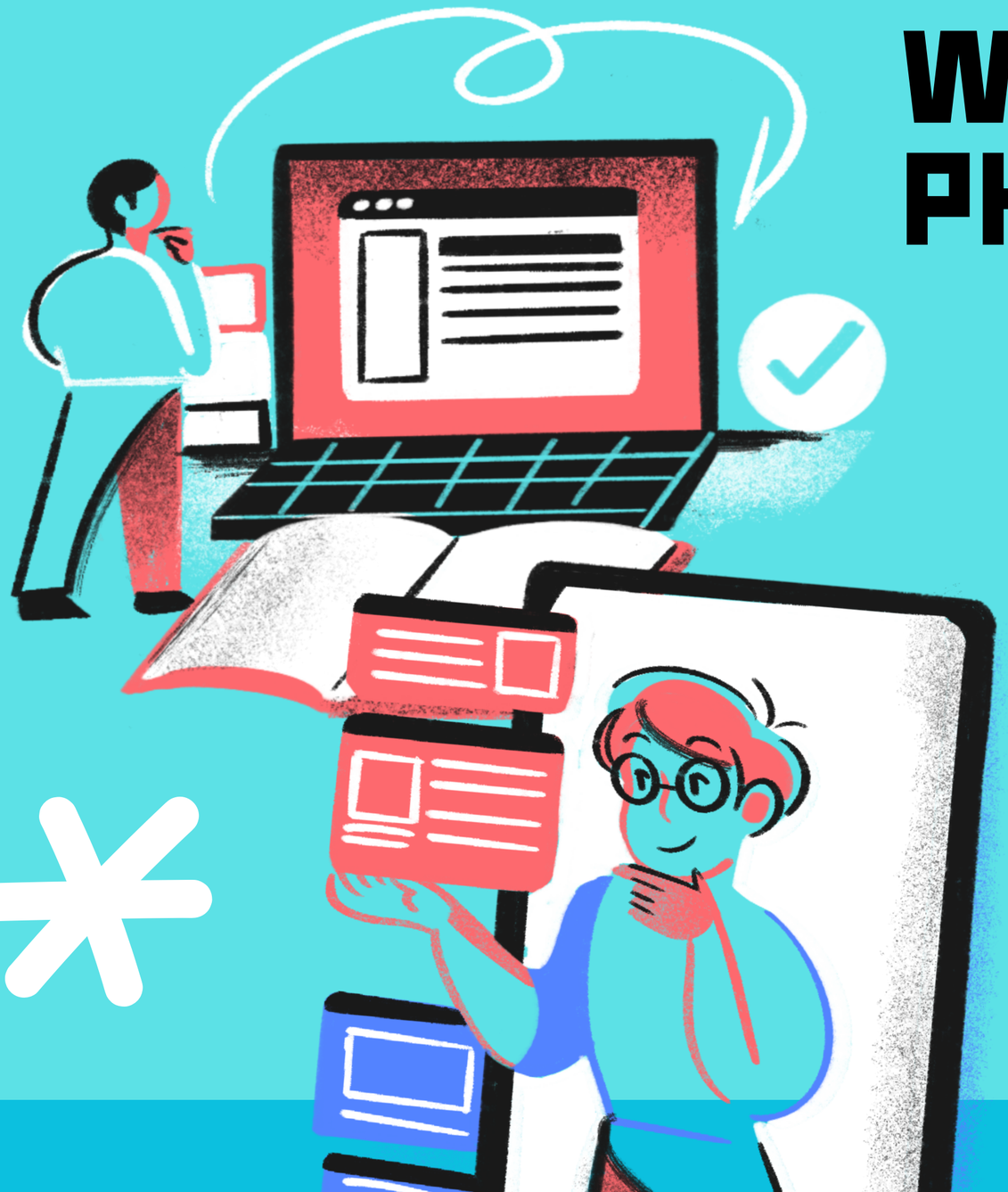
@tayssir_riahi

PHISHING ATTACKS.. DEFINITION & HOW TO AVOID THEM?



WHAT IS A PHISHING ATTACK ?

A phishing attack is a type of cyber attack where an attacker attempts to trick individuals into providing sensitive information, such as usernames, passwords, credit card numbers, or other personal details.

This is typically done by sending fraudulent messages(an email for example) that appear to come from a legitimate source, such as a bank, social media site, or trusted company.

These messages often contain a link to a fake website that looks real, where the victim is prompted to enter their information, which is then captured by the attacker.

HOW IT WORKS ?

1-Planning and Research:

The attacker identifies their target and gathers information. This might include names, email addresses, and any other details that can make the attack more convincing.

2-Creating a Deceptive Message:

The attacker creates a fraudulent email, text message, or social media message.

This message is designed to look like it comes from a legitimate source, such as a bank, online store, or a colleague.

It usually contains a sense of urgency or an enticing offer to prompt the target to take immediate action.

3-Creating a Fake Website:

The attacker sets up a fake website that looks almost identical to the legitimate website of the trusted entity. This site is designed to capture the target's sensitive information when they enter it.

