By Zakaria TOUYEB

PHISHING AWARENESS TRAINING: RECOGNIZING AND AVOIDING PHISHING ATTACKS

Educating on recognizing and avoiding phishing threats

INTRODUCTION TO PHISHING

Understanding Common Phishing Attack Vectors

- **Definition of phishing**

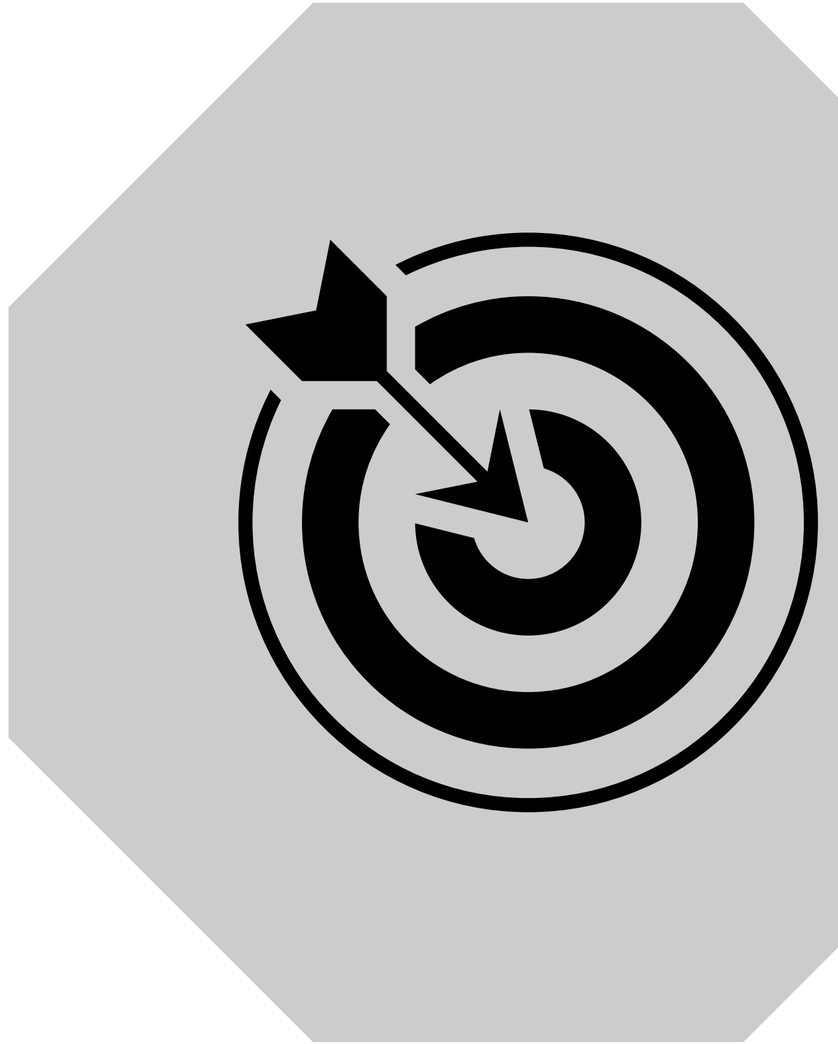
  Phishing is a cybercrime where attackers deceive individuals into providing sensitive information via fraudulent communications.

- **Historical background**

  Phishing has evolved since the 1990s, adapting to technological advancements and user behaviors.

- **Importance of phishing awareness in the digital age**

  Awareness is crucial to prevent falling victim to phishing, which can lead to identity theft and financial loss.



TYPES OF PHISHING ATTACKS

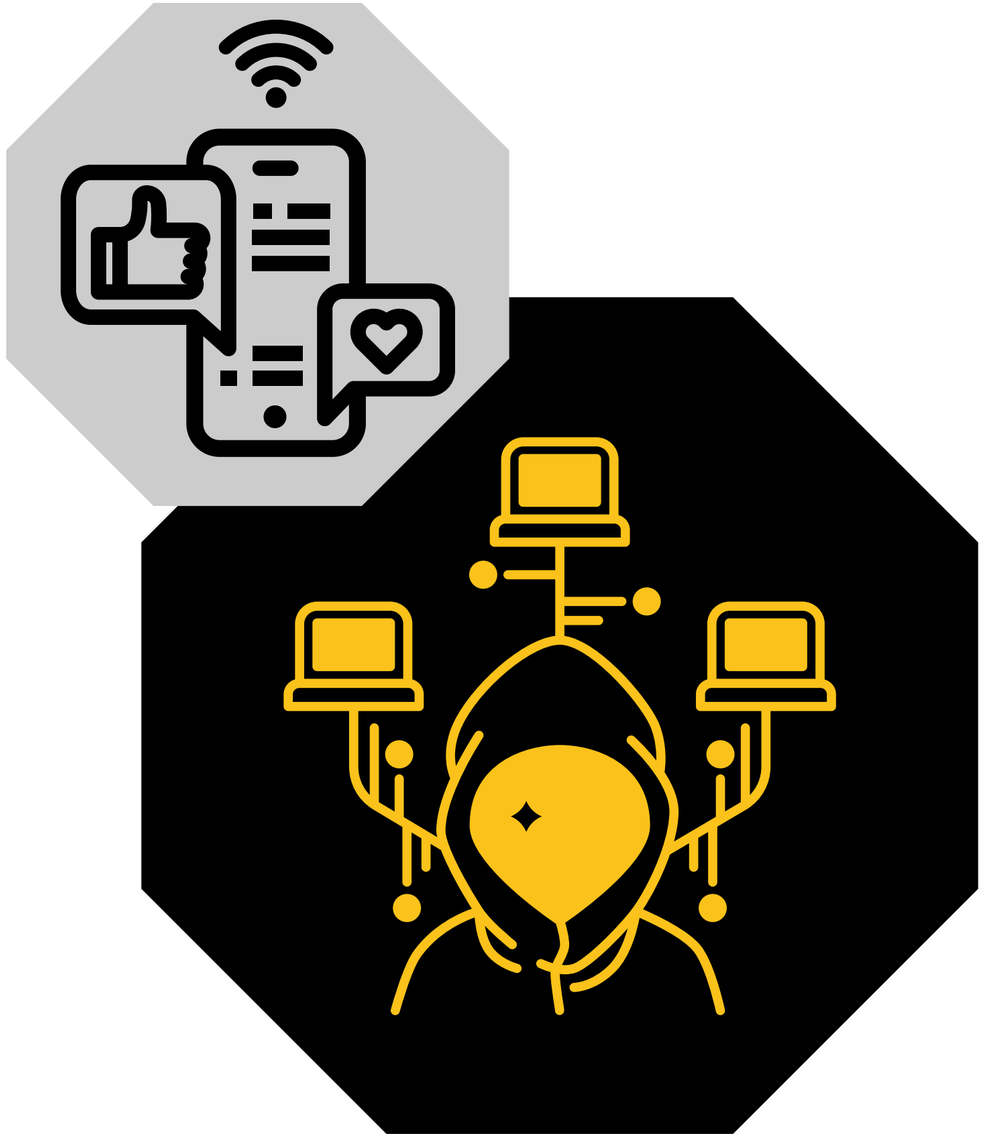
Email Phishing
Impersonates organizations to elicit personal information.

