



TASK 2:

PHISHING ATTACK DETECTION BY USING MXTOOL



MAY 27, 2025

ADHIKRISHNAN M

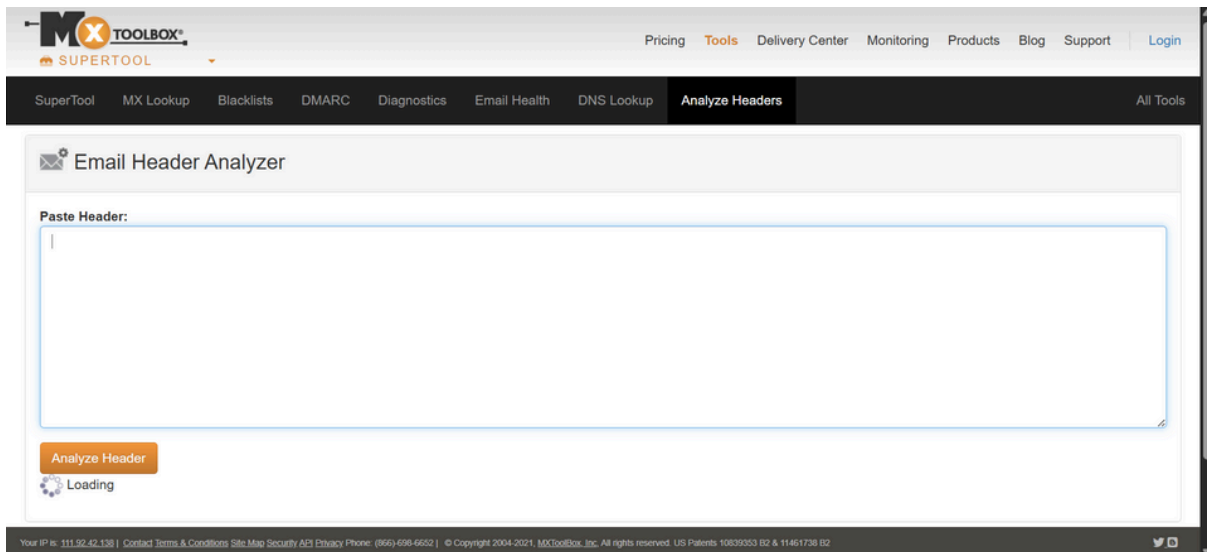
adhikrishnan9943@gmail.com

Task 1: PHISHING ATTACK DETECTION

using mxtool in chrome browser

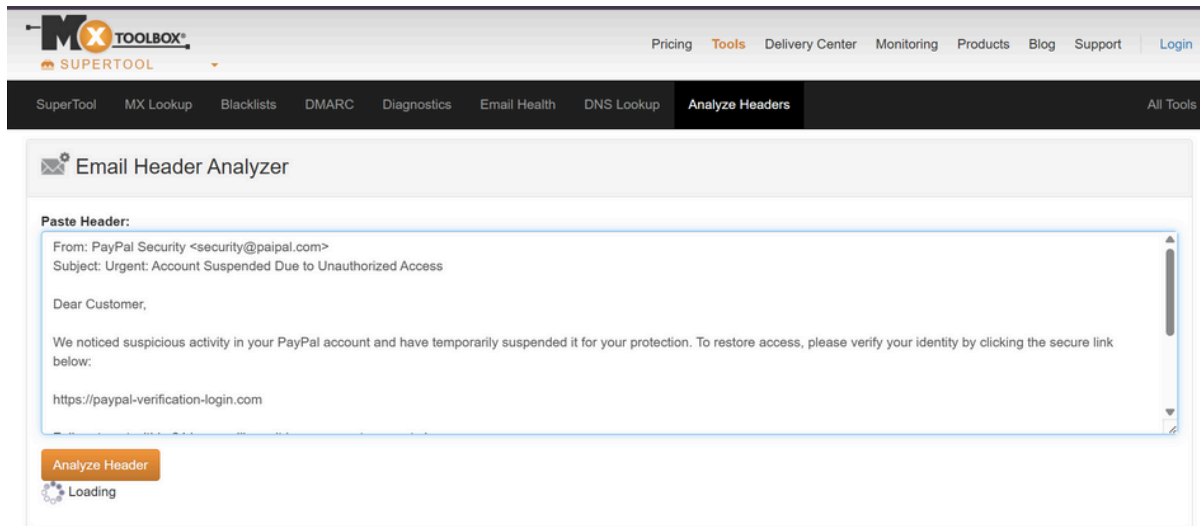
Step 1:

