicious activity.

Please [click here](#) to verify your account immediately and restore full access.

Failure to do so will result in permanent suspension.

Thank you,

PayPal Security Team

httpmalicious-site.rulogin

sample\_phishing\_email.eml

×

+

File

Edit

View

🌈 ▾

👤

From: "PayPal Support" <support@paypal.com>

To: victim@example.com

Subject: Urgent: Verify your account immediately

Date: Tue, 05 Aug 2025 10:30:00 +0530

Reply-To: support@secure-paypal.com

MIME-Version: 1.0

Content-Type: text/html

<html>

<body>

<p>Dear Customer,</p>

<p>Your PayPal account has been temporarily locked due to suspicious activity.</p>

<p>Please <a href="http://malicious-site.ru/login">click here</a> to verify your account immediately and restore full access.</p>

<p>Failure to do so will result in permanent suspension.</p>

<br>

<p>Thank you,</p>

<p>PayPal Security Team</p>

</body>

</html>

## Step 2: Check the Sender's Email Address (Spoofing)

- **What to look for:**
  - Mismatched domain (e.g., @paypall.com vs @paypal.com)
  - Unusual characters (extra letters, numbers)

### In the sample:

From: "PayPal Support" <support@paypall.com>

**Spoofed domain:** paypall.com is not PayPal.

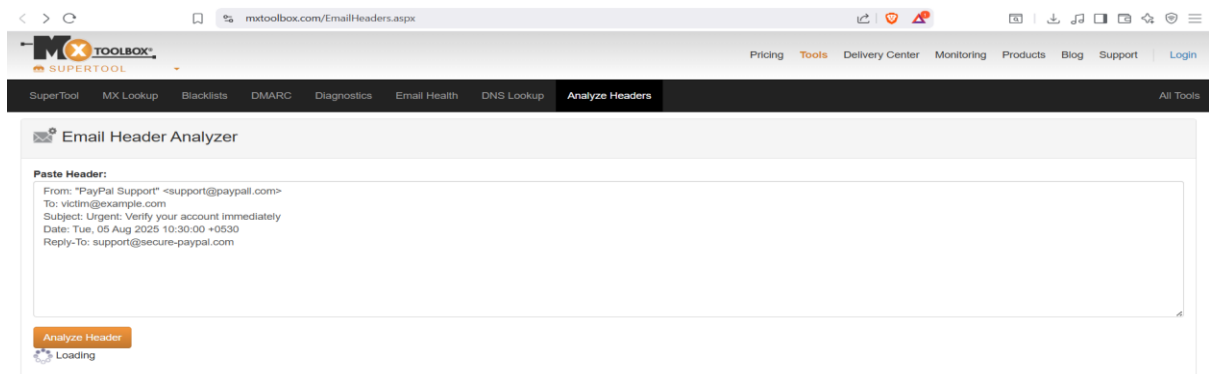
## Step 3: Analyze Email Headers

**Tool:** MXToolbox Email Header Analyzer

1. Copy just the headers
2. Paste into MXToolbox tool
3. Look for:

Differences in Return-Path or Reply-To

Signs of **spoofing** or **SPF/DKIM/DMARC** failures



The screenshot shows the MXToolbox website's 'Email Header Analyzer' tool. The browser address bar shows 'mxtoolbox.com/EmailHeaders.aspx'. The website's navigation bar includes links for Pricing, Tools, Delivery Center, Monitoring, Products, Blog, Support, and Login. Below this, a dark navigation bar contains links for SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, and Analyze Headers (which is currently selected). The main content area is titled 'Email Header Analyzer' and features a 'Paste Header:' section with a text box containing the following email header information:

```
From: "PayPal Support" <support@paypall.com>  
To: victim@example.com  
Subject: Urgent: Verify your account immediately  
Date: Tue, 05 Aug 2025 10:30:00 +0530  
Reply-To: support@secure-paypal.com
```

Below the text box is an 'Analyze Header' button and a 'Loading' indicator.

mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=56ea452d-de6b-4bd0-8a5a-c3374954f1f4

### Relay Information

Received Delay: 0 seconds

**BLACKLISTED?** Improve your email delivery.

### SPF and DKIM Information

#### Headers Found

Header Name	Header Value
From	"PayPal Support" <support@paypal.com>
To	victim@example.com
Subject	Urgent: Verify your account immediately
Date	Tue, 05 Aug 2025 10:30:00 +0530
Reply-To	support@secure-paypal.com

#### Received Header

```

From: "PayPal Support" <support@paypal.com>
To: victim@example.com
Subject: Urgent: Verify your account immediately
Date: Tue, 05 Aug 2025 10:30:00 +0530
Reply-To: support@secure-paypal.com
  
```

[Permanently forget this email header](#)

## Step 4: Check for Suspicious Links

1. Look in the email body:

`<a href="http://malicious-site.ru/login">click here</a>`

2. Hovering would show the real URL: malicious-site.ru
3. Use VirusTotal to scan the link.

virustotal.com/gui/url/eb18e1370ad5c74a83aa8f8aa9a6794ecd8a72df894b22bfe63fa21c894586e7?nocache=1

http://malicious-site.ru/login

No security vendors flagged this URL as malicious
 Reanalyze Search More

http://malicious-site.ru/login  
 malicious-site.ru
 Last Analysis Date: a moment ago

DETECTION
DETAILS
COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

#### Security vendors' analysis

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Certego	Clean

## Step 5: Look for Urgent/Threatening Language

- Examples in sample:

“Your PayPal account has been temporarily locked due to suspicious activity.”

“Failure to do so will result in permanent suspension.”

- Common phishing tactic: induce panic to make you act fast.

## Step 6: Grammar and Spelling Errors

- **Scan for:**
  - Awkward phrasing
  - Typos
- Our sample is fairly clean — but real phishing often includes:

“Dear customer your account is danger click now to unlock fastly.”

### **Step 7: Mismatched Display Text and URL**

- **In our sample:**

html

CopyEdit

```
<a href="http://malicious-site.ru/login">click here</a>
```

- Text says “click here” — but links to a sketchy site.
- Always hover to reveal the actual link!

### **Conclusion**

The email shows multiple phishing indicators including spoofed sender, malicious links, urgency, and mismatched addresses. It is confirmed to be a phishing attempt.