

WELCOME TO PHISHING AWARENESS  
TRAINING

# GUARDING AGAINST PHISHING ATTACKS

---

TASK2: Atitallah Sirine



Code Alpha

# OBJECTIVES

## Phishing Awareness Training: Strengthening Your Cybersecurity Shield

1

Define phishing and identify common methods used by scammers

2

Recognize red flags in phishing emails, messages, or posts

3

Develop critical thinking skills to discern legitimate requests from potential phishing attempts

 **01** WHAT IS PHISHING?


 **02** TYPES OF PHISHING

 **03** RECOGNIZING PHISHING  
EMAILS

 **04** AVOIDING PHISHING  
WEBSITES

 **05** SOCIAL ENGINEERING  
TACTICS

 **06** PROTECT YOURSELF FROM  
PHISHING

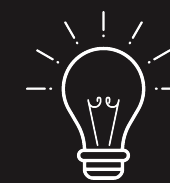
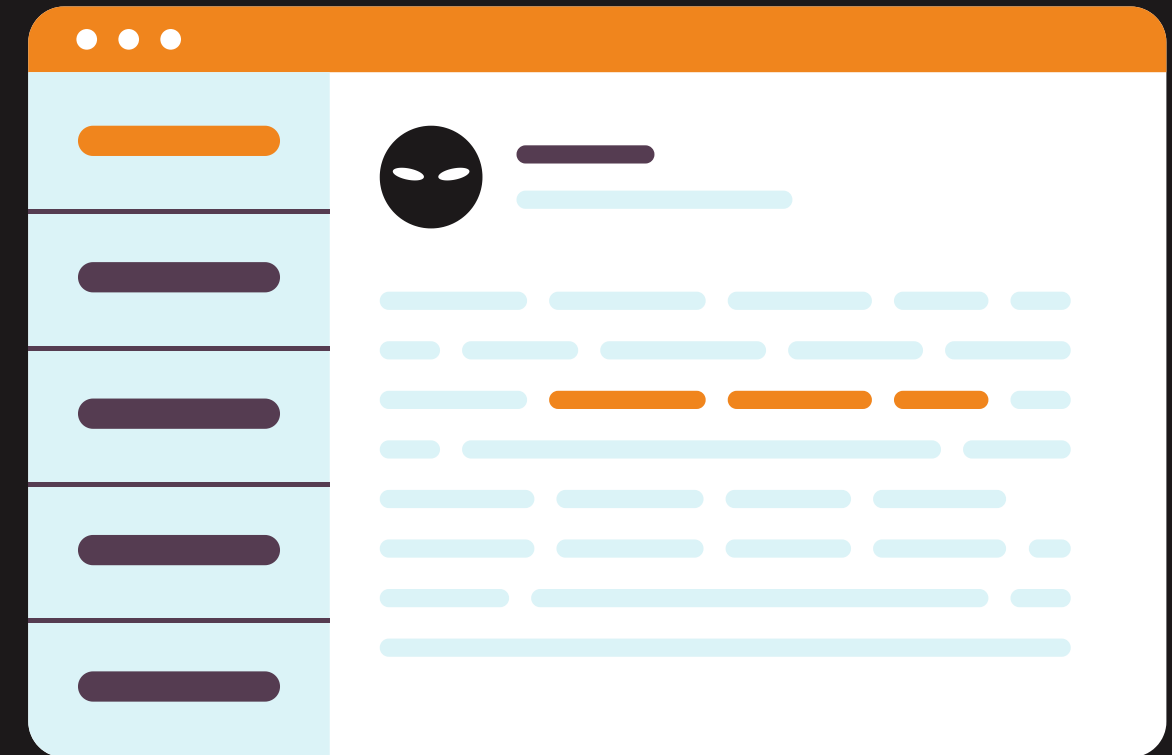
 **07** TWO-FACTOR  
AUTHENTICATION (2FA)

 **08** CASE STUDIES

 **09** PREVENTION TIPS

# WHAT IS PHISHING?

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.



*Think of an email or message you received that asked for personal information. What made it suspicious?*

# TYPES OF PHISHING

Phishing attacks come in different forms



## EMAIL PHISHING

Deceptive attempts via email to trick individuals into revealing sensitive information.



## SMS PHISHING

Phishing attacks through SMS (text messages), typically containing deceptive content or links.



## WEBSITE PHISHING:

Creating fake websites to impersonate legitimate ones, aiming to steal user credentials or sensitive data.



# RECOGNIZING PHISHING EMAILS

## 01

### BEHAVIOR-BASED ANALYSIS

Security systems can establish a baseline of normal user activities by continuously monitoring user behavior, such as browsing patterns, mouse movements, and keystrokes.

## 03

### URL AND DOMAIN REPUTATION ANALYSIS

By scrutinizing URLs in real time, security systems can thwart phishing attacks before users unknowingly interact with dangerous websites.

## 02

### MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

Through continuous learning, ML-powered systems improve their accuracy in detecting real-time phishing attacks while reducing false positives, ensuring more effective protection against evolving threats.

## 04

### EMAIL AND CONTENT ANALYSIS

By examining emails in real-time, security systems can promptly flag suspicious messages and prevent users from falling victim to phishing attempts. Additionally, analyzing attachments and embedded links allows systems to identify malicious files or redirect attempts, safeguarding users from potential malware infections.

# AVOIDING PHISHING WEBSITES

Phishing websites mimic legitimate ones to trick users into divulging sensitive information. To avoid falling victim:



- 1 Check the website's URL
- 2 Look for HTTPS
- 3 Verify website legitimacy
- 4 Use website safety tools/browser extensions



# SOCIAL ENGINEERING TACTICS

- 1 Manipulation techniques
- 2 Building trust
- 3 Impersonation of trusted entities
- 4 Emotional manipulation





**THINK BEFORE YOU CLICK!**

# **PROTECT YOURSELF FROM PHISHING**

- Never share sensitive information via email
- Use secure websites for transactions
- Verify requests for personal or financial information

# TWO-FACTOR AUTHENTICA TION (2FA)



*Two-Factor Authentication (2FA) adds an extra layer of security beyond just a password.*

## ADVANTAGES OF 2FA:

- Enhances security by requiring multiple forms of identification.
- Mitigates the risks associated with password-only authentication.
- Adds an extra layer of protection against unauthorized access.

## IMPLEMENTING 2FA: EMPOWERING USERS WITH STRONGER AUTHENTICATION

# CASE STUDIES



*Explore a few instances where individuals or organizations fell victim to phishing attacks, emphasizing key takeaways:*

## EXAMPLES

- AOHell, the First Recorded Example. ...
- The Nordea Bank Incident. ...
- Operation Phish Phry. ...
- RSA. ...
- Dyre Phishing Scam. ...
- The Sony Pictures Leak. ...
- Facebook & Google. ...
- 2018 World Cup.

# PREVENTION TIPS

Phishing attacks can be mitigated with proactive measures. Here are key prevention tips:



- 1 Regularly update passwords
- 2 Be cautious with email attachments
- 3 Verify unexpected emails with the sender
- 4 Stay informed about the latest phishing tactics

# THANKS FOR YOUR ATTENTION!

Thank you for participating in our Phishing Awareness Training. By enhancing your understanding of phishing attacks, recognizing red flags, and adopting preventive measures, you are now better equipped to safeguard against cyber threats.

Stay Vigilant, Stay Secure!