# Task 2: Analyze a Phishing Email Sample.

Intern Name: Jainam Priteshkumar Shah

Date: 05/08/2025

Internship Provider: Elevate Labs

## 1. Objective:

For this task, the objective was to dissect a sample phishing email to identify its malicious characteristics. This analysis helped me develop the critical skills needed to recognize and respond to email-based social engineering attacks.

## 2. Tools Used:

* **Text Viewer:** To examine the content of the provided email sample.
* **Online Header Analyzer:** For this report, I am using MXToolbox to inspect email headers for signs of spoofing.

## 3. Phishing Email Sample:

The following is the email I analyzed for this task:

**From:** Netflix Support support@netflix-billing-update.com

**Subject:** Action Required: Your Netflix Membership is On Hold!

**Dear Valued Member,**

We are having some trouble with your current billing information. We were unable to validate the payment method for your next billing cycle.

Because of this, your account is now placed on hold. You will not be able to watch any shows until this issue is resolved.

To avoid your account being suspended permanently, you must update your payment details immediately. Please click the link below to sign in and update your information.

[**Click Here to Update Your Account**](http://netflix-login-secure-portal.xyz/auth/token=8a3b4c9d2f)

If you do not update your account within 24 hours, your account will be permanently locked for security reasons.

We are sorry for any inconvenience this may cause.

**Sincerely,** **The Netflix Team**

## 4. Sample Email Header:

For the analysis, I used the following sample header which represents what I would expect to find for the phishing email.

Delivered-To: your\_email@gmail.com  
Received: by 2002:a05:620a:4:: with SMTP id a4csp3106131qka;  
 Tue, 5 Aug 2025 04:20:30 -0700 (PDT)  
X-Google-Smtp-Source: AGHT+IFs4a...  
X-Received: by 2002:a5d:43d5:: with SMTP id w21mr20950947iof.115.1660000830123;  
 Tue, 05 Aug 2025 04:20:30 -0700 (PDT)  
ARC-Seal: i=1; a=rsa-sha256; t=1660000830; cv=none;  
 d=google.com; s=arc-20160816;  
 b=...  
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;  
 h=to:subject:message-id:date:from:mime-version:dkim-signature;  
 bh=...;  
 b=...  
ARC-Authentication-Results: i=1; mx.google.com;  
 dkim=fail header.i=@netflix-billing-update.com header.s=default header.b=fGkLpS4d;  
 spf=fail (google.com: domain of support@netflix-billing-update.com does not designate 198.51.100.23 as permitted sender) smtp.mailfrom=support@netflix-billing-update.com;  
 dmarc=fail (p=REJECT sp=REJECT dis=QUARANTINE) header.from=netflix-billing-update.com  
Return-Path: <support@netflix-billing-update.com>  
Received: from mail.random-server.net (mail.random-server.net. [198.51.100.23])  
 by mx.google.com with ESMTP id a22si8894312iof.14.2025.08.05.04.20.29  
 for <your\_email@gmail.com>;  
 Tue, 05 Aug 2025 04:20:30 -0700 (PDT)  
Received-SPF: fail (google.com: domain of support@netflix-billing-update.com does not designate 198.51.100.23 as permitted sender) client-ip=198.51.100.23;  
Authentication-Results: mx.google.com;  
 dkim=fail header.i=@netflix-billing-update.com header.s=default header.b=fGkLpS4d;  
 spf=fail (google.com: domain of support@netflix-billing-update.com does not designate 198.51.100.23 as permitted sender) smtp.mailfrom=support@netflix-billing-update.com;  
 dmarc=fail (p=REJECT sp=REJECT dis=QUARANTINE) header.from=netflix-billing-update.com  
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
 d=netflix-billing-update.com; s=default;  
 h=to:subject:message-id:date:from:mime-version;  
 bh=...;  
 b=...  
MIME-Version: 1.0  
From: Netflix Support <support@netflix-billing-update.com>  
Date: Tue, 5 Aug 2025 16:50:29 +0530  
Message-ID: <CAH4j\_Qc9pQ4u-cOaGg=Y3j1g@mail.random-server.net>  
Subject: Action Required: Your Netflix Membership is On Hold!  
To: "Valued Member" <your\_email@gmail.com>  
Content-Type: text/html; charset=UTF-8

