

# Phishing Attacks

Presentation Slides

Training Kit



Middle School



**CyberEco**

معا لدعم السلامة الرقمية  
Together to support digital safety



الوكالة الوطنية للأمن السيبراني  
National Cyber Security Agency

# Intellectual Property rights

The National Agency for Cyber Security in the State of Qatar owns the work, and copyright, publishing, printing rights, and all other intellectual property rights are protected by the National Agency for Cyber Security in the State of Qatar.

As a result, the Agency retains all rights to these materials, and it is prohibited to republish, quote, copy, or transfer them in whole or in part in any form or by any means whether electronic or mechanical, including photographic reproduction, recording, or the use of any information storage and retrieval system, whether existing or invented in the future, unless the agency has given written permission.

**Anyone who breaks this could face legal consequences.**

**December, 2023**

**Doha, Qatar**

This content is produced by the team of

**National Cybersecurity Excellence Management, National Cyber Security Agency.**

For inquiries about the initiative or program, you can contact us through the following websites or phone numbers:



الوكالة الوطنية للأمن السيبراني  
National Cyber Security Agency

🌐 <https://www.ncsa.gov.qa/>

✉ [cyberexcellence@ncsa.gov.qa](mailto:cyberexcellence@ncsa.gov.qa)

☎ 00974 404 663 78

☎ 00974 404 663 62

# Time Table for the Lecture

Content	Allocated Time
General introduction	5 minutes
The theoretical aspect	25 minutes
Educational Videos	25 minutes
Short break	20 minutes
Training games	25 minutes
Dialogue and discussion with students	15 minutes
Graduation project	5 minutes
Total training time	2 hours

# Scientific Content Index

## Chapter One:

### The concept of phishing and its types.....19

First: The concept of phishing.....20

Second: Types and forms of phishing.....24

## Chapter Two:

### How to carry out phishing attacks.....35

First: The gaps that perpetrators of phishing attacks exploit.....36

Second: Mistakes committed by Internet users.....38

Third: Digital fingerprint and phishing.....40

## Chapter Three:

### How to act if exposed to phishing.....45

First: Instructions for protection against phishing.....46

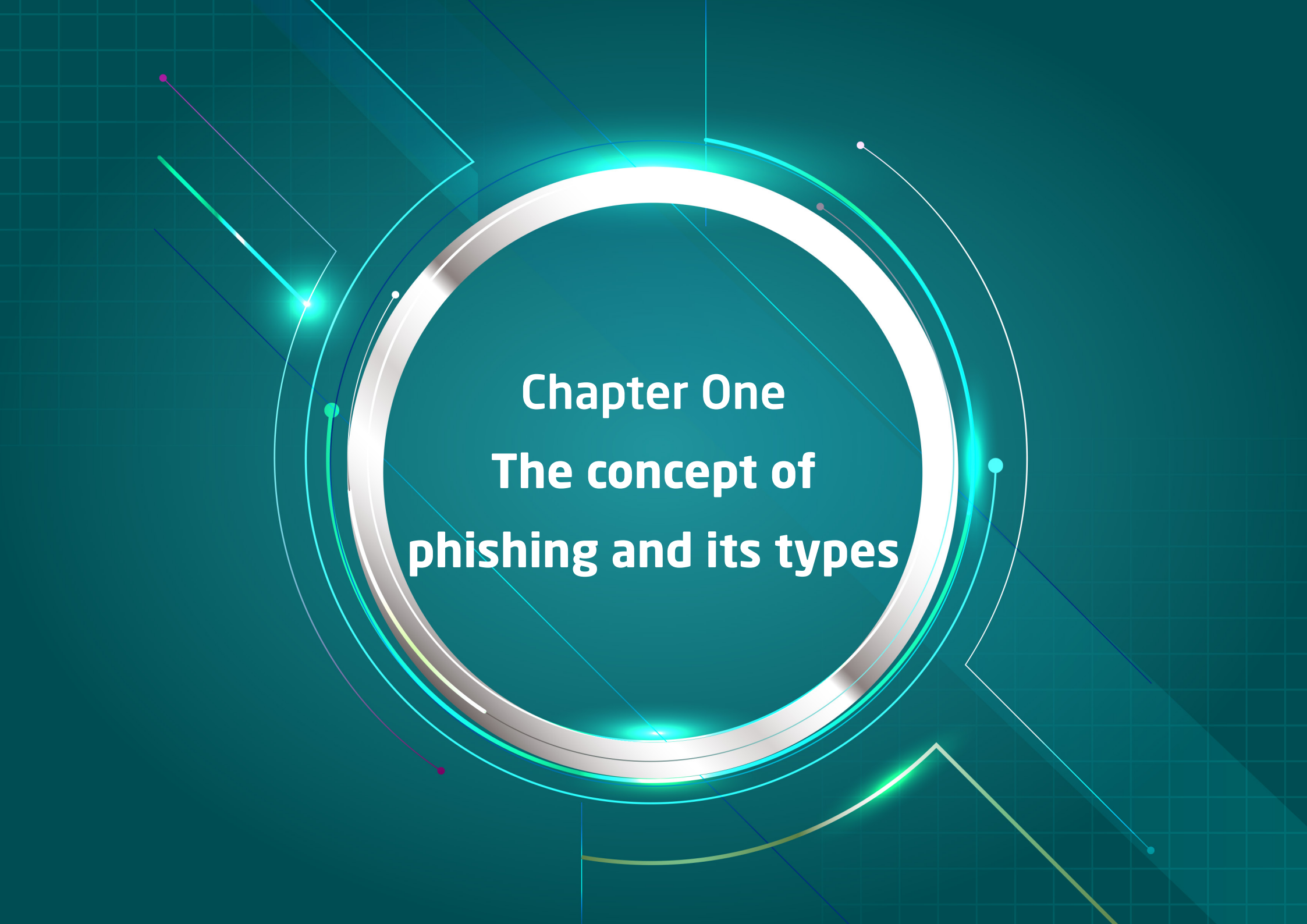
Second: Protecting data from hacking.....47

