Final Report – Phishing Email Indicators Identified

1. Introduction

This report presents the findings from the analysis of a suspicious email pretending to be from Amazon. The goal of the task was to identify phishing indicators using sender details, email headers, embedded links, tone, formatting, and technical authentication checks. The investigation confirmed multiple signs of phishing and malicious intent.

2. Summary of Email Content

The email claims that the user's Amazon order payment failed and urges them to verify payment within 24 hours to avoid cancellation or account suspension. It contains:

- A malicious link disguised as an Amazon action button

- A fake invoice attachment

- Urgent and threatening messages

- A spoofed Amazon branding

3. Phishing Indicators Identified

A. Sender-Based Indicators

- Spoofed sender email using lookalike domain: amaz0n-support.com

- Mismatch between From and Reply-To addresses

- Domain not owned by Amazon

B. Email Header Indicators

- SPF softfail

- DKIM missing

- DMARC failure

- Suspicious sending IP address (185.203.112.14)

- No reverse DNS mapping

C. Malicious Link Indicators

- Displayed link vs actual malicious link mismatch

- HTTP instead of HTTPS

- Fake .xyz domain

- Credential harvesting login page

D. Attachment Indicators

- Suspicious invoice PDF reference

- Potential malware or phishing form

- Not standard Amazon practice

E. Urgency & Threat-Based Indicators

- Threats of order cancellation and account suspension

- Use of “URGENT” in subject line

- Demands for immediate action

F. Grammar & Formatting Indicators

- Spelling errors like “cancelld”

- Unnatural or unprofessional formatting

- Generic signatures

4. Conclusion

The analyzed email clearly demonstrates all major signs of phishing including spoofed sender identity, failed authentication methods, malicious links, suspicious attachments, urgent tone, and grammar issues. It is conclusively a phishing attempt aimed at stealing Amazon login credentials.

The email should be reported and not interacted with under any circumstances.