🔍 Phishing Email Analysis Report

📌 Email Subject: "Urgent: Your Account Has Been Suspended!"

📤 Sender Address: support@netflix-support.com

# 🛠️ Tools Used

* • Email Header Analyzer: https://mxtoolbox.com/EmailHeaders.aspx
* • Email Client: Outlook Web
* • URL Inspection: Hover feature & https://www.virustotal.com

# ⚠️ Phishing Indicators Found

## Spoofed Sender Address

* • Appears as: support@netflix-support.com
* • Actual Netflix domain is @netflix.com, so this is fake and misleading.
* • Trick: Adding a hyphen (-support) to seem legitimate.

## Header Discrepancies

* • Return-Path: bounce@abc.ru (suspicious foreign domain)
* • SPF/DKIM checks failed in header analysis.
* • Origin IP located in Russia, unrelated to Netflix.

## Suspicious Links

* • Visible link: https://netflix.com/verify
* • Actual link (on hover): http://netflix-login-security-update.xyz
* • Link leads to phishing site disguised as a login page.

## Urgent Language

* • “Your Netflix account has been suspended. Immediate verification required or your account will be deleted within 24 hours.”
* • Scare tactic to force quick action.

## Spelling & Grammar Errors

* • "verificaiton" instead of “verification”
* • "you’re account will be delete"

## Fake Branding

* • Netflix logo embedded, but image hosted on an external server img001.evilcdn.net.
* • No personalization (e.g., 'Dear User' instead of user's name).

## Attachment

* • Attached file: Netflix\_Update.pdf.exe
* • PDF and .exe combined — classic malware delivery trick.
* • Antivirus flagged it as malicious.

# 🧾 Summary of Phishing Traits

|  |  |
| --- | --- |
| Trait | Found |
| Spoofed sender email | ✅ |
| Failed authentication (SPF/DKIM) | ✅ |
| Mismatched URLs | ✅ |
| Threatening/Urgent language | ✅ |
| Grammar/spelling issues | ✅ |
| Suspicious attachment | ✅ |
| Generic greeting (no name) | ✅ |

# ✅ Conclusion

This email is a phishing attempt designed to trick users into providing login credentials or installing malware. Users must:  
• Never click on unknown links.  
• Always verify sender email domains.  
• Use a secure browser and email scanner.