PHISHING AWARENESS TRAINING

Mugeha

Understanding Phishing

Identify	Identify Phishing
Learn	Learn to recognize the signs of phishing attempts, including suspicious email addresses, grammatical errors and urgent requests for personal information to protect yourself.
Report	Report suspicious emails
Encourage	Encourage individuals to report suspicious emails to IT support or management immediately, helping to mitigate potential threats and reinforce a culture of security awareness.

Understanding Phishing: Definition and Types

Recognize the various phishing techniques such as spear phishing, whaling and vishing. Implement multi-factor authentication and regular security training to strengthen defenses against targeted attacks, ensuring employees are equipped to identify and report suspicious communications promptly.

Common Phishing techniques and tactics

- Email Spoofing

Check sender's email address thoroughly to confirm it matches official domains before responding.

- Malicious Links

Hover over links to preview URLs without clicking, and verify them with official websites.

- Urgent Requests

Be cautious of unexpected messages using immediate actions; always verify through trusted communication channels.

Recognizing Phishing Attacks in Emails

- Check Sender

Ensure the sender's email is familiar and legitimate.

- Look for Errors

Be cautious of spelling or grammatical mistakes in the message.

- Attachments Caution

Never open attachments from unknown or suspicious sources.

- Too Good to be True

Be skeptical of emails offering unrealistic deals or prizes.

- Monitor Links

Hover over the links to see if they lead to trusted websites.

- Urgency Tactics

Beware of emails that create a false sense of urgency to act quickly.

- Verify Requests

Check if request for personal information seem legitimate.

Spotting Phishing Websites and Links

- Check URL

Ensure the website URL matches the legitimate site, including spelling and domain extensions.

- Look for HTTPS

Confirm that the website uses HTTPS, without it, your data might not be secure.

- Text Here

Evaluate the website design, poorly designed sites often indicates a phishing attempt.

- Review Contact Information

Legitimate websites provide clear contact details: phishing sites usually lacks this information.

- Verify Email Source

Always verify that the email source requesting your information is legitimate before clicking links.

The Role of Social Engineering in Phishing

- Trust Exploitation

Attackers exploit established trust relationships for deceptive communication.

- Urgency Tactics

Create a false sense of urgency to elicit immediate responses from targets.

- Text Here

Use personal details to make phishing attempts appear more authentic.

Mimic legitimate entities to manipulate victims into revealing sensitive data.

Leverage fear, curiosity, or sympathy to push victims into compliance.

Real World Phishing Case Studies

- Problem Faced

Employees fell for a fake bank email scam.

- Solution Offered

Implementing a multi-layered email filtering system

- Benefits

Reduced phishing attempts by 80% instantly.

Effective Strategies To Prevent Phishing

- Verify Sources

Always confirm the identity of the sender before responding.

- Use Strong Passwords

Implement complex passwords and change them regularly to enhance security.

- Report Suspicion

Immediately report any suspicious emails to your IT department.

- Educate Staff

Regular training sessions improve awareness and reduce risk of phishing.

Implementing Cybersecurity Policies and Procedures

- Assess

Evaluate current cybersecurity risks and vulnerabilities

- Develop

Create comprehensive cybersecurity policies and protocols.

- Train

Provide employees with an education on security practices.

- Implement

Enforce policies across all levels of the organization.

- Monitor

Regularly check compliance with cybersecurity measures.

- Update

Revise policies as threats and technology evolve

- Test

Conduct exercises to assess response to incidents

- Review

Continuously evaluate the effectiveness of policies.

Reporting Phishing Attempts: Best Practices

- Verify Sender

Always check the email address and its domain for legitimacy.

- Do Not Click

Avoid clicking on any links or downloading attachments in suspicious emails.

- Report Immediately

Notify your IT department or designated personnel as soon as possible.

- Provide Details

Include all relevant information such as eamil headers and content

- Educate Others

Inform co-workers or team members about the phishing attempt you received.

- Secure Devices

Ensure your devices have updated anti-virus and security software in place.

- Follow Protocol

Adhere to organization's specific procedures for reporting phishing incidents.

Future Trends in Phishing Attacks and Defense

- AI techniques

Utilizing AI for detecting and analyzing phishing patterns effectively.

- Multi-Factor Authentication

Implement multi-factor authentication to mitigate unauthorized access risks.

- Email Filtering

Adopt advanced email filtering systems to block phishing attempts automatically.

- User Training

Conduct regular training sessions to aware users about phishing tactics

- Incident Response Plans

Establish clear incident response protocols for phishing incidents.

- Threat Intelligence Sharing

Engage in threat Intelligence sharing to stay updated on phishing trends.

- Regular Software Updates

Ensure all software is kept up to date to fix known vulnerabilities.

THANK YOU

- Contact Number

0757657334

- Email Address

jacklinemugeha@gmail.com