Cyber Security Internship - Task 2 Report

Task Description

Task 2: Analyze a Phishing Email Sample

Objective: Identify phishing characteristics in a suspicious email sample.

Tools: Email client or saved email file (text), free online header analyzer.

Hints / Mini Guide:

1. Obtain a sample phishing email (many free samples online).
2. Examine sender's email address for spoofing.
3. Check email headers for discrepancies (using online header analyzer).
4. Identify suspicious links or attachments.
5. Look for urgent or threatening language in the email body.
6. Note any mismatched URLs (hover to see real link).
7. Verify presence of spelling or grammar errors.
8. Summarize phishing traits found in the email.

Outcome: Awareness of phishing tactics and email threat analysis skills.

Task Answer - Phishing Email Analysis

Phishing Email Analysis - Sample Report:

1. Sender's Email Spoofing: The sender's email appeared to be from a legitimate source (support@paypal.com) but on inspection, the actual address was something like support@ppyal-secure.com, indicating spoofing.
2. Email Header Discrepancies: Used an online header analyzer to find that the source IP originated from a non-corporate ISP, and SPF failed-strong sign of spoofing.
3. Suspicious Links: The email asked to "verify your account" with a link to a lookalike site. On hovering, the real URL was completely unrelated.
4. Language and Tone: The message used threatening language: "Your account will be locked in 24 hours".

This urgency is typical of phishing.

5. Attachments: The email had a ".html" attachment named "verify-now.html", which is unusual for trusted services.

6. Grammar Errors: Multiple minor grammar and punctuation mistakes were present, a common red flag in phishing emails.

7. Social Engineering: The email attempted to scare the user into acting quickly without thinking.

Conclusion: The email contained classic phishing markers and would be classified as a phishing attempt.

Interview Questions with Sample Answers

Interview Questions and Sample Answers:

1. What is phishing?

Phishing is a type of cyberattack where attackers impersonate legitimate entities to trick users into providing sensitive information like passwords or credit card details.

2. How to identify a phishing email?

Check for mismatched sender addresses, poor grammar, threatening language, suspicious attachments, and links that don't match the legitimate domain.

3. What is email spoofing?

Email spoofing is the forgery of email headers so the message appears to come from someone or somewhere other than the actual source.

4. Why are phishing emails dangerous?

They can lead to financial loss, credential theft, malware infections, and unauthorized access to sensitive systems.

5. How can you verify the sender's authenticity?

Cyber Security Internship - Task 2 Report

Check the email headers, SPF/DKIM results, verify the domain, and contact the sender through alternate official channels.

6. What tools can analyze email headers?

Tools like MXToolbox, Google Admin Toolbox, or MessageHeaderAnalyzer can be used for header inspection.

7. What actions should be taken on suspected phishing emails?

Do not click any links or download attachments. Report it to your IT/security team and delete the email.

8. How do attackers use social engineering in phishing?

They exploit emotions like fear, urgency, or curiosity to trick users into clicking malicious links or disclosing personal information.