Third: The authorities I turn to when I am exposed to phishing.....48

## Student exercises and trainings

## References





**Chapter One**  
**The concept of**  
**phishing and its types**

# First the concept of phishing :

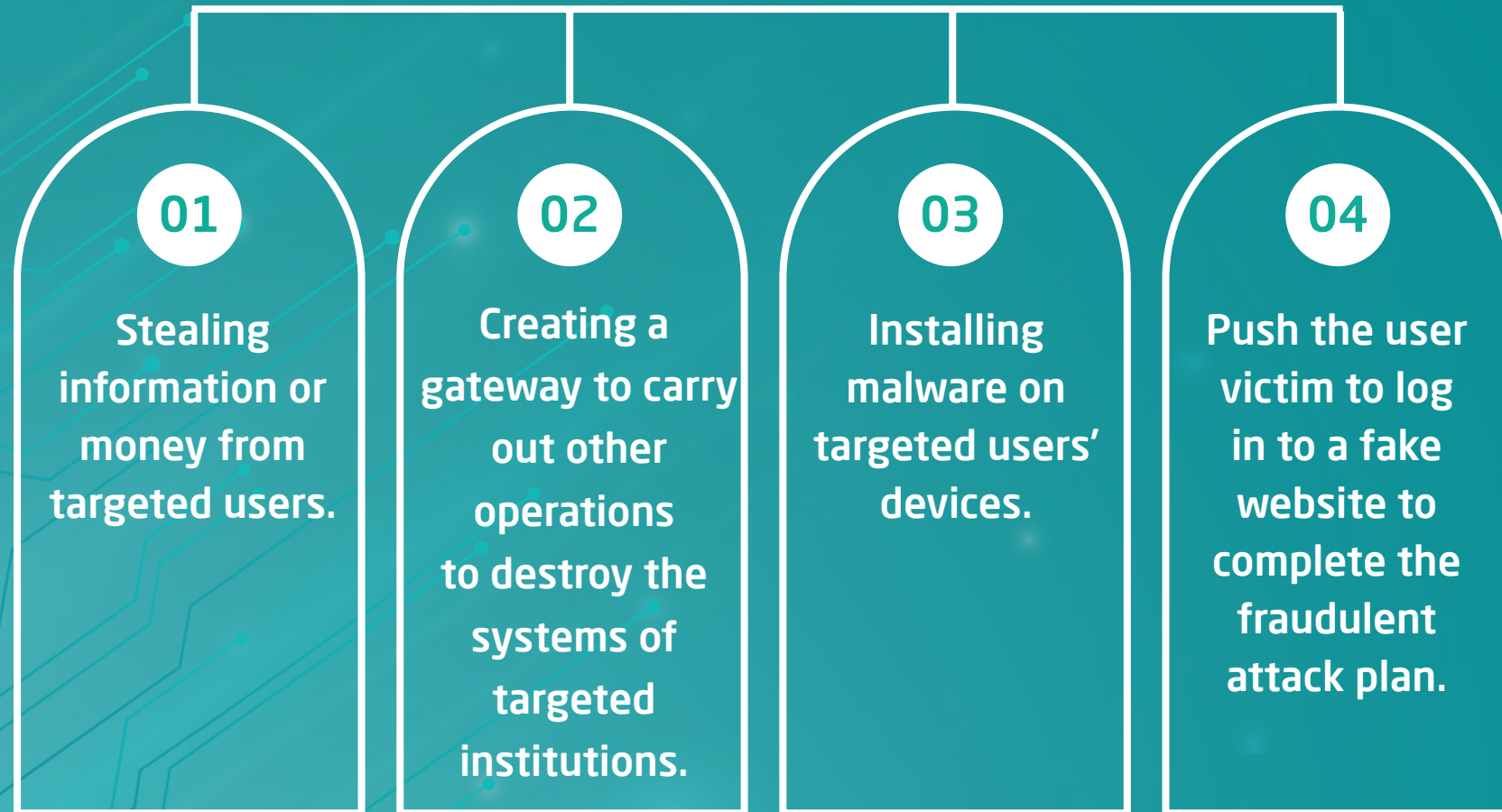


# the concept of phishing

Phishing means that digital attackers masquerade as a known entity such as Amazon or a reputable person and send an email or other form of communication. Attackers usually use phishing emails to distribute malicious links or attachments. Through which the attacker obtains sensitive data of interest to the victim, such as login credentials, bank account numbers, family or work personal information, and soon .



## The aim of phishing attacks is the following points:





# Types of phishing





# 1- Spear phishing

Spear phishing means targeting an individual within a specific institution to steal his login credentials; the cyber attacker collects personal information about the targeted individual before the fraud begins, such as his name, position, and contact details.

Cyber attackers carry out spear phishing; For the purpose of identity theft, financial fraud, manipulation of stock prices, spaying, or theft of confidential data in order to resell it to those interested in it, often competitors.

Individuals targeted by this type of phishing include executive managers in organizations who may open unsafe email messages. Which allows criminals to penetrate the institution's public system through the officials' device.



## 2- Vishing

It is a type of phishing attack that is carried out via phone calls or voice mail, with the aim of obtaining the victims' money or other personal information.

The reason behind the spread of these cyber attacks is what is known as "social engineering," which is a modern technology that relies on natural human instincts such as trust or fear and other feelings that cyber attackers exploit to influence the victims to push them to make a specific decision that leads to achieving the attacker's goal, like theft money or sensitive information.

The cyber attacker often pretends to be an individual the victim knows or an official in an institution with which the victim has dealt, such as the tax authority, insurance companies, or banks, to begin luring him to obtain important information from him to implement the rest of the fraud plan.



### 3- Email phishing

In this type of phishing operation, the cyber attacker relies on email to carry out his attack on the victim. It sends an e-mail message that appears to be from a trusted source. With the aim of hacking the device to steal sensitive data, steal money, or steal identity and later exploit it in other crimes such as a ransomware attack.



# There are several signs to distinguish phishing emails:

## Writing style

The message carries the name of a person close to the victim; it is unlikely that it will be spoken in an official manner. Here, if the message is in this style, the possibility of it being a fraudulent message increases

## Grammatical and spelling mistakes

If the message claims to be from a well-known institution, such as Google, most major institutions have the feature of checking the spelling and grammar of their email messages, which distinguishes their messages from others.

## Inconsistency in email addresses and links

Searching for inconsistencies in email addresses and links is one way to detect fraudulent messages. For example, the user must match the email address received from a large institution such as Google with the original address announced on its official website.

# علامات تمييز الرسائل البريدية التصيدية

## Insistence and arousing feelings of fear

Cyber attackers often resort to manipulating victims' feelings by inciting fear and anxiety in them regarding their banking transactions or personal information and begin requesting sensitive data from them.

## Suspicious attachments

If you receive an email that includes attachments from unknown sources, you must be careful before clicking on them, and search for the source in search engines to confirm its existence.

## Request to download programs and links

If the email claims to be from a well-known authority and requests that certain programs or links be installed on devices, you must be alert. Most likely they are fraudulent messages.



# علامات تمييز الرسائل البريدية التصيدية

## Prizes messages

In most fraudulent operations, the victim receives an email that prompts him to respond in order to receive large financial prizes or in-kind gifts, and has a specific time that he must follow, even though he has not participated in any competition before. Which means that this type of message is fraudulent.

## Fake web pages

The attacker may create a fake page and then direct a link from it to the victims in order to appear official and trustworthy, in order to push them to take an action, such as: visiting the page and registering on it, or clicking on its link to fall into the trap.

## Targeting employees in institutions

Employees in institutions may receive phishing emails with the aim of harming the institution or entering its system, manipulating, stealing customer data, exploiting it, or selling it to third parties. Therefore, employees must be made aware of the importance of cybersecurity, and avoid clicking on unknown links or responding to messages from unfamiliar authorities.

## 4- HTTPS Phishing

An HTTPS phishing attack is carried out by sending an email to the target user containing a link to a fake website, with the aim of deceiving the victim into entering his or her private information. This type of fraudulent attack is described as low risk and high reward.





