Phishing Awareness Training

Objective

To educate individuals about phishing attacks, how to recognize them, understand the tactics used by attackers, and adopt safe online practices to avoid falling victim.

What is Phishing?

Phishing is a type of cyberattack where attackers impersonate legitimate entities to steal sensitive information such as login credentials, credit card numbers, or personal data.

Types of Phishing Attacks

- Email Phishing
- Spear Phishing
- Smishing
- Vishing
- Website Spoofing

How to Recognize a Phishing Email

- Urgent or threatening language
- Unfamiliar or misspelled sender addresses
- Unexpected attachments or links
- Poor grammar and spelling
- Requests for sensitive info
- Mismatched URLs

Social Engineering Tactics

Phishing Awareness Training

- Trust exploitation
- Fear-based pressure
- Incentive baiting
- Impersonation of authority

Best Practices to Prevent Phishing

- Verify sender's email address
- Avoid suspicious links
- Use MFA
- Use a password manager
- Report suspicious messages

Real-World Examples

- PayPal Scam: Fake login alert
- COVID-19 Scams: Fake health advisory emails
- Job Offer Scams: Unrealistic offers asking for personal info

Interactive Quiz (Sample)

1. What is a common indicator of a phishing email?
   - A) Proper grammar
   - B) Known sender
   - C) Urgent and threatening tone [Correct]

2. What should you do if you suspect phishing?
   - A) Click and see

Phishing Awareness Training

- B) Report it and delete it [Correct]

- C) Reply for confirmation

Conclusion

Phishing attacks are increasingly sophisticated. By staying vigilant, understanding attacker tactics, and following cybersecurity best practices, individuals can significantly reduce their risk of falling victim.

Submission Instructions

- Upload as PDF or module

- Post video explanation on LinkedIn

- Include GitHub link: CodeAlpha_PhishingAwareness

- Submit using the provided form