Phishing Email Analysis - Cybersecurity Task

Task Overview

This project involves analyzing a suspicious email to identify phishing indicators and document the findings in a structured report.

Objective

Identify phishing characteristics such as:

- Spoofed sender information
- Malicious links or attachments
- Threatening or urgent language
- Mismatched URLs
- Poor grammar or spelling

Tools Used

- Email client (for viewing email structure)
- MXToolbox Email Header Analyzer
- Browser (to inspect URLs safely by hovering)
- Text editor or Markdown for report writing

Steps Followed

1. Collected a sample phishing email from public sources.
2. Inspected sender's email address for spoofing signs.
3. Analyzed email headers using an online analyzer.
4. Checked links and attachments for suspicious behavior.
5. Reviewed email content for urgent language or threats.

6. Hovered over URLs to detect mismatches.

7. Verified for spelling and grammar issues.

8. Compiled findings into a summary report.

Sample Analysis Summary

Sender Email: support@paypa1.com

Spoof Detected: Yes (domain misspelled)

SPF/DKIM/DMARC: SPF: Fail, DKIM: Missing

Suspicious Links: http://malicious-paypal-login.com

Threatening Language: 'Your account will be suspended within 24 hours'

Grammar Errors: Present

Attachment: invoice.zip (Potential Malware)

Verdict: Phishing Email

Deliverable

The deliverable includes:

- This PDF report

Disclaimer

This project is for educational and training purposes only. Do not click on any suspicious links or open malicious attachments. Always handle phishing samples in a safe and secure environment.

Phishing Email Analysis - Cybersecurity Task

Author

Asiya Irshad

Cybersecurity Enthusiast | B.Tech Final Year Student