## 5- Phishing attack known as pharming

Pharming is a combination of the words “Phishing” and “farming”, and is an online fraud similar to phishing. Where a fake website is designed and then targeted users are redirected to it to steal confidential information.



## 6- Pop-up Phishing

It means that fraudulent messages appear to users while they are browsing the Internet.

Attackers infect original websites with malware, causing these pop-up messages to appear when they are visited.



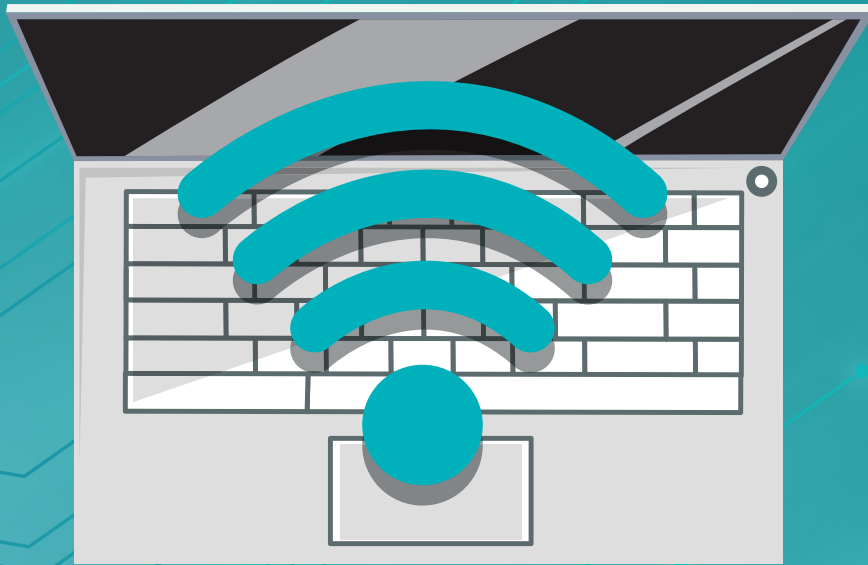
## Steps To avoid phishing attacks:

---

- It must be understood that the presence of an anti-virus software on your device means that fraudulent pop-up messages appear on some websites, and this does not mean that your computer is infected, but rather that the website you are visiting is infected with this malware.
- You should not give anyone remote access to your computer.
- If you doubt the reliability of the messages you see, you should contact the site owner or his support team directly .

## 7- Evil twin phishing

It is a cyber attack that deceives the targets into connecting to a fake Wi-Fi network that resembles the original one. Upon connection, the attacker begins to hack the victims' devices to steal all their data and files.



# The attacker uses several steps to carry out his cyber attack:

---

- Choose a public place with free Wi-Fi, such as airports, public libraries, or cafes, to launch the attack.
- Setting up a Wi-Fi access point. The attacker creates a new access point using a friendly name to make it easier for users to believe the network and start using it.
- Creating a fake captive portal page, the attacker places a portal on a public Wi-Fi network that asks users for passwords or personal information to access the network.
- Approaching the victims, after the attacker has completed the previous steps, he begins directing his devices near the potential victims to create a stronger signal, and thus they choose the fake network to use, which leads to them falling into the trap.
- Monitoring and stealing user data. After the targeted user enters the network, the attacker begins monitoring what he does online and collects data from important numbers and information.





## 8- Whaling

It is a phishing attack that targets senior executives in global institutions. It comes disguised as a familiar email message and is designed malware to motivate its victims to perform actions such as transferring money or sending personal data.

Financial institutions and payment services are the most targeted by this type of phishing attacks, as they contain personal information about the targeted institutions or influential individuals.



**1**

Paying victims to click on links to websites containing malware.

## Aim of whaling attacks

**3**

Requesting data related to institutions or individuals in order to launch further attacks, such as a ransomware attack.

**2**

Request to transfer funds to the cyber attacker's bank account.

# The damage resulting from whale attacks:

## 01 Data loss

Once you click on links or download email attachments, internal networks begin to become infected with malware that enables hackers to enter and steal whatever data they want.

## 02 Damage to the reputation of institutions and individuals

Data loss may result in significant financial losses to institutions and individuals, as well as damage to their reputation before the official authorities in the country that has enacted data protection legislation.

