# PHISHING ATTACKS AND TESTING

**Think Before You Click!**

**BY:**

**ANIS LOUAIL**
**ISSAM HAMANI**

# OBJECTIVES

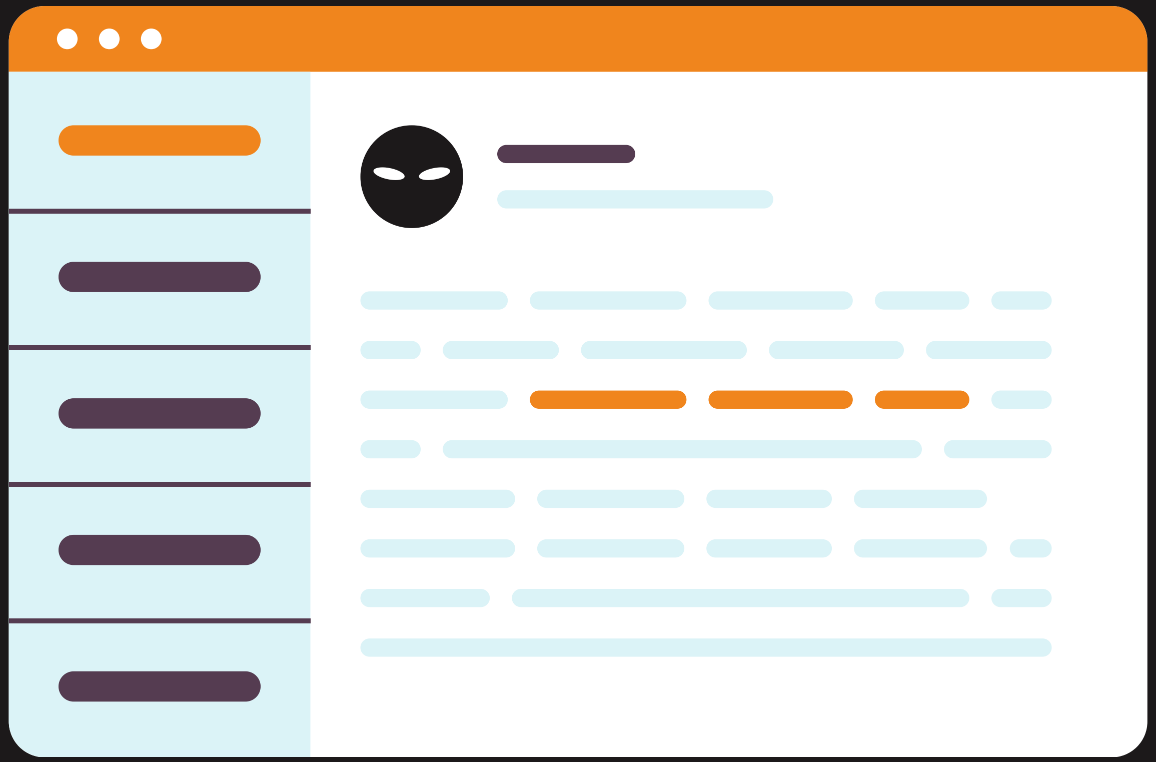
**By the end of this lesson, we will be able to:**

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
4. Simple simulation of Credential Harvesting (KALI LINUX)

# WHAT IS PHISHING?

Phishing is when someone tries to trick you into revealing personal information like your password, credit card numbers, or social security number.

Phishing can happen through emails, text messages, or other online platforms.



*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

Scammers send fake emails pretending to be a trustworthy organization

## SMS PHISHING

Scammers send text messages with fake links or requests for personal information

## SOCIAL MEDIA PHISHING

Scammers create fake profiles or posts to trick you into clicking on links or sharing personal informaion

## VISHING

scammers impersonate trusted entities, such as tech support, to extract personal information or gain remote access to the victim's device.

## CREDENTIAL GATHERING

Attackers use fake login pages  to trick users into entering their usernames and passwords.

## WATERING HOLE

Attackers compromise websites that are frequently visited by their intended targets.

# RED FLAGS

Red flags in phishing attempts are warning signs or indicators that help individuals identify potential scams. Some common red flags in phishing include:

1. Urgent or threatening language
2. Suspicious sender information
3. Requests for personal information
4. Misspellings or grammatical errors
5. Suspicious links or attachments
6. Generic greetings
7. Too good to be true

## 01 URGENT OR THREATENING LANGUAGE

Phishing attempts often create a sense of urgency or use threatening language to prompt immediate action. Phases like "urgent action required," "account suspended," or "your account will be deleted" may indicate a phishing attempt.

## 02 SUSPICIOUS SENDER INFORMATION

Check the sender's email address or social media profile. Phishing emails or messages often use generic or suspicious email addresses that do not match the legitimate entity they claim to represent.

## 03 REQUESTS FOR PERSONAL INFORMATION

Legitimate organizations do not request personal information, such as usernames, passwords, or credit card numbers, via email, social media, or other online means. Be cautious of any request for personal information.

## 04 MISSPELLINGS OR GRAMMATICAL ERRORS

Phishing emails or messages may contain misspellings, grammatical errors, or awkward phrasing. Legitimate organizations usually have professional communications and do not contain obvious errors.

## 05 SUSPICIOUS LINKS OR ATTACHMENTS

Be cautious of links or attachments in emails or messages from unknown or untrusted sources. Hover over links to check their actual destinations, and do not click on suspicious links or download attachments that you were not expecting.

