Phishing Awareness Training

Md Zahidul Islam

From

CodeAlpha Cyber Security Intern

Introduction

Protect Yourself from Cyber Threats

- Welcome participants.
- Explain the importance of understanding and recognizing phishing attacks.
- Brief overview of the training agenda.

What is Phishing?

- Definition: Phishing is a type of cyber attack where attackers attempt to trick individuals into providing sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity.
- Mention common mediums: emails, websites, and messages.

Types of Phishing Attacks

- **Email Phishing**: Fake emails that look legitimate.
- **Spear Phishing**: Targeted attacks on specific individuals or organizations.
- **Whaling**: Targeting high-profile individuals like executives.
- **Smishing**: Phishing via SMS messages.
- **Vishing**: Phishing via phone calls.
- **Clone Phishing**: Duplicating a legitimate email with malicious content.

Recognizing Phishing Emails

- **Suspicious Sender**: Check the email address for inconsistencies.
- **Generic Greetings**: Use of non-personalized greetings.
- **Urgency and Threats**: Phrases like "urgent action required" or "your account will be locked."
- **Unexpected Attachments or Links**: Be cautious of unsolicited attachments or links.
- **Spelling and Grammar Mistakes**: Poor language usage can be a red flag.

Recognizing Phishing Websites

- **Check the URL**: Look for misspelled or altered URLs.
- **HTTPS and Security Certificates**: Ensure the website uses HTTPS.
- **Pop-up Forms**: Avoid entering information in pop-up windows.
- **Poor Design and Layout**: Unprofessional appearance and layout.

Social Engineering Tactics

- **Impersonation:** Attackers pretend to be someone you trust.
- **Pretexting:** Creating a fabricated scenario to steal information.
- **Baiting:** Offering something enticing to trick individuals.
- **Tailgating:** Following someone to gain physical access to a restricted area.

How to Protect Yourself

- **Verify Sources:** Always verify the sender before responding.
- **Don’t Click on Suspicious Links:** Hover over links to check the URL.
- **Use Strong Passwords:** Utilize complex and unique passwords for different accounts.
- **Enable Two-Factor Authentication (2FA):** Adds an extra layer of security.
- **Keep Software Updated:** Regular updates can protect against vulnerabilities.
- **Report Phishing Attempts:** Report to IT or relevant authorities.

Real-World Examples

- Share examples of phishing emails and websites.
- Discuss recent phishing attacks and their impact.

Interactive Quiz

- Provide a short quiz with scenarios for participants to identify phishing attempts.
- **Example Question:** "You receive an email from your bank asking for your password. What should you do?"

Summary and Q&A

- Recap key points from the training.
- Open the floor for questions and discussion.
- Provide contact information for further assistance.

Thank You

Phishing Awareness Training

Md Zahidul Islam

From

CodeAlpha Cyber Security Intern