PHISHING AWARENESS TRAINING

By
Lokesh Sarode

Introduction

- Welcome to our presentation on mitigating phishing attacks.
- Today, we will discuss the various aspects of recognizing and avoiding phishing emails, websites, and social engineering tactics.

Understanding Phishing

- Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity.
- It is commonly executed through emails, websites, or social engineering techniques.

Types of Phishing Attacks

1. Email Phishing: Deceptive emails that appear to be from legitimate sources, urging recipients to click on malicious links or provide personal information.
2. Website Phishing: Fake websites designed to mimic legitimate ones, aiming to steal login credentials or financial information.
3. Social Engineering: Manipulative tactics used to trick individuals into divulging confidential information or performing certain actions.

Recognizing Phishing Emails

- Look for spelling and grammatical errors.
- Verify the sender's email address.
- Be cautious of urgent or threatening language.
- Avoid clicking on suspicious links or attachments.
- Verify requests for sensitive information through other means of communication.

Avoiding Phishing Websites

- Check the website's URL for inconsistencies or misspellings.
- Look for secure connections (HTTPS) and trust indicators like padlock icons.
- Be wary of pop-ups or requests for sensitive information.
- Use reputable security software to detect and block malicious websites.

Social Engineering Tactics

Be cautious of unsolicited requests for information or assistance.

Verify the identity of individuals asking for sensitive data.

Avoid sharing personal or financial information over the phone or online without verification.

Educate yourself and your team on common social engineering tactics and how to recognize them.

Best Practices for Protection

- Keep software and security solutions up to date.
- Enable multi-factor authentication wherever possible.
- Educate employees through regular training and awareness programs.
- Implement strict policies for handling sensitive information.
- Encourage reporting of suspicious emails or activities.

Conclusion

- Phishing attacks continue to pose a significant threat to individuals and organizations.
- By staying vigilant, educating ourselves, and implementing proactive measures, we can effectively mitigate the risks associated with phishing.