PHISHING AWARENESS TRAINING

BY: DHRUMAN DAS

INTRODUCTION

➢ What is Phishing?

- Phishing is a form of cyber attack where a malicious actor, often posing as a trustworthy entity, attempts to deceive individuals into divulging sensitive information such as passwords, credit card numbers, or other personal data.
- This is typically done through fraudulent emails, messages, or websites that mimic legitimate sources.

➢ How does Phishing attacks generally works?

- Deceptive Communication
- Sense of Urgency or Fear
- Fake Websites
- Malware Delivery
- Targeting Individuals or Organizations
- Spear Phishing

Types of Phishing Attacks

Social Engineering

Manipulating individual's to divulge confidential information's.
Examples: Impersonation, emotional manipulation.

Website Phishing

Fraudulent websites imitating legitimate ones.
Examples: Fake login pages, malicious websites.

Email Phishing

Deceptive emails to extract information.
Examples: Fake security alerts, account verification requests.

Common Characteristics of Phishing Attempts

- Urgency: Creating a sense of immediate action.
- Unexpected Emails: Receiving unsolicited emails.
- Suspicious Links: Hover our links to preview URL'S.
- Requests for Personal Information: Be Cautious.

Recognizing Phishing Emails

Check the Sender's Email Address.

Look for Spelling and Grammar mistakes

Verify Email Content

Hover Our Links to Preview URL's

Recognizing Phishing Websites

Check the URL'S

Look for HTTPS

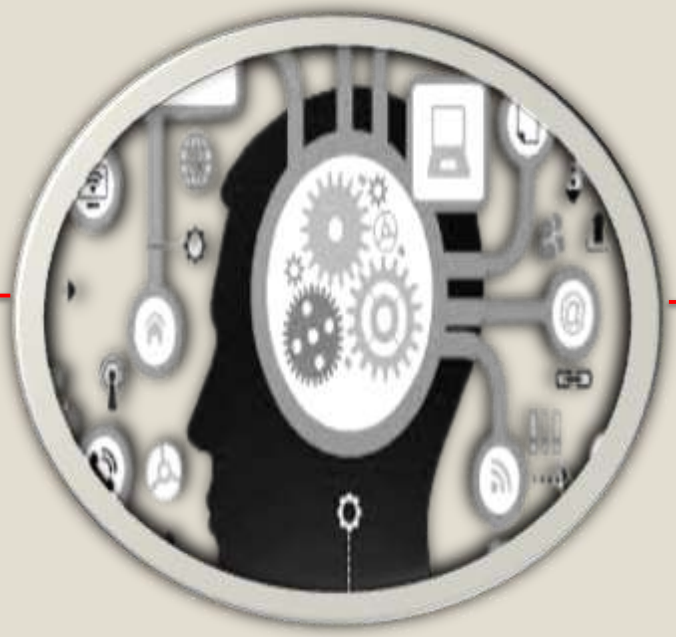
Verify Website Legitimacy

Be Cautions with Pop-Up Forms

SOCIAL ENGINEERING TACTICS

Impersonations Techniques

Manipulations of Trust



Exploiting Human Emotions

Awareness of Social Media Manipulation

Protecting Personal Information

- Never Share Passwords via Email.
- Use Two-Factor Authentication.
- Verify Requests for Sensitive Information.
- Be Cautions with Personal Information Sharing.

Best Practices for Avoiding Phishing Attacks

- Keep software updated and use security software.
- Educate and train employees.
- Regularly backup important data.

Conclusion

- Key Points Recap:

  - Phishing attacks are pervasive and continuously evolving tactics used by cybercriminals to deceive individuals and organizations.
  - Email phishing, website spoofing, and social engineering are common methods used in phishing attacks.
  - Recognizing phishing indicators such as suspicious sender addresses, urgent language, and deceptive URLs is crucial in mitigating risks.

- Importance of Vigilance:

  - Maintaining high level of awareness and skepticism towards unsolicited communications is essential
  - Regularly verify the authenticity of websites and refrain from clicking on links or downloading attachments from unknown or suspicious sources.

- Take Action:

- Implement robust cybersecurity measures, including spam filters, antivirus software, and multi-factor authentication (MFA), to protect against phishing promptly.

- Educate employees, friends, and family members about phishing techniques and encourage reporting of suspicious activities promptly.

- Continuous Learning:

- Cybersecurity is a dynamic field; staying informed about emerging threats and best practices is a key to safeguarding personal and organizational information.

- Regularly update security protocols and participate in phishing awareness training to reinforce knowledge and readiness.

THANK YOU