## 10- Deceptive Phishing

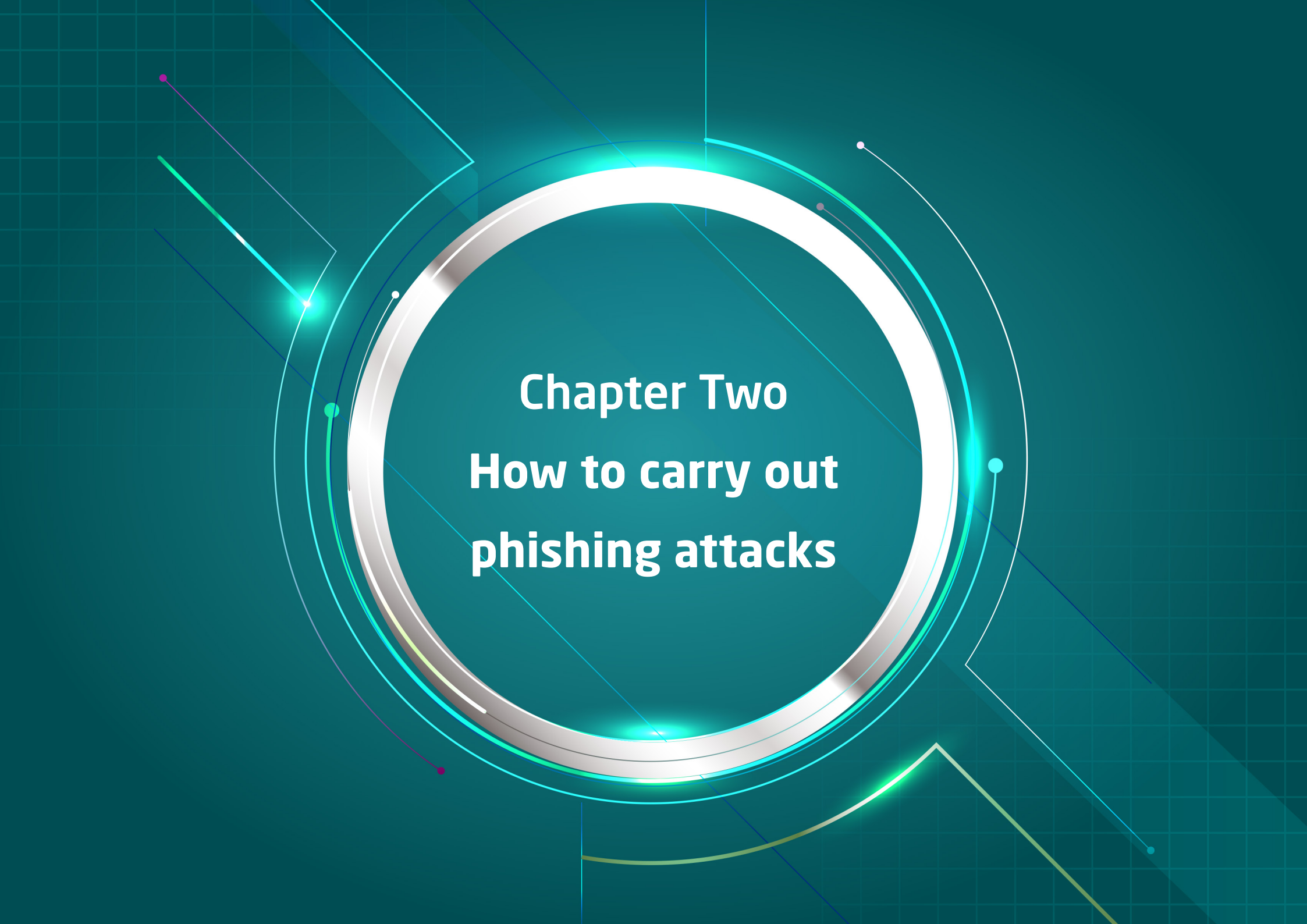


Cyber attackers use deceptive technology to pretend that they are working with a real company, such as Apple, to inform targeted users that they are actually being subjected to a cyber attack, to get them to click on a specific link, but in reality it is harmful, which causes their computers to be infected.

## 9- Clone Phishing



It means that a hacker makes an exact copy of a message that the target has already received. It may include something like “Resend this,” with a malware link in the email.



**Chapter Two**  
**How to carry out**  
**phishing attacks**



# Common methods that cyber attackers exploit to penetrate their target users' devices:



Sending fake text messages or emails containing links that contain malware programs



Fraud by claiming to provide technical support.



Users' failure to update programs and applications makes them an opening for attackers to in hacking personal devices.



Using weak passwords or they can be guessed on the user's devices and Wi-Fi network,



Clicking on unknown or untrusted links by users

# There are indicators that indicate the possibility of electronic devices being hacked:

---

- Receive email notifications about attempts to log in to your accounts even though you have not done so.
- The device is slow, its temperature increases, and there is a delay in executing the commands it receives from the user.
- The appearance of pop-up windows containing annoying messages claiming that your electronic device is infected with viruses.
- Opening browser windows, tabs and applications on the user's device on their own.
- Receive a warning communication from the workplace about the data hacking.
- Unsuccessful login attempts to your accounts.
- Friends and co-workers receiving unusual messages from the target user.
- Receive spam messages in your inbox.
- Constantly redirecting the target user to unwanted websites while trying to browse the Internet .



# Mistakes committed by Internet users

Browsing on public Wi-Fi without taking the required security precautions, which makes them more vulnerable to hacking and falling victim to phishing attacks.

**1**

The similarity of passwords for a number of online accounts

**2**

Not updating the browser and applications on the devices.

**3**

Use passwords that are easy to guess

**4**

Sharing personal information on social media.

**5**

Not installing program updates automatically, which increases the chances of viruses hacking the system.

**6**

# Mistakes committed by Internet users

Being carried away by e-mails that contain surveys, gift opportunities, or competitions, without verifying their authenticity by searching on engines such as Google for the name of the company,

**7**

**8**

Ignoring basic security features, including two-factor.

Ignoring basic security features, including two-factor

**9**

**10**

Shopping online from untrusted sites.

There are many tempting tests spread on social media - especially Facebook - once the user visits these pages, he becomes a prey to fraud and theft.

**11**

**12**

Do not take advantage of your privacy settings on social media.

The background is a solid teal color with a pattern of light blue circuit-like lines and dots on the left side, extending towards the center. The lines are thin and have small circular nodes at their ends, creating a sense of digital connectivity and flow.

# Digital fingerprinting and phishing

## Digital fingerprint (electronic)

It is the way of the data that the user leaves when using the Internet, such as the signs he visits, email messages, shopping processes and intercourse (the dedications) ... and all the movements made by those who are used to express the accounts of those who are different, good or not.

Internet sites may contribute to forming the user's digital fingerprint by installing "cookies" on his devices, and applications may also collect data about users without their knowledge if they allow them to access stored files, whether text, videos, images, etc.





## Passive digital fingerprint



means that the information that is collected about users without their knowledge, such as Internet sites collecting information about the number of visits and pages visited, the number of views on a video, and IP addresses, as well as advertising agencies benefiting from the likes, shares, and comments made by the user. Spontaneously in order to direct contents that suit his interests later.

## The active digital fingerprint



means that the user intentionally publishes his information and data publicly, as happens on social media, or enters websites on the Internet through identifying data such as (username and password), or completes an online data form, as happens when subscribing to news services or jobs. And others

# Importance of the digital fingerprint

It is permanent and it is difficult to control how others use it.

**1**

**2**

It determines the user's digital reputation as well as offline.

Employers and universities can verify the digital fingerprints of potential employees and students

**3**

**4**

Words, images and videos shared can be misinterpreted.

Harmful to social relationships between individuals.

**5**

**6**

Hackers can exploit the digital fingerprint in phishing operations or to create fake identities.

# طُرُق تشكيل البَصْمَة الرِّقْمِيَّة

1

Online shopping.

2

Registration for newsletters on electronic websites.

3

Financial transactions over the Internet.

4

Social media.

5

Joining websites.

6

Subscribe to newsletters.

7

Subscription to different applications

# Protection of fingerprint

Verifying our digital fingerprint through search engines.

**1**

Removing personal information from unimportant sites.

**2**

Controlling the amount of information that is shared via social media and other websites.

**3**

Adjust your privacy settings.

**4**

Verifying which websites are visited or whose links are received via email.

**5**

Do not use public Wi-Fi networks.

**6**



## Protection of fingerprint

Deleting old accounts.

**7**

**8**

Create strong and different passwords for accounts.

Do not log in to websites or applications using Facebook data.