Spear Phishing
Targeted attacks using personal information to craft convincing messages.

Smishing
Phishing via SMS messages.

Whaling
Targets high-ranking officials with tailored messages.

Vishing
Phishing via voice calls.



SOCIAL ENGINEERING TACTICS

Understanding various tactics used in phishing attacks to enhance awareness.

PHISHING STATISTICS AND TRENDS

Daily Phishing Emails

3.4 billion phishing emails are sent eacn day, indicating a widespread threat.

Sophisticated Tactics

Sophistica.ted Tactics Phishing tactics are becoming increasingly sophisticated, necessitating advanced awareness strategies.

Business Impact

83% of UK businesses reported phishing as a primary attack vector in 2022,stressing the need fortraining.

Data Breaches

30% of all data breaches involve phishing, showing its significant rote in cybersecurity incidents.

Al-Driven Phishing

Al-Driven Phishing There is a rise in Al-driven phishing attacks, complicating detection and prevention efforts.

PREVENTION STRATEGIES

1

Enable Multi-Factor Authentication (MFA)

MFA adds an extra layer of security, making it harder for attackers to gain unauthorized access.

2

Regularly update software

Keeping software up to date closes security loopholes that could be exploited by phishing attempts.

3

Conduct employee training on phishing awareness

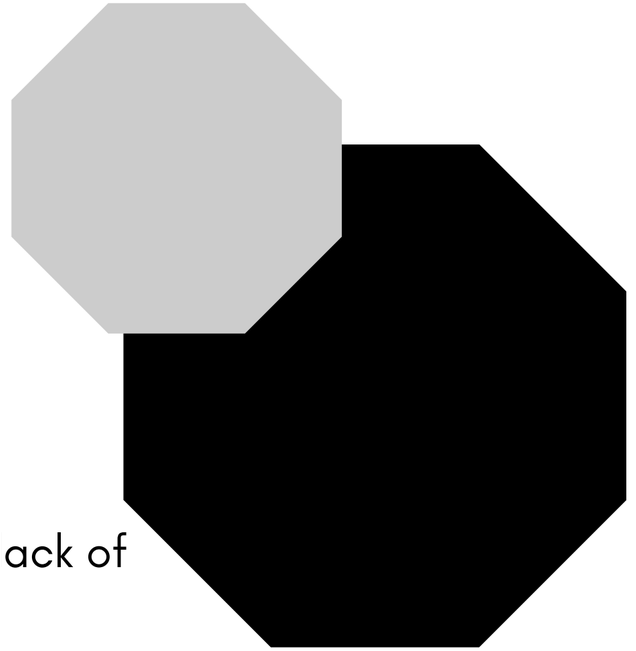
Training equips employees with the knowledge to identify and avoid phishing threats effectively.

4

Prioritize email authentication protocols (SPF, DKIM, DMARC)

mplementing these protocols helps verify the legitimacy of emails and reduces phishing risks.

RECOGNIZING PHISHING EMAILS



1. **Suspicious sender addresses**
   Impersonates organizations to elicit personal information.

2. **Generic greetings**
   Phishing emails often use vague greetings instead of personal names, signaling a lack of authenticity.

3. **Urgent or threatening language**
   Be wary of emails that create a false sense of urgency or demand immediate action to trick you.

4. **Unexpected attachments or links**
   Avoid clicking on unexpected attachments or links, asthey may contain malware or lead to fraudulent sites.

5. **Poor grammar and spelling**
   Many ohishing emails contain errors in grammar and spelling, indicating a lack of professionalism and authenticity.

THANK YOU FOR YOUR ATTENTION!

STAY SECURE, STAY VIGILANT.