Phishing Email Analysis Report Task-2

Analyst : Kashif Raja

Date: 16 November 2025

Sample Email source: SamplePhishemail.txt

1. Sender Analysis

From: Netflix Support <billing@netfllix.com.co>

Return-Path: billing@netfllix.com.co

Observations: The email uses the spoofed footer of a US-based company but is sent from a .co (Colombia/Company) domain, creating a geographic mismatch.

2. Header analysis (done)

SPF and DKIM Information

Headers Found

Header Name	Header Value
From	Netflix Support <billing@netfllix.com.co>
Subject	URGENT: Your account has been SUSPENDED - Update Payment Immediately
Date	Friday, Nov 15, 2025 (4:42 PM PST)

Received Header

3. Links and attachments

- **URL:** https://verify-billing-update.id/netflix-login-secureEmail
- **Attachment:** In this specific sample, the method of attack is Credential Harvesting via a malicious link, not through file delivery via an attachment.

4. **Risk assessment**

Likelihood Assessment (High)

The probability of this specific phishing email successfully tricking a user is **High** due to strong social engineering techniques.

Impact Assessment (Critical)

The consequences of a successful attack (the user clicks the link and enters credentials) are **Critical** for the individual and potentially for the organization if the account is used for business purposes.

5. Conclusion

The analysis confirms this email is a high-risk phishing attempt. The combination of brand impersonation, emotional manipulation, and a verifiable malicious link serves as a successful blueprint for cybercriminals.

6. Mitigation

The primary defense against this Critical Risk is User Awareness Training. Users must be trained to identify:

- Typosquatting (netfllix.com.co).
- The use of Urgency and Threats.
- The Mismatch between the displayed link and the actual Hover URL.

Prepared by : Kashif Raja

Notes: Header analyzer result is saved and attached to the report.