CYBER SECURITY INTERNSHIP – TASK 11

Phishing Attack Simulation & Detection

---

1. Introduction

Phishing is a social engineering attack in which attackers attempt to trick users into revealing sensitive information such as usernames, passwords, or financial details. Phishing attacks are commonly carried out through emails, messages, or fake websites that appear legitimate. This task focuses on simulating a phishing attack in a safe and controlled manner and learning how to detect and prevent such attacks.

---

2. What is Phishing?

Phishing is a cyber attack technique that uses deception to manipulate users into performing actions that compromise security. Attackers often impersonate trusted organizations to gain user trust.

---

3. Types of Phishing Attacks

- **Email Phishing:** Fraudulent emails sent to many users
- **Spear Phishing:** Targeted phishing attack on specific individuals
- **Smishing:** Phishing through SMS messages
- **Vishing:** Phishing through voice calls
- **Clone Phishing:** Copy of a legitimate email with malicious links

---

4. Phishing Email Simulation

A simulated phishing email was created for learning purposes.

Sample Phishing Email

Subject:

```
Urgent: Verify Your Account Immediately
```

Email Body:

```
Dear User,

Your account has been temporarily suspended due to suspicious activity.
Please verify your account immediately to avoid permanent suspension.

Click the link below to verify your account.

Thank you,
Security Team
```

This email uses urgency and fear to manipulate users into clicking a malicious link.

---

5. Fake Landing Page (Conceptual)

In a real phishing attack, the email link redirects users to a fake login page that looks like a legitimate website. This page is designed to steal user credentials.

For this task, the landing page concept was studied without creating or deploying a real phishing page.

---

6. Phishing Simulation Method

The phishing attack was simulated for awareness purposes only. No real users were targeted, and no real credentials were collected. The simulation helps in understanding how phishing campaigns are structured.

---

7. Phishing Indicators and Red Flags

Common signs of phishing emails include:

- Urgent or threatening language
- Unknown or suspicious sender
- Unexpected attachments or links
- Spelling and grammar mistakes
- Requests for personal or login information

---

8. Detection and Analysis

Phishing detection involves analyzing email headers, checking sender authenticity, hovering over links to inspect URLs, and verifying message content. User awareness plays a critical role in detecting phishing attacks.

---

9. Phishing Prevention Techniques

- Verify sender email addresses
- Avoid clicking suspicious links
- Enable Multi-Factor Authentication (MFA)
- Use email spam filters
- Conduct regular security awareness training

---

10. Impact of Phishing Attacks

Phishing attacks can lead to:

- Account compromise
- Financial loss
- Identity theft
- Malware infection
- Data breaches