Phishing Email Analysis Report

# 1. Objective

To examine a suspicious email for potential phishing characteristics using both visual inspection and technical analysis of the email headers. The goal is to determine if the email is a phishing attempt and document the indicators found.

# 2. Tools Used

- Email Client (e.g., Gmail, Outlook, Thunderbird)

- Online Header Analyzer Tools:

- MxToolbox: https://mxtoolbox.com/EmailHeaders.aspx

- Google Header Analyzer: https://toolbox.googleapps.com/apps/messageheader/

- AbuseIPDB: https://www.abuseipdb.com/

- Web browser and hover preview for URL checks

# 3. Step-by-Step Procedure

Follow these steps to analyze a suspicious email:

Step 1: Open the suspicious email in your email client.

Step 2: Access the full email headers:

- In Gmail: Click the three dots > 'Show original'

- In Outlook: File > Properties > Internet headers

Step 3: Copy the entire header text.

Step 4: Paste the headers into an online header analyzer (e.g., MxToolbox or Google Header Tool).

Step 5: Analyze the results:

- Check SPF, DKIM, DMARC authentication results

- Look for mismatched 'From' and 'Return-Path' fields

- Identify sender IP and verify it on AbuseIPDB

Step 6: Review the email body for phishing signs:

- Look for urgent or threatening language

- Hover over links to check the actual URL

- Check for requests for personal or sensitive information

- Look for poor grammar or spelling mistakes

Step 7: Document your findings in this report.

# 4. Observations and Indicators

- Email uses urgent language to scare the recipient.

- URL in email text differs from the actual hyperlink when hovered.

- SPF, DKIM, and DMARC checks fail.

- Sender IP is listed in known abuse databases.

- Spelling and grammar are inconsistent with professional communication.

# 5. Conclusion

The email exhibits several strong phishing indicators including authentication failures, mismatched sender information, suspicious links, and requests for sensitive data. This email should be treated as a phishing attempt. Do not interact with any links or respond. Report and delete the email.

# 6. Recommendations

- Train users to recognize phishing signs.

- Use email filters and advanced spam detection tools.

- Regularly check email header authenticity using analyzers.

- Report phishing attempts to appropriate internal/external teams.