PHISHING AWARENESS TRAINING PRESENTATION

Title: Phishing Awareness Training

Subtitle: Protect Yourself Against Online Scams

INTRODUCTION TO PHISHING

What is Phishing?

A brief definition explaining phishing as a type of cyber attack where attackers deceive individuals into providing sensitive information by pretending to be a trustworthy entity.

WHY PHISHING IS DANGEROUS

Loss of personal or financial information.
Identity theft.

Unauthorized access to sensitive data and accounts.

COMMON TYPES OF PHISHING ATTACKS

Email Phishing:

- Examples of fake emails that look legitimate.
- Techniques used: fake links, urgent messages, requests for personal info.

Spear Phishing:

- Targeted attacks on specific individuals or organizations.
- Customized messages that appear more personal and convincing.

Vishing (Voice Phishing):

Phone calls pretending to be legitimate organizations to steal information.

Website Phishing:

Fake websites that mimic real ones to capture login credentials and other sensitive information.

Smishing (SMS Phishing):

Fraudulent SMS messages that ask for personal information.

RECOGNIZING PHISHING EMAILS

Key Indicators of Phishing Emails

Suspicious Sender Address

Slight variations in email addresses that mimic legitimate ones.

Urgent or Threatening Language

Phrases like "Your account will be suspended!" to create panic.

Generic Greetings

Emails that use "Dear Customer" instead of your name.

Unusual Attachments or Link

Files or links that you weren't expecting.

Poor Grammar and Spelling

Common mistakes in the email body.

IDENTIFYING PHISHING WEBSITES

Signs of a Phishing Website

Check the URL

Verify the spelling and structure of the URL. Ensure it starts with "https://".

Look for a Padlock Icon

A sign that the website is secure (though not foolproof).

Suspicious Design

Poorly designed websites with broken links or odd layouts.

Contact Information

Fake websites often have fake or no contact details.

Social Engineering Tactics

What is Social Engineering?

- A method where attackers manipulate individuals into divulging confidential information.

COMMON SOCIAL ENGINEERING TECHNIQUES

Pretexting

Creating a fabricated scenario to gain your trust.

Baiting

Offering something enticing, like free software, to trick you into downloading malware.

Tailgating

Physically following someone into a restricted area by pretending to be authorized.

Avoiding Phishing Scams

BEST PRACTICES TO AVOID PHISHING

General Tips

Don’t Click on Suspicious Links

Always hover over links to see the actual URL.

Verify the Source

Contact the sender directly using known contact information before providing any sensitive info.

Use Strong Passwords

Regularly update your passwords and avoid reusing them across multiple sites.

Enable Two-Factor Authentication

Adds an extra layer of security to your accounts.

Regularly Update Software

Keep your operating system and applications up to date to protect against vulnerabilities.

Responding to Phishing Attempts

IMMEDIATE STEPS

General Tips

Do Not Respond

Ignore and delete suspicious emails or messages.

Report Phishing

Use your email provider’s phishing report feature or notify your IT department.

Change Passwords

If you suspect your credentials were compromised, update your passwords immediately.

Monitor Accounts

Keep an eye on your financial accounts and report any suspicious activity.

Incident Response Plan

Outline the steps your organization takes when a phishing attempt is reported.

INTERACTIVE QUIZ

Quiz Questions:

- Example1: "What is the first thing you should do if you suspect an email is a phishing attempt?"
- Example2: "Which of the following is a sign of a phishing website?"

CASE STUDIES

- Case Study 1: In group discusion or individual, analyze a real-life phishing attack and discuss how it was carried out and the consequences.
- Case Study 2: In group discusion or individual, discuss a situation where an individual successfully avoided a phishing scam and how they recognized the signs.

RESOURCES AND FURTHER READING

List of Resources

- Links to cybersecurity blogs, government websites, and online courses for further learning.
- IT Contact Information: Provide contact details for your organization's IT or cybersecurity team.
- Books and Articles: Recommend books or articles for deeper insights into phishing and cybersecurity.

8. CONCLUSION

- Recap: Summarize key points on recognizing and avoiding phishing attacks.
- Resources: Provide links to further reading, security tools, and contact information for IT support.

FEEDBACK AND Q&A

- Feedback Form: Collect feedback to improve the training module.
- Q&A Session: Address any questions or concerns from participants.

THANK YOU