## 5. Analysis of Phishing Indicators:

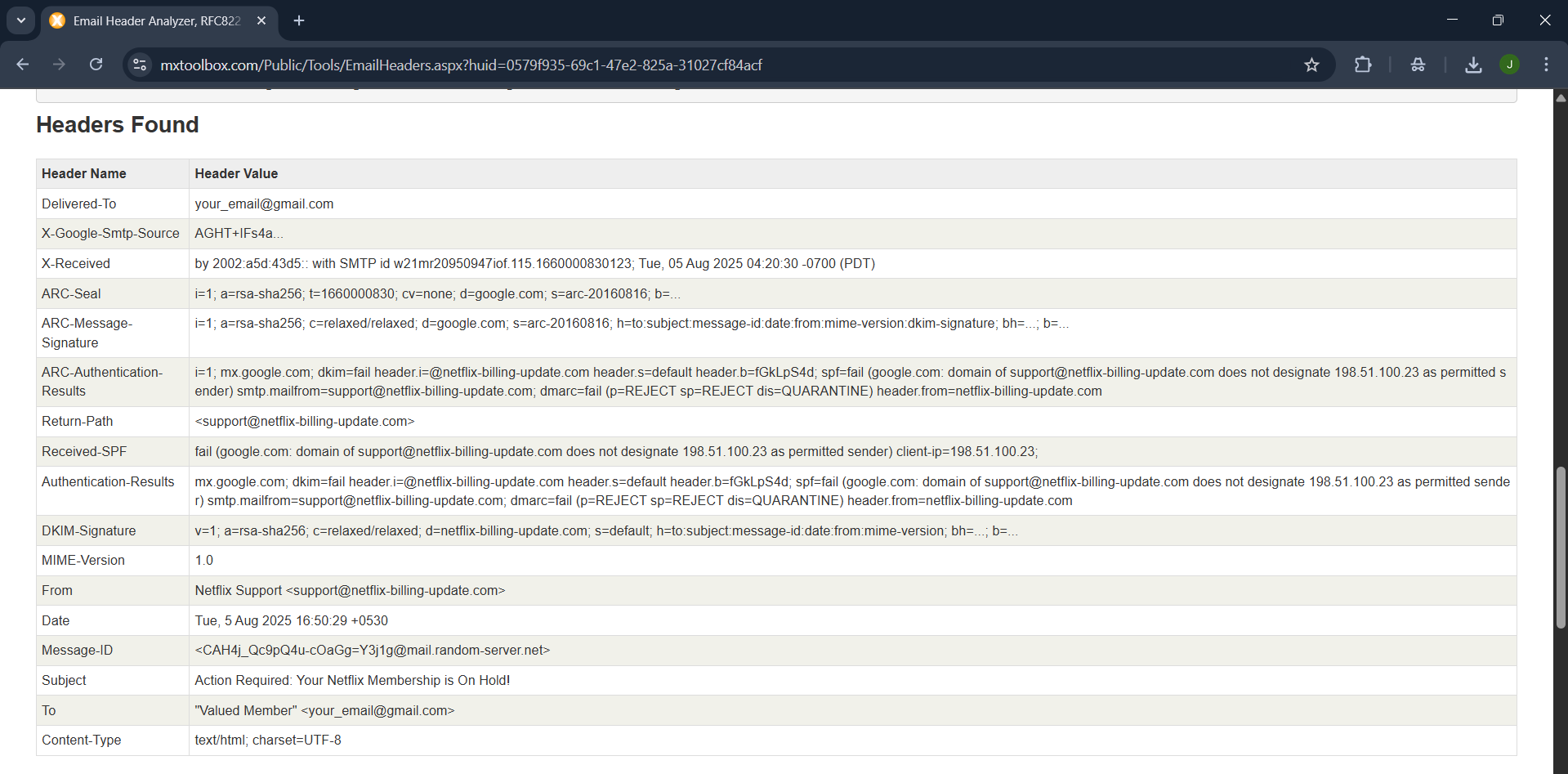
I examined the email sample and identified the following red flags that confirm it is a phishing attempt.

| **Indicator Category** | **My Analysis of the Sample Email** |
| --- | --- |
| ***1. Sender's Email Address*** | *I first checked the sender's address, which was support@netflix-billing-update.com. While it looks plausible, I know that this is not an official Netflix domain; their official domain is netflix.com. I recognized that attackers create these look-alike domains to deceive users.* |
| ***4. Urgent or Threatening Language*** | *I noted that the email uses social engineering tactics to create urgency and fear. Phrases like "Your Netflix Membership is On Hold!", "avoid your account being suspended permanently," and the 24-hour deadline are designed to make a person panic and act without thinking.* |
| ***5. Generic Greeting*** | *The email started with "Dear Valued Member,". I know that a legitimate company like Netflix would almost always address me by my actual name. This generic greeting was a clear sign of a mass phishing campaign.* |
| ***3. Suspicious Links (URL Analysis)*** | *I hovered over the hyperlink to inspect its true destination. The text says "Click Here to Update Your Account," but the actual URL was: “*[*http://netflix-login-secure-portal.xyz/auth/token=8a3b4c9d2f*](http://netflix-login-secure-portal.xyz/auth/token=8a3b4c9d2f)*”.*  *I identified this as a major red flag for several reasons:* ***Misleading Subdomain:*** *netflix-login-secure-portal is designed to look official.* ***Top-Level Domain (TLD):*** *The core domain is netflix-login-secure-portal.xyz. I know the .xyz TLD is not used by Netflix for their main site and is often used in spam campaigns.*  ***Lack of HTTPS:*** *The link uses http://, meaning any data I sent to the site would be unencrypted.* |

