Phishing Awareness Training

How to Identify and Avoid Phishing Emails

Introduction

- Phishing is a form of cyber attack where attackers impersonate legitimate entities to deceive individuals into providing sensitive information.

- In this training, we will learn how to identify phishing emails and protect ourselves and the organization.

What is Phishing?

- Phishing is a cybercrime where attackers disguise themselves as trusted entities to trick individuals into sharing confidential information.

- Common targets include personal data, login credentials, and financial information.

Indicators of Phishing Emails

- 1. Suspicious sender address
- 2. Generic greetings (e.g., 'Dear Customer')
- 3. Urgent language prompting immediate action
- 4. Poor grammar and spelling mistakes
- 5. Suspicious links or attachments
- 6. Requests for sensitive information
- 7. Unusual domain names

Examples of Phishing Emails

- Example 1:
- Sender: info@bankxyz.com
- Subject: Urgent: Account Verification Needed

- Example 2:
- Sender: support@randomservice.com
- Subject: Your Password Has Been Compromised

How to Avoid Phishing Emails

- 1. Verify the sender's email address.
- 2. Look for personalized greetings.
- 3. Avoid clicking on suspicious links; hover over them first.
- 4. Do not download attachments from unknown sources.
- 5. Be cautious of urgent requests for sensitive information.
- 6. Use official channels to verify requests.

Reporting Suspicious Emails

- If you receive a suspicious email:
- 1. Do not respond or click any links.
- 2. Forward the email to your IT department or security team.
- 3. Delete the email from your inbox.
- 4. Inform your colleagues about the phishing attempt.

Conclusion

- Awareness and vigilance are key to preventing phishing attacks.
- By following these guidelines, you can help protect yourself and our organization from cyber threats.