**9**

**10**

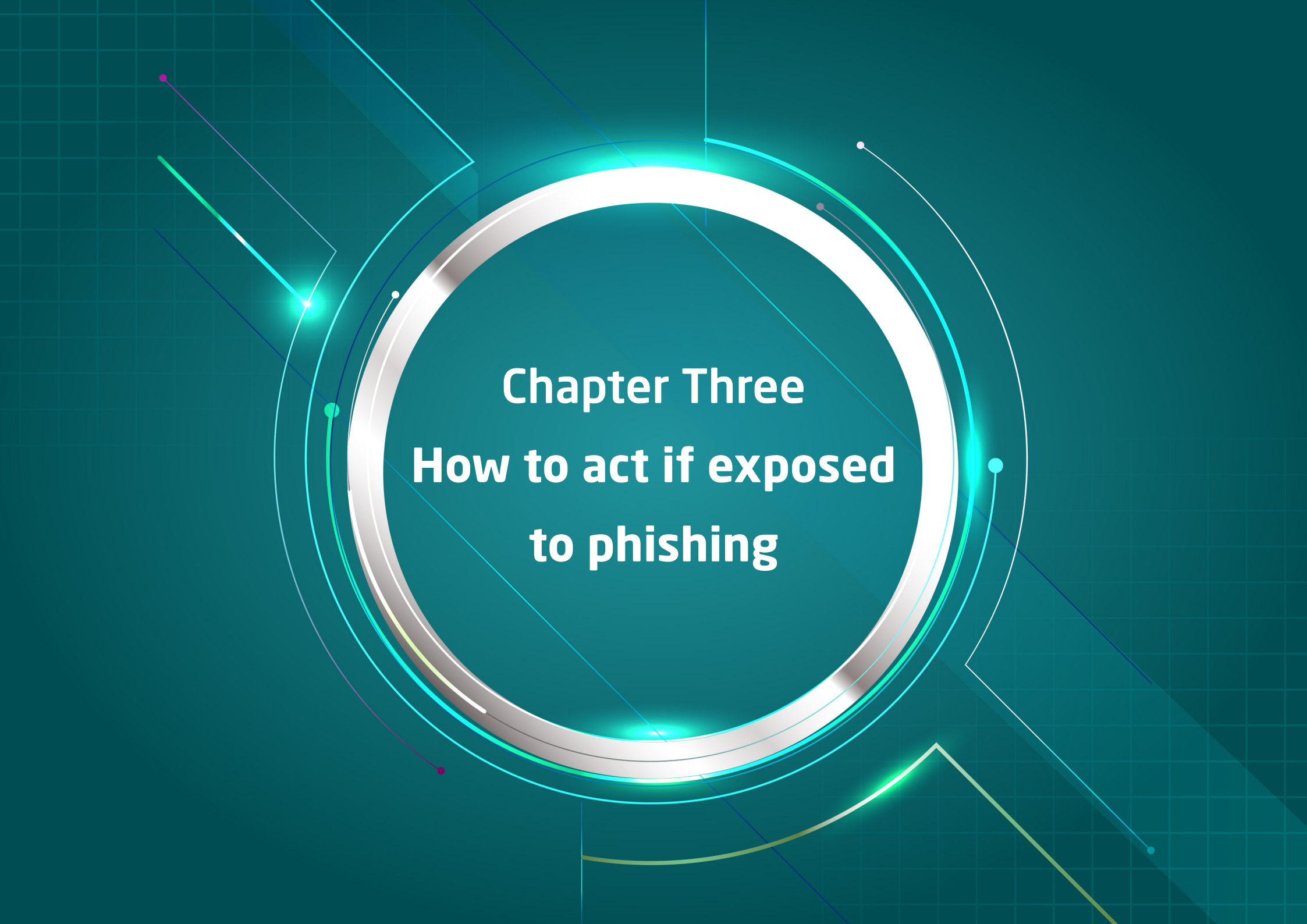
Updating programs and applications.

Set a password for the smartphone.

**11**

**12**

If you are hacked, you must change the passwords for all accounts immediately.



**Chapter Three**  
**How to act if exposed**  
**to phishing**

# How to act if exposed to phishing

01

You should avoid clicking on links or attachments sent in emails from unknown or unexpected sources.

02

If he receives repeated notifications about an attempt to log in to the user's accounts, he must change the password immediately in all accounts, provided that the word is strong and long.

## Signs that distinguish fraudulent e-mail messages are

**1**

The messages contain exaggerated kindness.

**3**

Many spelling and grammatical mistakes in mail messages.

**2**

Messages invite the user to click on a link to update their account details.



# How to protect yourself from phishing attacks?

Spam filtering process does not always help in getting rid of all fraudulent messages because attackers circumvented to access user. Protection methods include:

01

Use security software to protect computers, while setting automatic updates for programs and applications to be able to confront cyber threats.

02

Set a password for the smartphone, and set automatic software update on it.

03

Use two-factor authentication to provide additional security for accounts, whether by passwords, answering a question, or fingerprint and face.

04

Make an additional copy of the stored data, and place it somewhere other than the computer so that it can be restored if it is hacked (1).

# Protecting data from hacking

---

- Use anti-virus software, as it represents the first line of defence against fraudulent attacks.
- Activate two-factor authentication, as it is the best way to protect accounts from unauthorized access and data theft.
- Updating software and applications is necessary due to the introduction of permanent modifications to them by the technology companies that produce them to fill any security gaps that appear in them.
- A backup copy of the data must be placed in another place away from the personal device to protect it in the event that the device is hacked, lost, or damaged.

- Education of cybersecurity principles. This step contributes to protecting individuals from falling into the trap of phishing and other cyberattacks whose primary goal is to cause harm to Internet users.
- Avoid using public (free) Wi-Fi as much as possible on your personal device.
- Check mailed links before clicking on them.
- Turn off Bluetooth on the personal device if it is not needed.
- Reducing the digital fingerprint and activating privacy settings for social media.

# The authorities I turn to when I am exposed to phishing

01

If the user suspects that he has been exposed to a phishing attack, such as a fake email, then if he has dealings with the individuals or authorities listed in the messages, he must contact them personally via the approved numbers or official accounts.

02

If any attachment or link is opened in the fraudulent e-mail message, the user must contact the bank and stop his credit card if he suspects that it is at risk of being stolen.



# The authorities I turn to when I am exposed to phishing

03

If the user's computer is hacked, he must act quickly and disconnect from his Wi-Fi network, while activating anti-virus software to search for malware and delete questionable applications.

04

In this case, the user should update its operating systems, reset all passwords, activate two-factor authentication, scan the device, and start the installation again.

# The authorities I turn to when I am exposed to phishing

05

Warn friends, family members, co-workers, and schoolmates about the possibility of receiving fraudulent messages, this is to prevent them from being exposed to phishing attacks.

06

Perform an advanced offline scan using the security program built into the Windows system, by opening the user's settings on the computer and moving to the security settings menu, then selecting "Virus and Threat Protection" to begin performing a comprehensive anti-virus scan and other malware on the device without the need to connect to the Internet.

# The authorities I turn to when I am exposed to phishing

07

You can benefit from technical support services provided by technology companies such as Microsoft by calling the approved number or means of communication declared, and the same applies to other technology companies such as Mac and Apple.

08

Communicating with the authorities concerned with combating cybercrimes within the country when exposed to a type of phishing, as these authorities possess the devices and competencies that enable them to intervene and address the problem before it escalates, restore data, and arrest cyber hackers.



# Exercises and training





**First:**  
**In-Class Exercises**



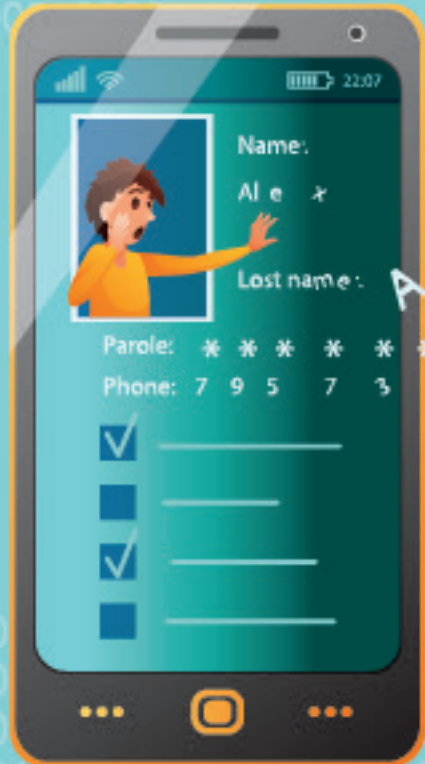
# Pay attention!

