Task 11 – Phishing Attack Simulation & Detection

Objective

The objective of this task is to understand phishing attacks, simulate a phishing scenario in a controlled and ethical environment, identify common phishing red flags, and learn prevention techniques to improve social engineering awareness.

Tool Used

GoPhish (conceptual simulation)
Manual phishing email and landing page templates

Task Description

In this task, a phishing attack scenario was simulated strictly for educational purposes. A fake email template resembling a password expiry notification was created to demonstrate how phishing emails are designed. A dummy landing page was used to explain how attackers attempt to steal user credentials. No real users were targeted and no real credentials were collected during this simulation.

Phishing Scenario

Email Theme: Password Expiry Notification
Attack Method: Email Phishing
Landing Page: Dummy login page created only for awareness and training purposes

Red Flags Identified

Urgent and threatening language asking for immediate action
Suspicious sender email address
Generic greeting instead of user name
Unverified or misleading links
Request for sensitive information such as passwords

What is Phishing?

Phishing is a type of social engineering attack where attackers impersonate legitimate organizations or individuals to trick users into revealing sensitive information like usernames, passwords, banking details, or personal data.

Types of Phishing

Email phishing
Spear phishing
Smishing (SMS-based phishing)
Vishing (voice-based phishing)

Why Phishing is Dangerous?

It can lead to credential theft
Financial fraud and monetary loss
Identity theft
Data breaches and system compromise

Prevention Techniques

User awareness and security training
Verifying sender email addresses and URLs
Avoid clicking on unknown or suspicious links
Using Multi-Factor Authentication (MFA)
Email filtering and security solutions

Conclusion

This task helped in understanding how phishing attacks work and how they exploit human psychology rather than technical vulnerabilities. It improved awareness of phishing red flags and reinforced best practices for preventing social engineering attacks in real-world scenarios.