Elevate Labs – Cyber Security Internship

Task 2: Analyze a Phishing Email Sample

By: Ministry of MSME, Govt. of India

Objective

The objective of this task is to identify phishing characteristics in a suspicious email sample and develop practical email threat analysis skills.

Tools Required

- Email client or saved email file (text format)
- Free online header analyzer (e.g., MXToolbox, Google Admin Toolbox)

Execution Steps

1. Obtain a sample phishing email
    - Choose an example from trusted cybersecurity resources (e.g., PhishTank, APWG datasets).
2. Examine the sender's email address
    - Look for domain spoofing or slight misspellings, e.g., `support@micros0ft.com`.
3. Analyze email headers
    - Use an online header analyzer to check for:
        - SPF/DKIM/DMARC failures
        - Mismatch between `Return-Path` and `From` address
        - Suspicious originating IP addresses
4. Inspect links and attachments
    - Hover over links to spot mismatches between displayed and actual URLs.
    - Check suspicious or executable attachments for potential malware.
5. Identify urgent/threatening language
    - Look for pressure tactics such as “Immediate action required” or “Your account will be suspended.”
6. Check for mismatched URLs

- Example: A link labeled as "PayPal.com" actually pointing to `paypl-secure-login[.]ru`.

7. Spot spelling or grammar errors
    - Many phishing attacks contain awkward phrasing or mistakes.
8. Summarize phishing traits found
    - List each suspicious indicator and what it implies.

Findings / Phishing Indicators

- Sender address spoofed — Example: `support@micros0ft.com` (imposter domain)
- Header anomalies — SPF check failed, Return-Path mismatched with sender domain
- Suspicious URLs — Displayed text: *PayPal Security*, Actual link: `paypl-secure-login[.]ru`
- Attachments — Malicious .exe file detected by antivirus scan
- Urgency tactics — “Your account will be locked within 24 hours”
- Language issues — Poor grammar and awkward sentence structures
- Social engineering — Creating fear and urgency to prompt hasty clicks

---

Security Analysis

This phishing email uses multiple layered attack vectors — spoofed domains, malicious links, and malware-laden attachments — to trick the recipient. The urgency and fear-based tactics increase the likelihood of user error, making these attacks effective if not detected early.

Recommendations

- Enable SPF, DKIM, and DMARC policies on mail servers.
- Train users on phishing detection techniques.
- Use advanced email filtering systems with malware scanning.
- Always hover over links before clicking.
- Avoid downloading suspicious attachments.

Outcome

- Developed analytical skills in detecting phishing emails.
- Learned to interpret email headers and validate sender authenticity.

- Gained awareness of social engineering tactics employed in phishing schemes.

Key Concepts

- Phishing
- Email Spoofing
- Header Analysis
- Social Engineering
- Threat Detection