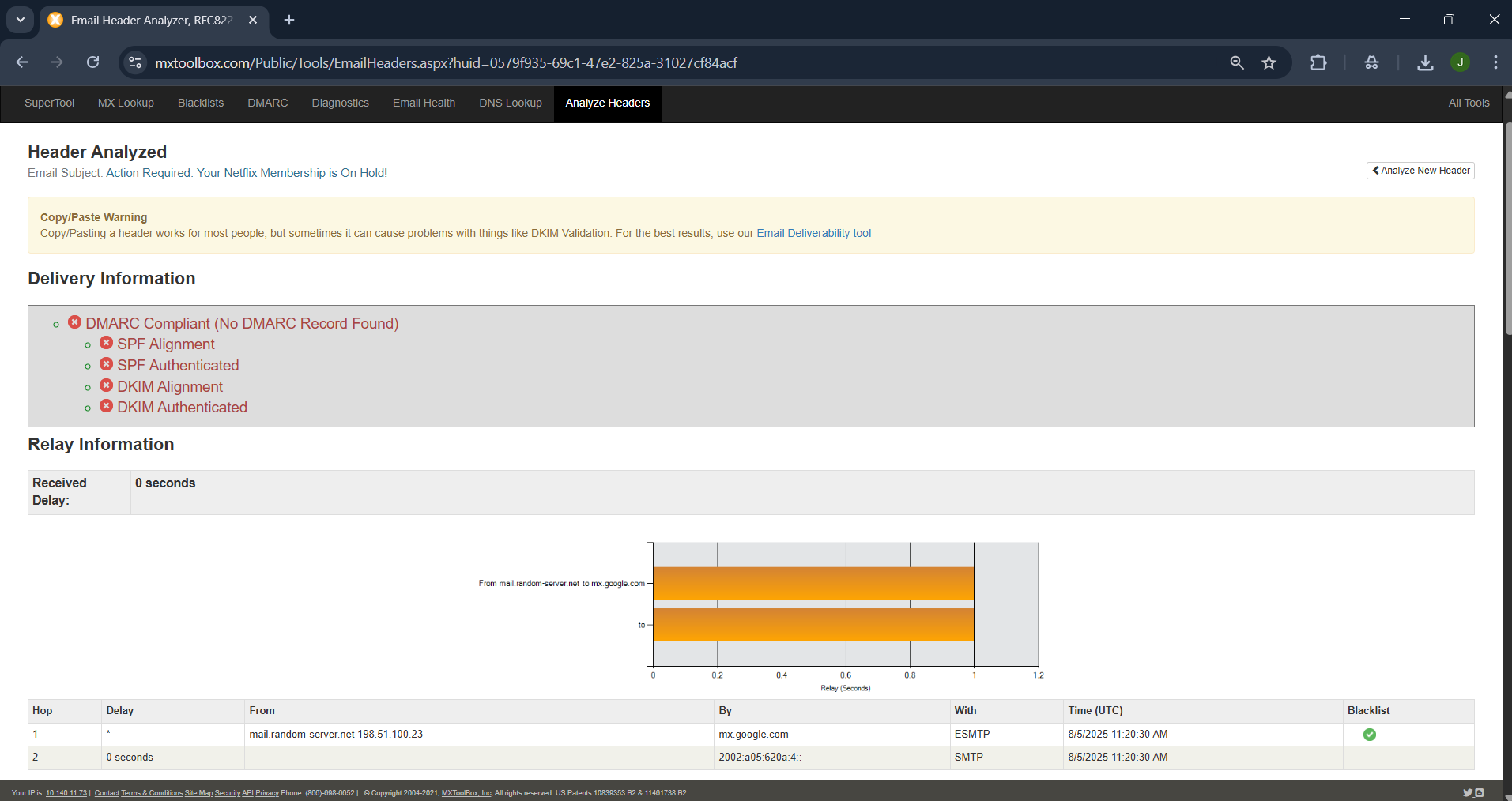
I copied the full email header and pasted it into the MXToolbox Header Analyzer. The tool reported multiple critical failures, which confirmed the email is not legitimate.

