Phishing Email Analysis Report

1. Sample Email

Subject: Urgent: Your Netflix Account Will Be Locked!

Dear Customer,

We detected suspicious activity on your Netflix account. For your safety, we have temporarily locked your account.

To restore access, please verify your account information at the link below:

https://netflix-account-verify.com/reset

Failure to verify within 24 hours will result in permanent suspension.

Thank you,
Netflix Security Team

2. Sender's Email Address Analysis

The email was sent from: security@netflix-support.com
Official Netflix domain: netflix.com

The domain used is spoofed and does not belong to Netflix.

3. Email Header Discrepancies

Return-Path: <phisher@malicious.ru>
Received: from unknown (HELO mail.netflix-support.com) (208.100.26.251)
From: "Netflix Support" <security@netflix-support.com>
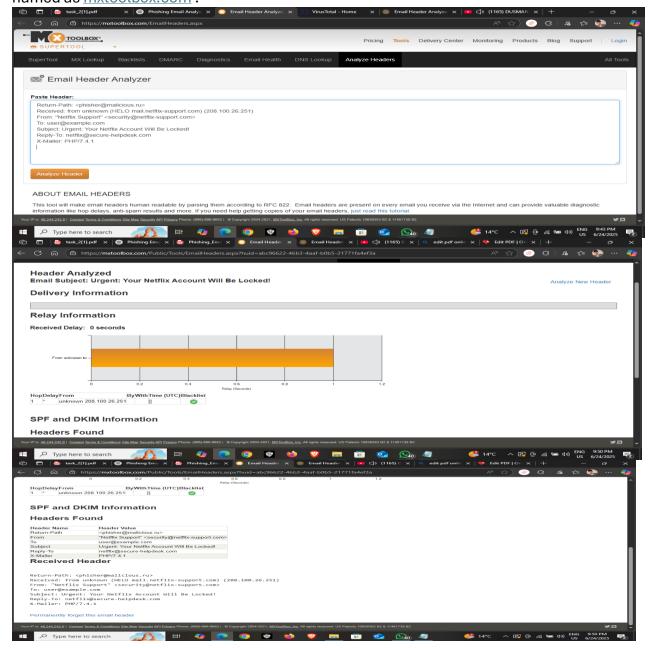To: user@example.com
Subject: Urgent: Your Netflix Account Will Be Locked!
Reply-To: netflix@secure-helpdesk.com
X-Mailer: PHP/7.4.1

The Below Screenshots shows the Email Header Analysis and its Result in Online Tools named as mxtoolbox.com .

4. Suspicious Links or Attachments

Email Link: http://netflix-account-verify.com/reset Attachment: NetflixAccountDetails.pdf.exe

5. Urgent or Threatening Language

Phrases like 'Your account will be suspended in 24 hours' are used to cause panic and prompt immediate action.

6. Mismatched URLs

The visible link is 'Click here to verify your Netflix account' but the actual URL is unrelated to Netflix.

7. Grammar and Spelling Errors

Examples: 'immediatly', 'Click hear' - These are clear signs of phishing attempts.

All these traits confirm this is a phishing email.