## Phishing

It means that cyber attackers masquerade as a known entity such as Amazon or a reputable person in an email or any other form of communication. Attackers usually use phishing emails to distribute malicious links or attachments through which the attacker gets sensitive data belonging to the victim, such as login credentials, bank account numbers, family or work personal information, etc



# Do you know that...?



Spear phishing attacks are widespread attacks targeting sensitive data of users in general.



## Pay attention!

# Spear phishing

It is targeting an individual within a specific institution; In order to steal his login credentials; the cyber attacker collects personal information about the targeted individual before the fraud begins, such as: his name, position, and contact details. Individuals targeted by this type of phishing include CEO in organizations who may open unsecured e-mail messages, which allows criminals to hack the organization's general system through the device of officials.



## Exercise 1

Determine what is **true** and **false** about phishing.

### Instruction:

Read the phrases below carefully, and think about whether these phrases express true or false information regarding phishing. A solved example is given in the table.

Phishing is an attempt to steal money or identities by revealing personal information

true

Phishing criminals are interested in confidential information such as posts on social media platforms.

Phishing depends on revealing confidential information, which includes credit card numbers, passwords, and banking information.

Sometimes websites carry out phishing frauds.

Phishing criminals do not pretend to know the victim and do not pretend to be friends or family.

Fake messages are used in phishing frauds.

Suspicious links are one of the most prominent methods of phishing.

Phishing criminals cannot take advantage of bank information or credit card numbers.

Phishing criminals don't care about identity.

You cannot protect yourself from phishing no matter how hard you try.

# Pay attention!

## Vishing

It is a type of phishing attack that is carried out via phone calls or voice mail, with the aim of obtaining the victims' money or other personal information. The reason behind the spread of these cyber attacks is what is known as "social engineering", it is a modern technology that relies on natural human instincts, such as trust, fear, and other feelings that cyber attackers exploit to affect victims to push them to make a specific decision that leads to achieving the attacker's goal, such as stealing money or sensitive information.

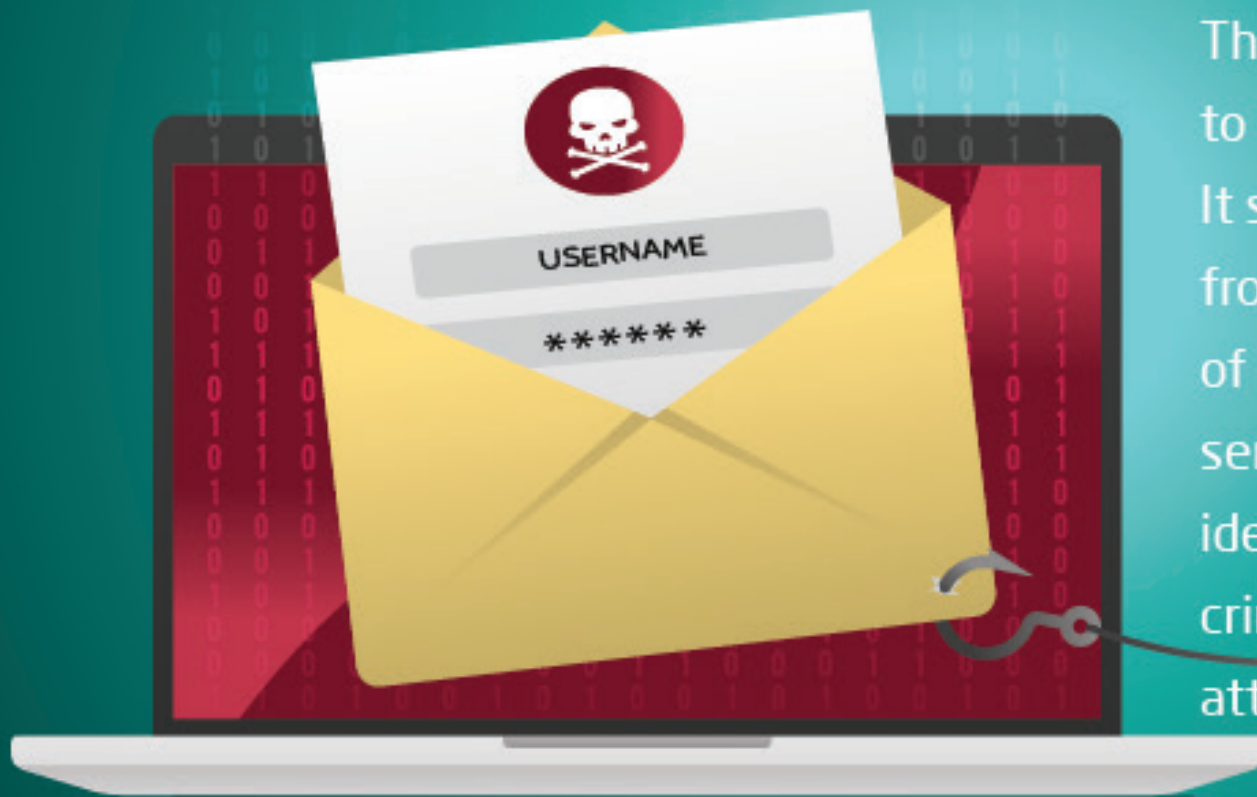




# Pay attention!

## Email phishing

The cyber attacker relies on e-mail to carry out his attack on the victim. It sends an email that appears to be from a credible source with the aim of hacking the device to steal sensitive data, steal money, or steal identity and later exploit it in other crimes such as a ransomware attack.





## Exercise 2

Put the appropriate word for each definition:



It is the most common form of phishing and it uses email programs.

