**Phishing Email Simulation & Detection Analysis**

**Internship: Elevate Labs**

**Submitted by Sankabathula Abhishek**

**Introduction**

This report details a phishing email simulation conducted to test detection mechanisms using a crafted Netflix billing scam scenario. The analysis covers both manual email header review and automated verdicts from spam detection tools.

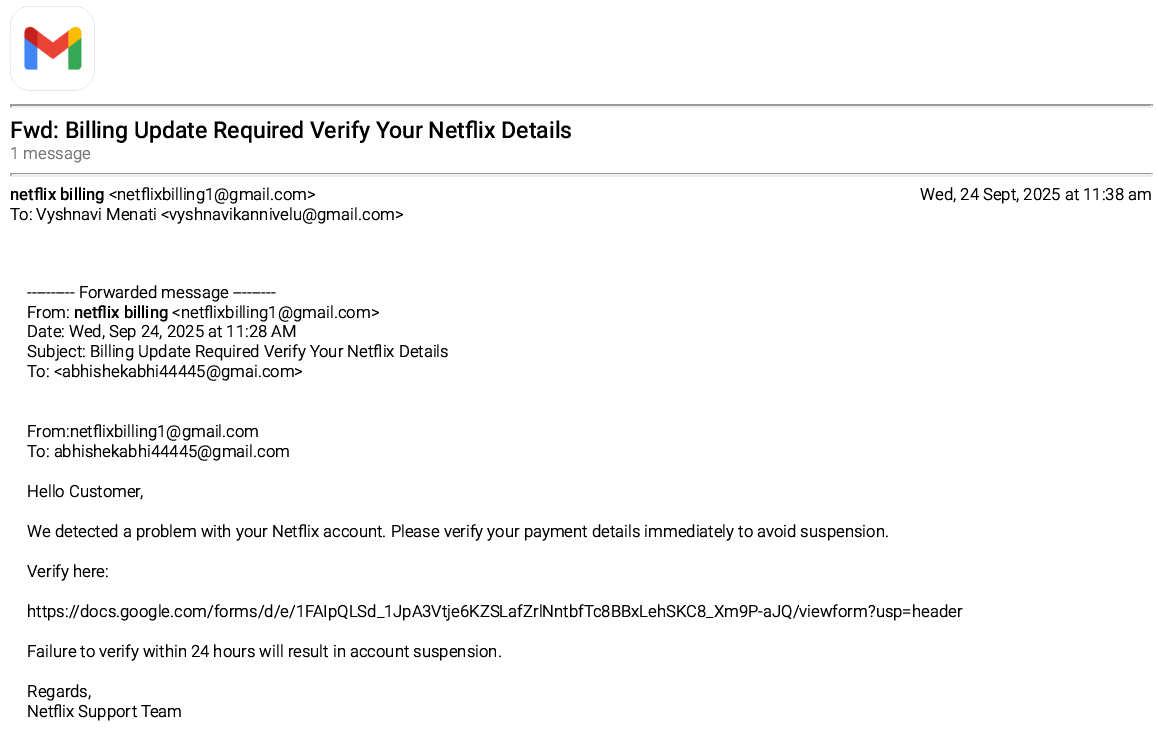
**Methodology**

A phishing email was created to impersonate Netflix, with sender address netflixbilling1@gmail.com and subject "Billing Update Required Verify Your Netflix Details".

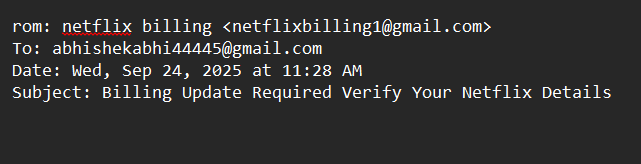
The message was sent to a real recipient (abhishekabhi44445@gmail.com), containing a Google Forms link prompting for payment verification under the threat of account suspension.

**Evidence and Analysis**

1**. Email Content Overview**

Simulation PDF: The sample email warns of an account issue and provides a Google Forms link for urgent action.

**Header File**: Email headers verify sender, recipient, subject, and timestamp, matching the intended simulation setup.

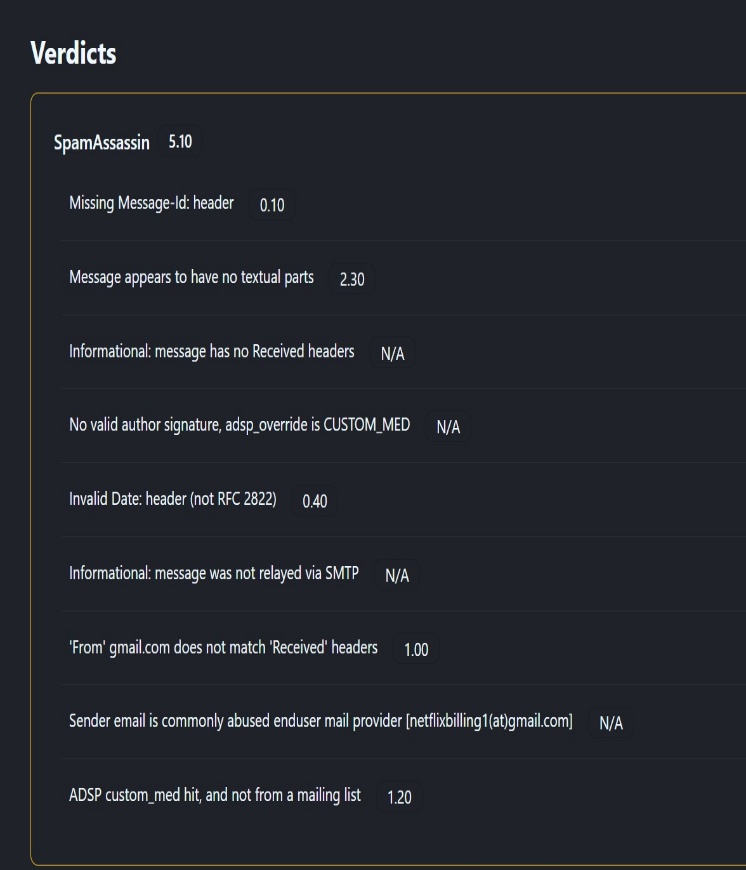
****

**Sender Address:** The email was sent from netflixbilling1@gmail.com. A legitimate company like Netflix would not use a free Gmail account for billing updates. The mismatch between the display name (“netflix billing”) and the actual address is a clear indicator of phishing**.**

