Task 11: Phishing Attack Simulation & Detection Report

---

1. Introduction

Phishing is a type of social engineering attack where attackers impersonate legitimate organizations or individuals to trick victims into revealing sensitive information such as usernames, passwords, credit card details, and OTP codes. Phishing attacks are commonly delivered through emails, SMS messages, phone calls, and fake websites.

Phishing is one of the most common cyber threats and is responsible for major data breaches and financial frauds worldwide.

---

2. Tools Used

The following tools were used for this task:

- GoPhish – An open-source phishing simulation framework
- Manual phishing email templates
- Fake landing page (HTML login page)

---

3. Phishing Simulation Methodology

Step 1: Understanding Phishing Attacks

Phishing attacks exploit human psychology by creating urgency, fear, or curiosity to trick users into clicking malicious links.

Step 2: Creating Phishing Email Template

A fake email template was created pretending to be a security alert message. The email contained a malicious link redirecting users to a fake login page.

Step 3: Setting Up Landing Page

A fake login page was designed to capture test credentials. This page simulates a real website login interface.

Step 4: Sending Test Phishing Email

Test phishing emails were sent to dummy accounts using GoPhish to simulate a real-world phishing campaign.

Step 5: Tracking Responses

GoPhish dashboard was used to track:

- Email opened
- Link clicked
- Credentials submitted

---

4. Findings and Observations

During the phishing simulation, the following observations were made:

- Users clicked phishing links due to urgency messages
- Fake domains successfully tricked users
- Lack of awareness increased phishing success rate
- Many users did not verify sender email addresses

---

5. Phishing Red Flags

The following red flags help identify phishing attacks:

1. Unknown or spoofed sender address
2. Urgent messages like “Account will be blocked”
3. Suspicious or shortened URLs
4. Grammar and spelling mistakes
5. Unexpected attachments

---

6. Prevention Methods

To prevent phishing attacks, the following security measures are recommended:

- Conduct cybersecurity awareness training
- Use email spam filters and anti-phishing tools
- Enable Multi-Factor Authentication (MFA)
- Verify suspicious emails before clicking links
- Do not share passwords or OTPs via email

---

7. Interview Questions and Answers

What is phishing?

Phishing is a social engineering attack where attackers impersonate trusted entities to steal sensitive information such as passwords and financial data.

Types of phishing?

- Email phishing
- Spear phishing
- Smishing (SMS phishing)
- Vishing (Voice phishing)

How to detect phishing?

Check sender address, suspicious links, urgent messages, grammar mistakes, and unknown attachments.

Why phishing is dangerous?

Phishing can lead to identity theft, financial loss, and data breaches.

Prevention methods?

User awareness training, MFA, email filtering, and verifying suspicious messages.

---

8. Conclusion

Phishing attack simulation helps organizations and individuals understand social engineering techniques and improve cybersecurity awareness. By identifying phishing red flags and applying prevention methods, cyber risks can be significantly reduced.

Prepared by: SAFFIQ MOHAMMED S