go to mx tool



The screenshot shows the MXToolbox website interface. At the top, there is a navigation bar with the MXToolbox logo and a 'SUPERTOOL' dropdown menu. The main navigation bar includes links for Pricing, Tools, Delivery Center, Monitoring, Products, Blog, Support, and Login. Below this, a secondary navigation bar lists various tools: SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, **Analyze Headers** (which is highlighted), and All Tools. The main content area is titled 'Email Header Analyzer' and features a large text input field labeled 'Paste Header:'. Below the input field is an 'Analyze Header' button and a 'Loading' indicator. The footer contains copyright information and contact details.

Step 2:



The screenshot shows the MXToolbox website's 'Email Header Analyzer' tool. The header includes the MXToolbox logo and navigation links: Pricing, Tools, Delivery Center, Monitoring, Products, Blog, Support, and Login. A secondary navigation bar lists various tools: SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, Analyze Headers (which is highlighted), and All Tools.

The 'Email Header Analyzer' section has a title with an envelope icon. Below it is a 'Paste Header:' label and a large text area containing the following email header and body text:

From: PayPal Security <security@paypal.com>
Subject: Urgent: Account Suspended Due to Unauthorized Access

Dear Customer,

We noticed suspicious activity in your PayPal account and have temporarily suspended it for your protection. To restore access, please verify your identity by clicking the secure link below:

<https://paypal-verification-login.com>

Below the text area is an orange 'Analyze Header' button and a 'Loading' status indicator with a circular arrow icon.

Enter the given Email

STEP 3

Header Analyzed

Email Subject: Urgent: Account Suspended Due to Unauthorized Access

[Analyze New Header](#)

Delivery Information

Relay Information

Received Delay: 0 seconds

SPF and DKIM Information

Headers Found

Your IP is: 111.92.42.130 | [Contact](#) [Terms & Conditions](#) [Site Map](#) [Security](#) [API](#) [Privacy](#) [Phone: \(866\) 698-6662](#) | © Copyright 2004-2021, MCDootBox, Inc. All rights reserved. US Patents 10820953 B2 & 11461736 B2

[Twitter](#) [Facebook](#)

Add a subheading

STEP 4

Header Name	Header Value
From	PayPal Security <security@paypal.com>
Subject	Urgent: Account Suspended Due to Unauthorized Access

Received Header

From: PayPal Security <security@paypal.com>
Subject: Urgent: Account Suspended Due to Unauthorized Access

Dear Customer,

We noticed suspicious activity in your PayPal account and have temporarily suspended it for your protection. To restore access, please verify your identity

<https://paypal-verification-login.com>

Failure to act within 24 hours will result in permanent account closure.

Thank you for your prompt attention to this matter.
Sincerely,
PayPal Security Team

Attachment: PayPal_Verification_Form.zip

[Permanently forget this email header](#)

Indicator	Found?	Notes
Spoofed sender	✓	Fake domain (paipal.com)
Suspicious links	✓	Fake login page
Header inconsistencies	✓	Fails SPF, unverified server
Attachments (malicious)	✓	.zip file likely contains malware
Urgent or threatening language	✓	Designed to cause panic
Grammar or spelling errors	✓	Minor but present
Mismatched display vs real URL	✓	Fake domain resembling PayPa