4-Distributing the Message:

The deceptive message is sent to the target via email, SMS, or social media. The message contains a link to the fake website or an attachment that, when opened, may install malware.

5-Capturing Sensitive Information:

If the target is deceived, they click the link and enter their sensitive information on the fake website. This information is then collected by the attacker.

6-Exploiting the Information:

The attacker uses the captured information for malicious purposes, such as stealing money, committing identity theft, or gaining unauthorized access to accounts.

@tayssir_riahi

HOW TO RECOGNIZE AND AVOID PHISHING ATTACKS:

Be Skeptical of Unsolicited Messages:

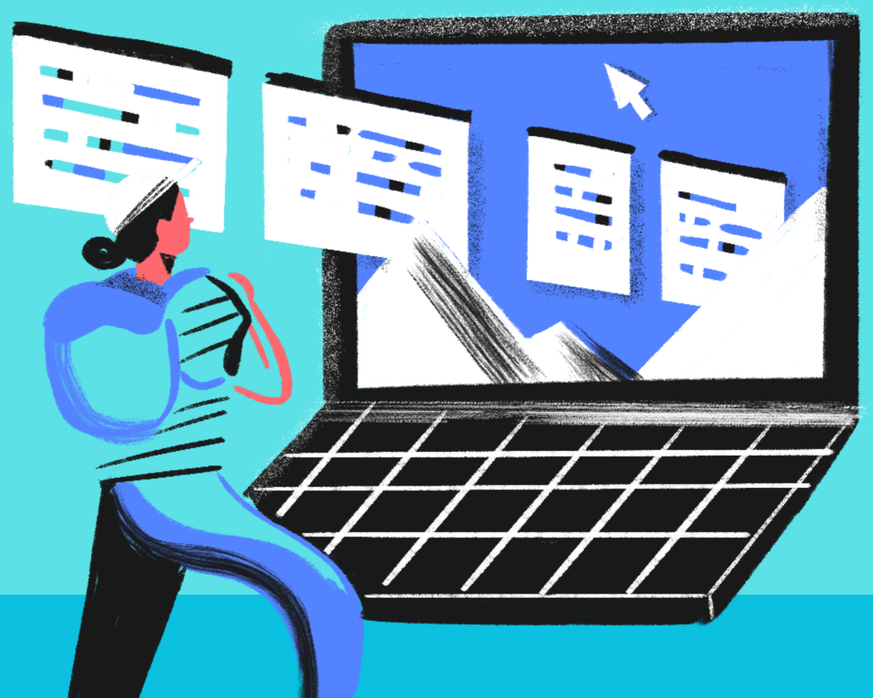
Be wary of unexpected messages, especially those that ask for sensitive information or prompt you to take immediate action.

Look for Red Flags:

Be cautious of messages that contain grammatical errors, urgent requests, or offers that seem too good to be true.
Hover over links to see the actual URL before clicking. Ensure it matches the legitimate website.

Verify the Source:

Check the sender's email address or phone number carefully. Look for subtle misspellings or discrepancies.
Contact the supposed sender directly using a trusted method (e.g., call the bank using the number on the back of your card).

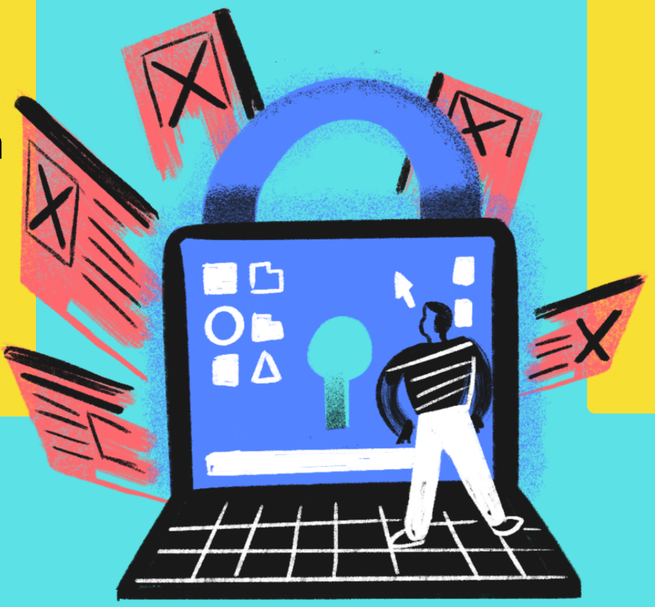


Use Security Software:

Keep your antivirus and anti-malware software up to date.
Use email filtering tools to help detect and block phishing attempts.

Enable Multi-Factor Authentication (MFA):

Use MFA on your accounts to add an extra layer of security. Even if your password is compromised, MFA can prevent unauthorized access.



Educate Yourself and Others:

Stay informed about the latest phishing tactics and educate yourself and others on how to recognize and avoid them.

IN A NUTSHELL :

Phishing attacks are a common and dangerous form of cyber attack. By understanding how these attacks are conducted and taking proactive steps to recognize and prevent them, individuals and organizations can significantly reduce their risk of falling victim to phishing.

THANKS FOR YOUR ATTENTION :)