Phishing Email Analysis Report

Email Overview:

Field	Value
From	Netflix Alert <support@netfliix-billing.com>
To	abcd123@gmail.com
Subject	Payment Failure – Account Suspension Alert
Date	Tue, 5 Aug 2025 20:15:00 +0530
Message-ID	<098qwe098qwe@example.com>
Return-Path	<support@netfliix-billing.com>

Email Authentication Results:

SPF	FAIL
DKIM	FAIL
DMARC	FAIL

Phishing Indicators:
- The sender's domain (netfliix-billing.com) mimics Netflix but is clearly fake.
- SPF, DKIM, and DMARC all failed, indicating the message likely didn't come from the legitimate domain.
- The subject line creates urgency, a common phishing tactic.
- IP address (45.77.120.3) is not associated with Netflix.
- Return-Path and From headers are the same, a sign of potential spoofing.

Header Analysis Tool Used:
We used the **MXToolbox Header Analyzer** (https://mxtoolbox.com/EmailHeaders.aspx) to inspect and evaluate the full email headers. This tool helps break down technical details like routing IPs, authentication results (SPF/DKIM/DMARC), and return paths. It is an essential tool in identifying whether an email was forged or relayed through suspicious servers.