Phishing Awareness Training

Task 2

Introduction

- Phishing is a cyber attack where attackers trick people into sharing sensitive information.
- They use fake emails, websites, or messages.
- This training helps you identify and avoid phishing attempts.

What is Phishing?

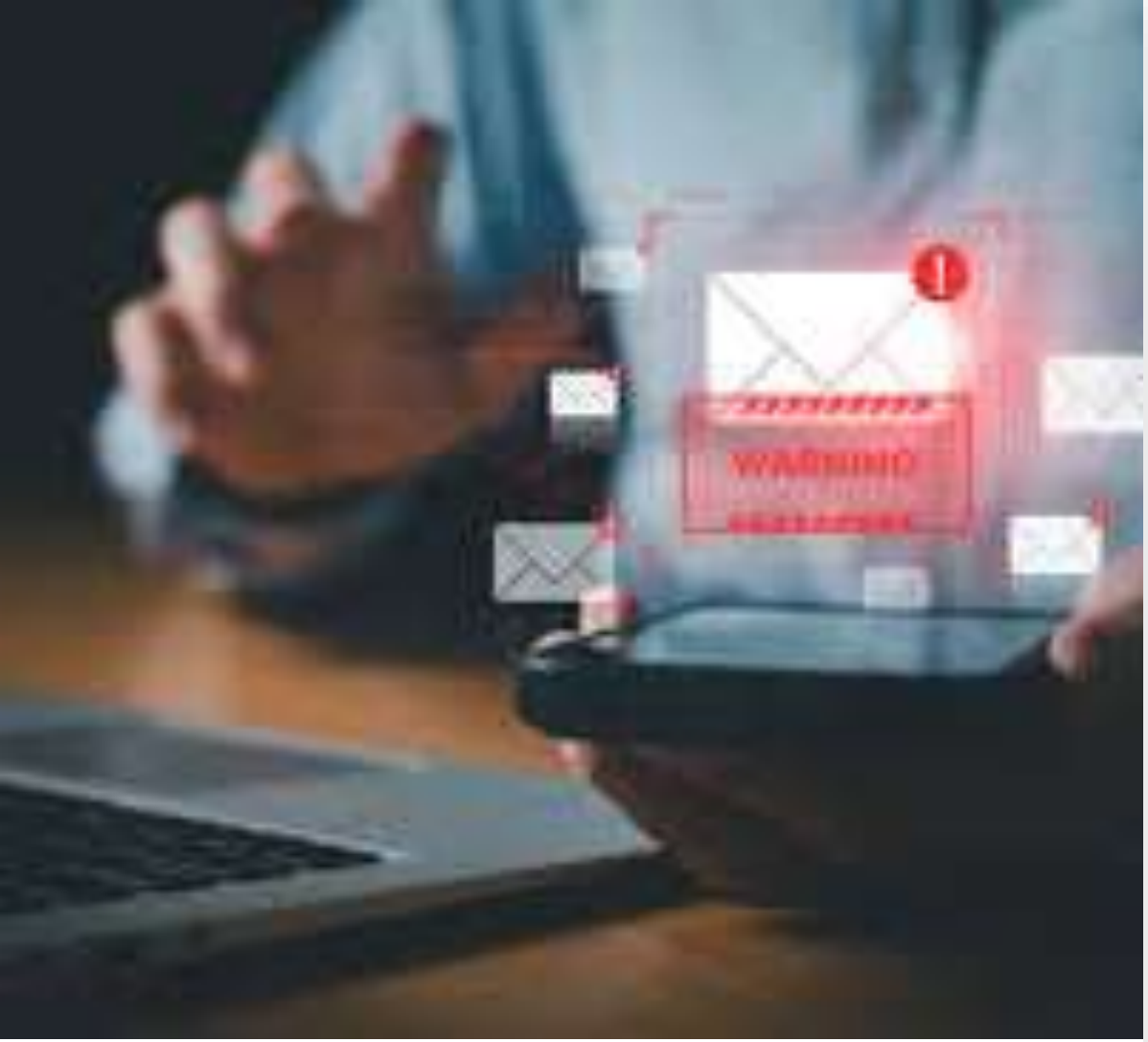
- Fake attempt to steal sensitive data (passwords, bank details, etc.).
- Done via emails, SMS, phone calls, or websites.
- Often looks like a trusted source.

Types of Phishing

- Email Phishing
- Spear Phishing (targeted attack)
- Smishing (SMS phishing)
- Vishing (voice call phishing)
- Clone Phishing (fake copy of real email)

How to Recognize a Phishing Email

- Spelling/grammar mistakes
- Suspicious sender address
- Fake URLs (hover to check link)
- Urgent language ('Your account will be blocked...')
- Unusual attachments



Real-World Examples

- Fake email pretending to be a bank
- Suspicious links and attachments
- Always verify before clicking any link

Social Engineering Tactics

- Fear (account suspended, fines, etc.)
- Curiosity (You won a prize!)
- Urgency (Reply within 24 hours)
- Trust (Pretend to be boss, bank, IT dept.)

Best Practices to Stay Safe

- Don’t click unknown links
- Verify sender before replying
- Never share passwords via email
- Enable two-factor authentication (2FA)
- Use updated antivirus & spam filters

Quick Quiz

- Q: If an email asks for your password, is it phishing? (Yes)
- Q: Should you click links from your bank email? (No)
- Q: What is Smishing? (Phishing via SMS)

Conclusion

- Phishing attacks are increasing every day.
- Awareness is the best defense.
- Stay alert, stay safe.