**Subject Line:** *“Billing Update Required Verify Your Netflix Details”* uses urgency and a call to action to pressure the recipient. Phrases like “update required” and “verify” are classic social engineering techniques to make the user act quickly without verifying the email’s authenticity**.**

**2. Automated Spam Verdict**

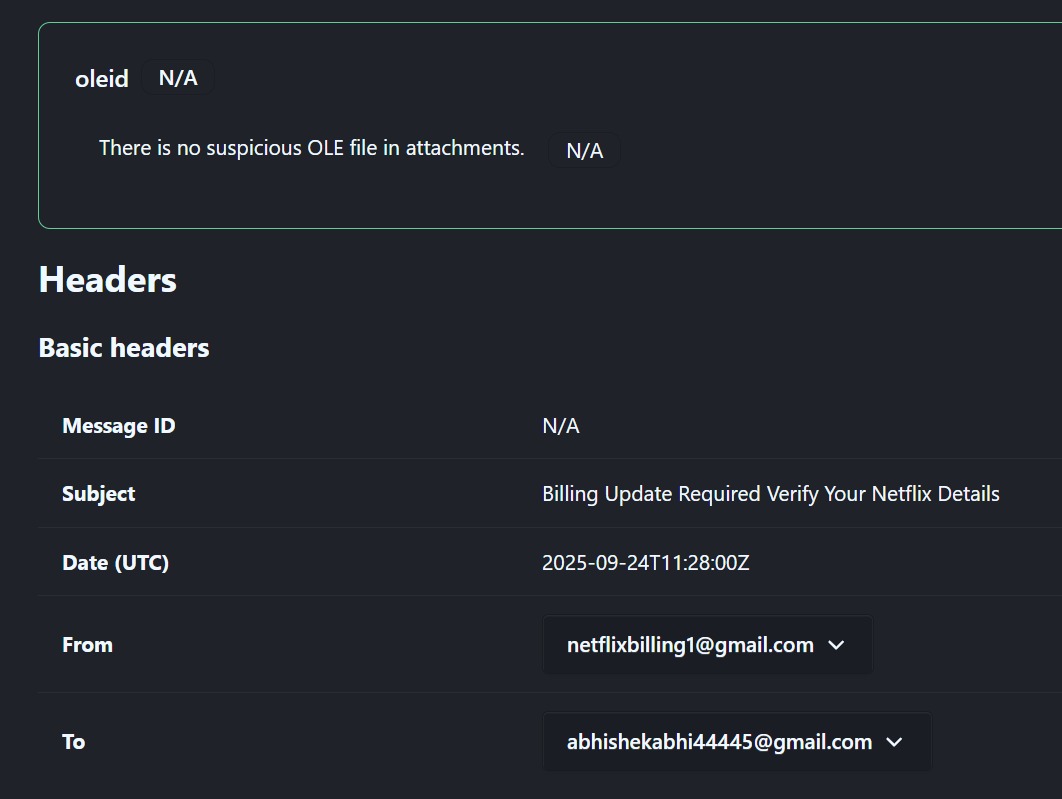
According to SpamAssassin and other tools (see included screenshots), the message is suspicious**:**

****

**SpamAssassin Score: 5.10 (high risk)**

Flags include: missing Message-ID, no textual parts, no 'Received' headers, invalid date, sender address anomalies, and use of a common webmail provider for phishing.

**3. Header Analysis**

****

From: netflixbilling1@gmail.com

To: [abhishekabhi44445@gmail.com](mailto:abhishekabhi44445@gmail.com)

Subject: Billing Update Required Verify Your Netflix Details

Multiple anomalies: missing or nonstandard headers, unusual sender address (not an official Netflix domain).

**The phishing traits found in the email are:**

Suspicious sender address - The sender uses a Gmail address (netflixbilling1@gmail.com) instead of an official Netflix domain, which is a common phishing sign.

Missing or incomplete email headers - Critical headers like Message-ID and Received headers are missing, showing lack of proper email origin authentication.

Urgent threat tone - The email warns about account suspension if payment details are not verified within 24 hours, creating urgency to prompt immediate action.

Suspicious links - The email contains a Google Forms link for payment verification rather than an official Netflix URL.

Email content anomalies - The message appears to have no textual parts in the header analysis, and it uses a generic greeting ("Hello Customer") rather than personalizing by name.

Header and date anomalies - The date header is invalid or not compliant with standards; the 'From' domain does not align with received headers.

SpamAssassin high spam score - A spam score of 5.10 indicates high suspicion.

The sender email is commonly abused by end-users for phishing and spam.

Lack of valid author signature or authentication seals.

These traits align with general phishing indicators such as suspicious sender, urgency, fake links, missing authenticity headers, and generic content.

**Conclusion**

This phishing simulation shows that combining manual header checks with automated tool analysis significantly enhances detection of sophisticated threats. Ongoing awareness, robust filtering, and simulation-based education are critical to maintaining email security.