PHISHING AWARENESS TRAINING

CodeAlpha Cyber Security Internship | Sujal Mahto

WHAT IS PHISHING?

- Phishing is a type of cyber attack where attackers trick users into revealing sensitive information like passwords, credit card numbers, or personal data by pretending to be a trustworthy entity.

TYPES OF PHISHING ATTACKS

- - Email Phishing
- - Spear Phishing
- - Whaling
- - Smishing (SMS Phishing)
- - Vishing (Voice Phishing)

HOW PHISHING WORKS

- Attackers send fake messages or websites to trick users. When the user clicks the link or submits information, the attacker captures it for malicious use.

COMMON SIGNS OF PHISHING EMAILS

- - Generic greetings (e.g., Dear User)
- - Urgent language or threats
- - Suspicious links or attachments
- - Spelling and grammar errors
- - Unusual sender email addresses

REAL-LIFE EXAMPLES

- - Fake bank login pages
- - Emails posing as company executives
- - Fraudulent job offer emails
- - Fake password reset links

HOW TO PROTECT YOURSELF

- - Never click suspicious links
- - Verify email addresses
- - Use multi-factor authentication
- - Install anti-virus and anti-phishing tools
- - Report phishing attempts

DOS AND DON’TS

- ✅ Do: Check URLs, use strong passwords, stay informed
- ❌ Don’t: Share OTPs or passwords, click unknown links, respond to suspicious messages

CONCLUSION & AWARENESS TIPS

- Phishing attacks are common but preventable. Stay alert, educate others, and report phishing emails. Cyber security starts with awareness!