



Phishing Awareness Training

Cyber Security Internship – CodeAlpha

Presented by: [Aditya]

Objective: To educate users about phishing attacks and how to stay safe online.

What is Phishing?



Understanding the Threat

Phishing is a **social engineering attack** where attackers impersonate trusted entities to trick individuals into revealing sensitive information.

Attackers steal:

- Login credentials
- One-Time Passcodes (OTPs)
- Credit and debit card details

Common platforms: Email, SMS, websites, and phone calls

Types of Phishing Attacks

Attackers use various methods to trick their victims. Here are the most common types:



Email Phishing

Fake emails pretending to be from banks or legitimate companies



Smishing

Phishing attacks delivered through SMS text messages



Vishing

Voice calls from attackers pretending to be support staff or officials



Website Phishing

Fake websites designed to look identical to legitimate ones

How to Identify Phishing Attempts

Warning Signs to Watch For

Unknown Sender

Messages from unfamiliar email addresses or phone numbers

Urgent Messages

Pressure tactics like "Account will be blocked immediately"

Spelling Mistakes

Grammar and spelling errors in professional communications

Suspicious Links

Links that look unusual or redirect to unexpected websites

Information Requests

Asking for personal or financial details you wouldn't normally share

How to Protect Yourself

Best Practices for Staying Safe

01

Don't Click Unknown Links

Never click on links in suspicious messages

02

Verify the Sender

Check email addresses and phone numbers carefully

03

Inspect URLs

Look for HTTPS and correct domain names

04

Enable 2FA

Two-Factor Authentication adds extra protection

05

Update Software

Keep browsers and security software current

06

Never Share Credentials

Don't share OTPs or passwords with anyone



Real-World Example

"Your account is suspended.
Click here to verify
immediately."



Why This is Phishing:

- **Fear and urgency:** Creates panic to bypass rational thinking
- **Suspicious link:** Redirects to fake verification page
- **Sensitive data:** Requests login credentials or financial information

Key Takeaways

- Phishing is one of the most common cyber attacks
- Awareness is your strongest defense
- Always think before you click
- When in doubt, verify through official channels