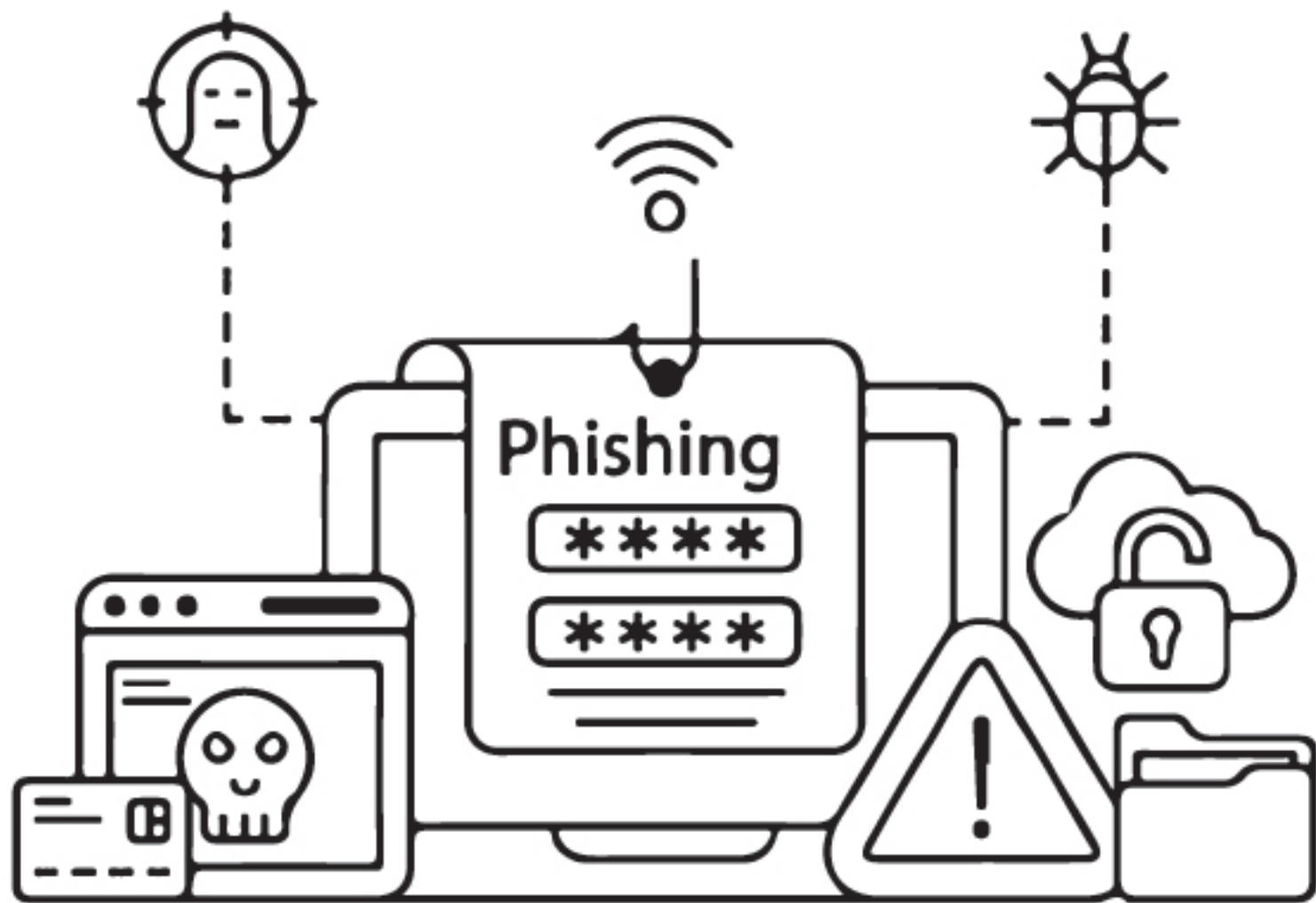
**Email phishing**

It is a type of malware that is hidden in an attachment that comes to you via e-mail, and once opened, it causes disruption of operating systems

A type of phishing attack targeting large networks or a group of specific people by exploiting research conducted about them, their work, and their social lives.

SMS messages are used disguised as trademarks or large, trusted websites to deceive the user into opening the link or text sent.

Voice is used to push the victim to provide sensitive and personal information over the phone by impersonating personalities close to the victims.



## Do you know that...?



- vishing is one of the types of phishing attacks that are carried out via phone calls. With the aim of obtaining the victims' money or other personal information.



# Pay attention!

## HTTPS Phishing

It occurs by sending an email to the targeted user that includes a link to a fake website, with the aim of deceiving the victim to enter his or her private information.





### Exercise 3

Complete the following sentences:

#### Instruction:

Read the phrases below carefully, and put the appropriate words in the blank so that the phrases have a useful meaning. A solved example has been placed in the table.

1

Attackers use communications to manipulate **victims' emotions** and obtain information and ..... This takes advantage of the victim's lack of awareness or failure to think about the dangers of exchange of ..... and data.

2

Trolls are keen to ..... the victims' needs in order ....., Job seekers often fall into this trap, so they rush to log ..... without verifying the site, and of course this data is exploited against them.

3

Overconfidence is one of the most prominent ....., in which victims fall, and those who are deceived by false ....., and do not make sure the validity of the information they receive.

4

Emotional manipulation is also used to ..... victims into acting without ....., or caution, exploiting the feelings of fear and ....., to get what they want without any effort.







## Exercise 4

Arrange the following steps in a logical order to show what to do in case of exposure to a phishing attack:

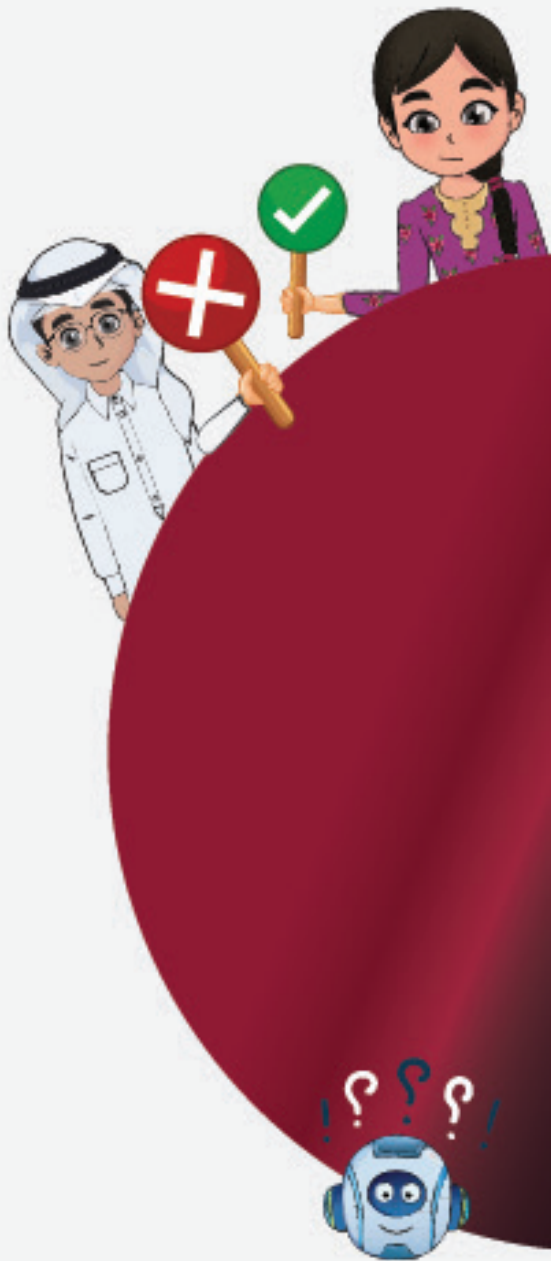
### Indication:

Read the phrases below carefully, and rearrange the phrases so that the first phrase is the first action you take when exposed to phishing, the second phrase is the second action, and so on until the end of the phrases.

1	If you use the name of a company or website, you must contact the company and warn it not to use its name for Fraudulent works and purposes.	
2	Go immediately to the Cybercrime Unit to report what happened to you, especially in the case of the theft of money.	
3	If bank account or credit card data is stolen, contact the bank immediately to stop any transactions on your account.	
4	Write posts explaining how you were exposed to phishing; So that no one else falls into the same trap.	
5	Stop all types of communications with this scammer who tried to deceive you.	
6	If the phishing is through a job advertisement, you must immediately report the suspicious advertisement.	
7	If you believe that your computer or phone has been hacked, you must immediately stop connecting it to the Internet and go to a specialist to help you secure your device and install protection software.	

