PHISHING EMAIL ANALYSIS

Task 2: Analyze a Phishing Email Sample

Objective:

- Identify phishing characteristics in a suspicious email sample.

Tools:

- Email client or saved email file (text format)
- Free online header analyzer (e.g., https://toolbox.googleapps.com/apps/emailheader/)

Deliverables:

- A report listing phishing indicators found in the email sample.

Mini Guide / Steps:

- Obtain a sample phishing email (many free samples available online).
- Examine the sender's email address for spoofing.
- Check email headers for discrepancies (use an online header analyzer).
- Identify suspicious links or attachments.
- Look for urgent or threatening language in the email body.
- Note any mismatched URLs (hover over links to see the real destination).
- Verify presence of spelling or grammar errors.
- Summarize all phishing traits found in the email.
-

Interview Questions:

- What is phishing?
- How do you identify a phishing email?
- What is email spoofing?
- Why are phishing emails dangerous?
- How can you verify the sender’s authenticity?
- What tools can analyze email headers?
- What actions should be taken on suspected phishing emails?
- How do attackers use social engineering in phishing?

Key Concepts:

- Phishing
- Email spoofing
- Header analysis
- Social engineering
- Threat detection