For my project, I analyzed a phishing email to understand common tactics used by cybercriminals. Here’s how I approached it:

I have square marked the points in image for understanding these points.

1. Obtained a Sample Phishing Email – I downloaded a free sample from a reputable cybersecurity resource to study its structure.

2. Examined the Sender’s Email Address – I checked for spoofing by looking for slight misspellings or fake domains (e.g., support@amaz0n.com instead of support@amazon.com ).

3. Analyzed Email Headers – I used an online email header analyzer to trace the sender’s real IP and found inconsistencies in the "Received" fields, indicating possible forgery.

4. Identified Suspicious Links & Attachments – The email had a fake login link I did not download any attachments to avoid malware risks.

5. Noted Urgent/Threatening Language – Phrases like "Your account will be suspended in 24 hours!" pressured users into acting quickly—a classic phishing tactic.

6. Checked for Mismatched URLs – Hovering over the "Verify Account" button revealed a different (malicious) link than what was displayed.

7. Looked for Spelling & Grammar Errors – The email had awkward phrasing (e.g., "Dear Costumer" ) and typos, common in phishing attempts.

8. Summarized Key Phishing Traits – The email used urgency, fake sender details, hidden malicious links, and poor grammar—all red flags of a phishing scam.

Through this analysis, I learned how to spot phishing attempts and the importance of verifying emails before clicking. This project helped me understand cybersecurity risks better.

For tutorial I watched a YouTube video link is : https://youtu.be/bAudsieH4o0?si=3Wvb6NBiUkJz\_hl7