## 06 GENERIC GREETINGS

Phishing emails will often use generic greetings they might say something like "Dear Valued Customer," instead of addressing you by your name. Legitimate organizations often personalize their communications with your name or other Related information.

## 07 TOO GOOD TO BE TRUE

Phishing attempts may lure individuals with enticing offers, such as winning a prize or getting a huge discount. If an offer seems too good to be true, it may be a phishing attempt.

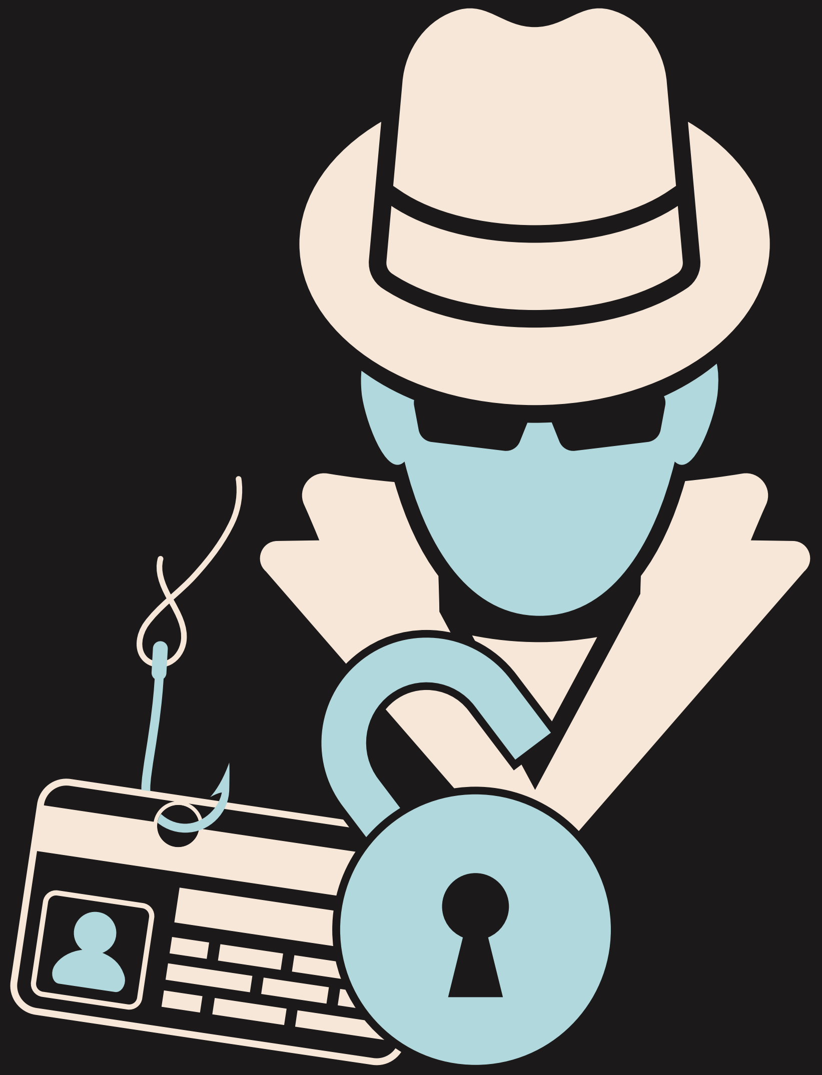
*Which of the seven red flags do you think is the hardest to detect? What makes you say that?*

- # PHISHING TESTING

## How Phishing Testing Fortifies Organizations

- also known as phishing simulation or phishing awareness testing, is a proactive cybersecurity measure used to assess an organization's vulnerability to phishing attacks and educate its employees about the risks associated with such attacks.

- The process of phishing testing involves creating convincing, phishing emails and sending them to employees within the organization. These simulated emails closely resemble real phishing attempts, often employing tactics like urgency, fear, or curiosity to prompt action.



# REPORT PHISHING ATTEMPTS

If you suspect a phishing attempt, You have sereval way to report the phishing attempts

- Forward the phishing email to The Anti-Phishing Working Group (APWG)
- Report the phishing attempt to the company that is being impersonated
- Report the phishing attempt to your email provider.

# IMPACT OF THE ATTACK

- The security of our nation's agencies is under threat.
- Impersonating Major Bank Leads to Unauthorized Transactions.
- Educational institutions have experienced a recent phishing attack, compromising student data.
- The healthcare sector is currently dealing with a data breach that occurred after a successful phishing attack.

# Real-World Examples

- ## UFAS 1 Phising (2023)

During the summer of 2023, an individual posing as an army general and made contact with a university administration, claiming to be a general. The fraudulent request was made in an attempt to obtain information from official university pages.

- ## COVID-19 Related Phishing (2020)

As the COVID-19 pandemic spread, phishing attacks surged. Scammers sent emails posing as health organizations, government agencies, and charities, exploiting fear and uncertainty to steal personal and financial information.

- ## Google and Facebook Impersonation (2017):

A Lithuanian hacker scammed both Google and Facebook into wiring over $100 million by impersonating a legitimate Asian hardware vendor in phishing emails.

# THINK CRITICALLY

Be skeptical of emails, messages, or posts that seem too good to be true or too urgent. Remember, if it sounds too good to be true, it probably is!

Think before clicking on any links, sharing personal information online, or opening any suspicious attachments. Ask yourself if it seems legitimate and if you were expecting it.

Verify the authenticity of the sender and the information provided before taking any action. Trust your instincts and be cautious when sharing information online.

Think before you click!

# PROTECT YOURSELF FROM PHISHING

*Don't share your personal information online!*