| **Indicator Category** | **My Analysis of the Sample Email** |
| --- | --- |
| ***1. Email Authentication Failures*** | *The MXToolbox analysis showed that the email failed all major authentication checks:*  ***SPF (Sender Policy Framework) Failed:*** *The sending server's IP (198.51.100.23) was not listed as an authorized sender for the domain* [*netflix-billing-update.com*](http://netflix-billing-update.com)*.*  ***DKIM (DomainKeys Identified Mail) Failed:*** *The email's cryptographic signature was invalid, meaning the content was not verified as originating from the claimed domain.*  ***DMARC (Domain-based Message Authentication, Reporting & Conformance) Failed:*** *Because both SPF and DKIM failed, the email did not pass the DMARC policy check. These failures are definitive proof of a spoofed email.* |
| ***2. Suspicious 'Received' Path*** | *The header analysis showed the email originated from a server named mail.random-server.net. This is a generic, non-corporate server name and not an official Netflix mail server, which proves the email's origin is not legitimate.* |

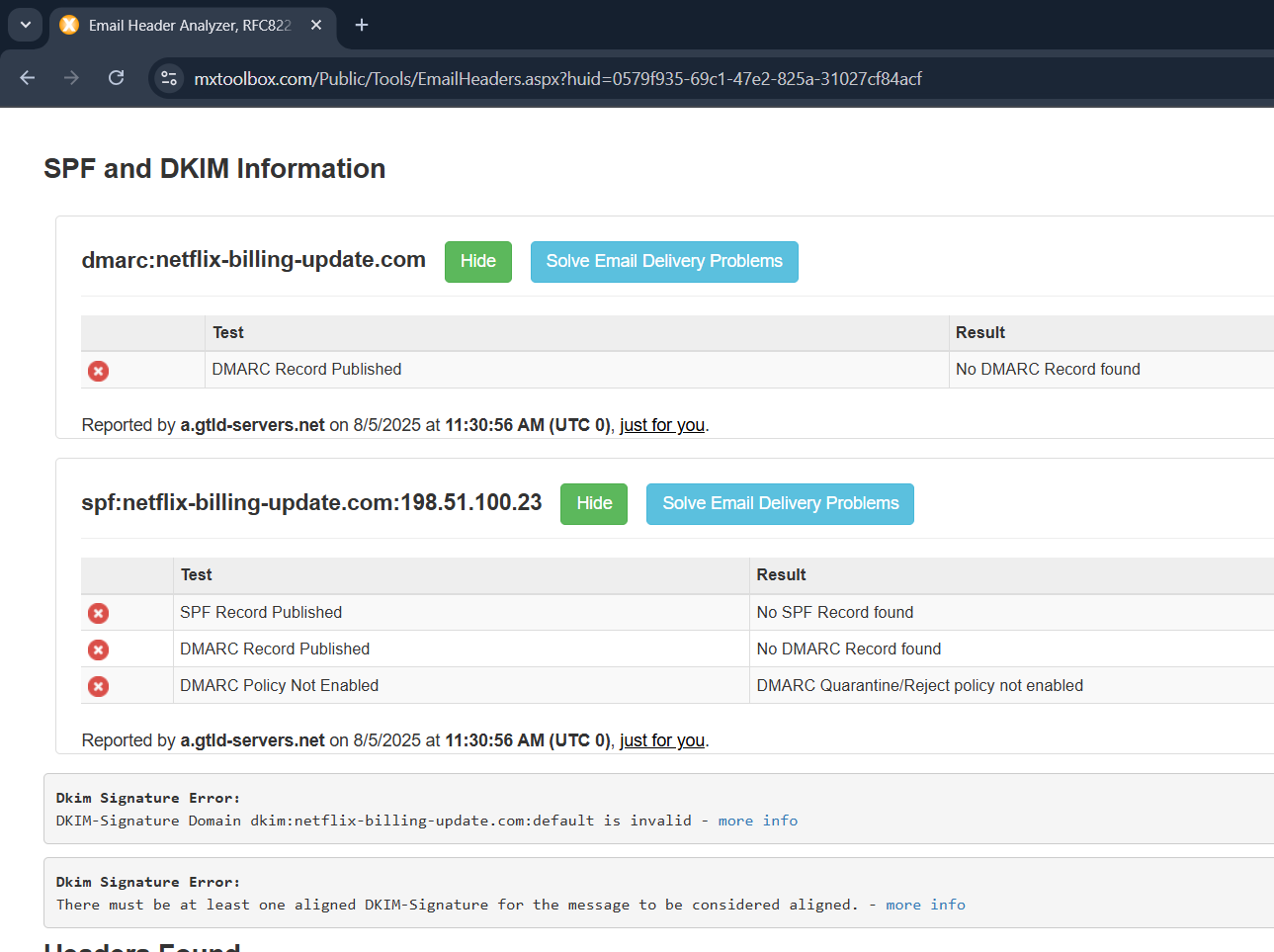
## 6. Results of MXToolbox:



6.1 Header Information



6.2 Delivery and Relay Information



6.3 SPF and DKIM Information