Task 11: Phishing Attack Simulation & Detection

🎯 Aim

To understand how phishing attacks work by simulating a controlled phishing campaign in a **test environment**, analyze user responses, identify phishing red flags, and learn prevention techniques to improve social engineering awareness.

🧠 Introduction

Phishing is a social engineering attack where attackers trick users into revealing sensitive information such as usernames, passwords, or OTPs by impersonating trusted entities via email or messages.

This experiment demonstrates a **phishing simulation** using **GoPhish** (or manual templates) for **learning and detection purposes only**.

🛠️ Tools Used

- **Primary Tool:** GoPhish (Phishing simulation framework)
- **Alternative:** Manual phishing email & landing page templates
- **Environment:** Localhost / Test email accounts only

🧪 Experiment Setup

Step 1: Understanding Phishing Attacks

Common phishing types:

- Email phishing
- Spear phishing
- Clone phishing
- Credential harvesting
- Malicious links & attachments

Step 2: Creating a Fake Email Template (Simulation)

A sample phishing-style email was created to imitate a common login alert.

Example Email Content (For Awareness Only):

- Subject: *Security Alert – Action Required*
- Message urges user to verify account
- Includes a clickable link
- Uses urgent language

⚠️ **Note:** This email is sent only to test accounts.

Step 3: Setting Up a Landing Page

- A fake login page was created
- Page mimics a generic login form
- Data submitted is **not used**, only logged for analysis
- Hosted locally via GoPhish

Step 4: Sending Test Phishing Email

- Emails sent to **dummy/test email IDs**
- Campaign launched inside GoPhish
- No real users involved

Step 5: Tracking Responses

GoPhish dashboard tracks:

- Email delivered
- Email opened
- Link clicked

- Credentials submitted

This helps measure how phishing attacks succeed.

📊 Observations & Results

Activity	Observation
Email opened	Yes
Link clicked	Yes
Credentials submitted	Yes (test data)
User awareness	Low initially

🚩 Identified Phishing Red Flags

- Urgent or threatening language
- Suspicious sender email address
- Generic greetings (Dear User)
- Unexpected login alerts
- URL mismatch on hover
- Spelling or grammar mistakes

🛡 Prevention Techniques

- Verify sender email carefully
- Hover over links before clicking
- Never share credentials via email
- Enable Multi-Factor Authentication (MFA)
- Use email spam filters
- Conduct regular phishing awareness training

✅ Final Outcome

- Gained practical understanding of phishing techniques
- Learned how attackers manipulate human behavior
- Identified phishing indicators
- Improved awareness of social engineering attacks
- Understood importance of cybersecurity training

📜 Conclusion

This phishing simulation highlights how easily users can be deceived through social engineering. Awareness, training, and technical controls are essential to prevent phishing attacks and protect sensitive information