Cybersecurity Internship Task 2: Phishing Email Analysis Report

Sujay Vegi

Date: May 27, 2025

Elevale Cybersecurity Internship

Contents

1 Objective

The objective of this task was to analyze a sample phishing email to identify characteristics of phishing attempts, such as spoofed sender addresses, suspicious links, and social engineering tactics. This exercise aimed to develop skills in email threat analysis and awareness of phishing tactics.

2 Tools Used

- **Email Client**: Used to view the sample phishing email and access its headers (e.g., Gmail's "Show original" feature).
- **Online Header Analyzer**: MXToolbox (https://mxtoolbox.com/EmailHeaders.aspx) for analyzing email headers.
- **Operating System**: [Your Operating System, e.g., Windows 11, Ubuntu 22.04, or macOS Ventura].

3 Methodology

1. **Obtained Sample Email**: Acquired a sample phishing email from a public dataset (e.g., PhishTank).
2. **Examined Sender's Address**: Checked the "From" field for signs of spoofing, such as misspellings or unrelated domains.
3. **Analyzed Email Headers**: Used MXToolbox to examine headers for discrepancies in `Return-Path`, `Received`, and authentication fields (DKIM/SPF/DMARC).
4. **Identified Suspicious Links**: Hovered over links to reveal true URLs and checked for mismatches.
5. **Noted Urgent Language**: Identified threatening or urgent phrases in the email body.
6. **Checked for Errors**: Looked for spelling or grammar mistakes in the email content.
7. **Summarized Findings**: Compiled a list of phishing indicators for the report.
8. **Saved Evidence**: Saved the email source as `email`$_{s}ample.txtandascreenshotoftheheaderanalysisas$`he`

4 Findings

The analysis of the sample phishing email, claiming to be from "PayPal Support," revealed the following phishing indicators:

Notes:

- The spoofed sender address suggests an attempt to impersonate PayPal.
- The suspicious link uses an unsecure protocol (HTTP) and a fake domain, a common phishing tactic.

Phishing Indicator	Details
Spoofed Sender Address	"From: PayPal Support <support@paypa1-security.com>" mimics "paypal.com" (note "1" instead of "l").
Header Discrepancy	`Return-Path: user@randomdomain.xyz` does not match the sender's domain; DKIM authentication failed.
Suspicious Link	Link labeled "PayPal Login" directs to `http://paypa1-security.com/update` instead of `https://www.paypal.com`.
Urgent Language	Email states, "Your account has been compromised. Click here to verify your account immediately."
Grammar Error	Phrase "account is at risk of been suspended" should be "being suspended."

Table 1: Phishing indicators identified in the sample email

- Urgent language is designed to prompt immediate action, a hallmark of social engineering.

5 Proof of Work

A screenshot of the email header analysis from MXToolbox is included in the GitHub repository as `header`$_s$*creenshot.png.Itshowstheanalysisresults*, *includingthefailedDKIMauthentica*