Code Alpha Internship

Task 2: Phishing Awareness Training

Submitted by: Saira Arshad

STUDENT ID: CA/AU1/8075

Date: August 2025

Duration : 1 month

Table of Contents

1. Introduction

Phishing is a deceptive cyberattack that manipulates users into revealing sensitive data like passwords and financial information. This report outlines the training content developed during the CodeAlpha Cybersecurity Internship, covering phishing detection, examples, and prevention strategies.

2. Objectives of the Training Module

- Educate about phishing threats and techniques - Help identify phishing emails and fake websites - Explain social engineering tactics - Provide prevention tips and best practices - Engage users through quizzes and real-world scenarios

3. Training Methods Used

- Simulated phishing campaigns - Email header analysis - Workshops and live discussions - Social engineering recognition - OSINT for threat hunting - Incident response simulations - Data-driven training adjustments

4. Recognizing Social Engineering Tactics -

Impersonation: Attackers pose as trusted contacts (boss, IT support) - Pretexting: Fabricated scenarios to gain trust -

Urgency & fear: Panic-inducing messages - Free offers: Bait using fake rewards or giveaways

5. Real-World Phishing Case Studies

1. Twitter Hack (2020): Spear phishing attack compromised high-profile accounts through internal tool access.

2. Google & Facebook Scam (2017): Over $100 million stolen via fake supplier invoices.

3. Pakistani Banks Breach (2018): Mass phishing resulted in credit/debit card data leaks and service suspension.

6. Best Practices to Avoid Phishing

- Avoid clicking on suspicious links - Verify sender details - Use 2FA and secure passwords - Report suspicious emails - Keep systems updated

7. Interactive Quiz (Sample Questions)

1. What should you do if a bank asks you to verify your password via email? - Correct: Call the bank using the official number. 2. Which is a sign of a phishing email? - Correct: Urgent and threatening language. 3. What does a mismatched URL imply? - Correct: Potential phishing link. 4. Should you give passwords over the phone? - Correct: Never. Report the

request. 5. How to best protect against phishing? - Correct: Use Two-Factor Authentication (2FA).

8. Conclusion

Phishing threats are real and evolving. Stay cautious, verify communication, and never act on impulse. Your awareness can protect both personal and organizational data. Cybersecurity is everyone's responsibility.