## Exercise 5

Put (✓) or (✗) in front of the following phrases:



1

Open any text messages that arrive on the phone, even from unknown numbers.



2

Open links and attachments that come through email.



3

Provide your confidential data over the phone, whether to the family or to the responsible authorities.



4

Sharing a lot of personal information via social media platforms.



5

Use strong passwords.







6

Avoid using protection programs and firewalls.

7

Sending money to charitable organizations that contact you without verifying them.

8

Share your bank card data on all e-shopping sites.

9

Avoid disclosing any personal data or sensitive information about you.

10

Return to the bank before disclosing any private data from the calls claiming to be from the bank's customer service.



**Pay attention!**

## Pharming attack

Pharming is a combination of the words "Phishing" and "Farming", and is an online scam similar to phishing; where a fake website is designed and then targeted users are redirected to it to steal confidential information.



## Exercise 6

Determine from the following activities that contribute to building a digital fingerprint:



E-procurement.

True

Registration on websites.

Download apps from app stores.

Talking on the phone.

Registration in general bulletins.

Go for a walk.

Buying and selling stocks.

Subscription to electronic journals.

Opening a bank account.

Social media posts.

Watching television programs.

Share information and photos with friends.

Republish the articles and information you read.

Subscribe to health blogs.

Publishing videos via social media platforms.



# Pay attention!

## Deceptive Phishing

Cyber attackers use deceptive technology to pretend that they are working with a real company, such as Apple, to inform the targeted user that they are actually being subjected to a cyber-attack, to push him to click on a specific link, but it is in fact malicious. Which causes their computers to be infected.









## Pay attention!

# Pop-up Phishing

It means that fraudulent messages appear to users while they are browsing the Internet. Where attackers infect original websites with malware; Which causes these pop-up messages .to appear when you visit it

## Do you know that...?

Evil twin phishing is a cyber-attack that deceives targets into connecting to a fake Wi-Fi network that looks like the real one.





# Pay attention!

## Whaling

It is a phishing attack targeting senior executives in global institutions, disguised as a familiar email, and is designed to incentivize its victims to perform actions such as transferring money or sending personal data.



## The goal of whaling attacks

1. Pushing victims to click on links to sites that included malware.
2. Transferring money to the cyber attacker's bank account.
3. Requesting data for institutions or individuals to launch further attacks, such as a ransomware attack.





## Exercise 1:

Extract the following words from the table:

## Indication:

Read the words below carefully, and search in the table for consecutive letters that form these words. Below is an example of the word "phishing," and how to find the letters of the word in the table:

m	a	n	i	p	u	l	a	t	i	o	n
f	r	a	u	d	c	r	i	m	e	z	p
m	e	s	s	a	g	e	s	z	q	m	h
v	i	c	t	i	m	s	t	r	a	p	i
m	a	l	l	v	o	i	c	e	i	d	s
f	o	r	g	e	r	y	f	e	a	r	h
d	a	t	a	t	h	e	f	t	n	l	i
p	a	s	s	w	o	r	d	m	x	q	n
a	t	t	a	c	k	d	a	t	a	z	g

Theft - Data - Fear - Forgery - Voice - Victims - Trap - Messages - Crime - ~~Phishing~~ - Fraud - Mail

Attack - Password - Data

# Pay attention! Clone Phishing

It is when a hacker makes an exact copy of a message that the recipient has already received. It might include something like "resend this" and include a malicious link in the email.





**Exercise 2**

Can you determine whether the message that arrived in your email is real or just a phishing scam? And how? How will you deal with it?

---

---

---

---

---

---

---

---

**Exercise 3**

Do you know Someone in your surroundings - family or friends - who has ever been exposed to a "phishing attack"? How was this attack? How did he deal with it? Do you think his action was wise or should he have done something else?

---

---

---

---

---

---

---

---





## Exercise 4

Mark (✓) or (✗) in front of the following phrases:

Check the sender, especially while opening emails that contain attachments.

Open any email from anyone, even if you don't know him.

Report the suspicious email to the service providers.

Respond to any calls or messages requesting your personal data. There is no harm in that.

Hover the pointer over the link to make sure that it is a real site before entering it.

Participate in promotions and leave your email on all sites and platforms.

It is okay to visit strange Internet sites or with unknown extensions.

Look for grammatical or spelling mistakes because they are an important indicator of fake messages.

If you are exposed to an attack or hack, do not worry, and never inform the responsible authorities.

Do not worry about updating the systems or applications on your device or phone.

## Exercise 5

**Give 5 tips to someone who will be using the Internet for the first time and you want to help and protect him/her from falling victim to phishing:**

---

---

---

---

---

---

---

---

---

---



## Exercise 6

Define the following terms:

Social engineering

.....  
.....  
.....

Password

.....  
.....  
.....

Phishing

.....  
.....  
.....

Digital fingerprint

.....  
.....  
.....

Cyber fraud

.....  
.....  
.....



# Goals of phishing attacks

1

Stealing information or money from targeted users.

2

Creating a portal to carry out other operations to destroy the systems of targeted institutions.

3

Installing malware on targeted users' devices.

4

Push the victim user to log in to a fake website on the Internet to complete the fraudulent attack plan.





## Signs that distinguish phishing emails

1

Writing style: a writing style that is unfamiliar to the recipient.

2

Grammatical and spelling mistakes.

3

Inconsistency in email addresses and links.

4

Insistence and provoking feelings of fear.

5

Suspicious attachments.

6

Request to download programs and links.

7

Awards messages.

8

Fake web pages.

9

Targeting employees in institutions.



## Evil twin phishing

It is a cyber attack that deceives targets into connecting to a fake Wi-Fi network that looks like the real one, and when it comes to connect, the attacker begins to hack the victims' devices to steal all their data and files.

One of the distinguishing signs between phishing messages and real messages sent is

They are filled with phrases that make the user feel afraid and want to make an immediate decision to overcome this fear and anxiety arising from their content.







## What is it?

- It is an attack that cyber attackers masquerade as a known entity or a reputable person in an email or any other form of communication. ....
- It is a fraudulent attack targeting an individual within a specific institution. With the aim of stealing his login credentials. ....
- It is a type of phishing attack that is carried out via phone calls, with the aim of obtaining the victims' money or other personal information. ....
- It is a Fraudulent attack that occurs by sending an email to the targeted user that includes a link to a fake website, with the aim of deceiving the victim to enter his or her private information. ....





- It is an attack that causes the appearance of fraudulent messages to users while they are browsing the Internet. Where attackers infect original websites with malware; which causes these pop-up messages to appear when you visit it. ....
- It is a cyber attack that deceives targets into connecting to a fake Wi-Fi network that looks like the real one, and when it comes to connect, the attacker begins to hack the victims' devices to steal all their data and files. ....
- It is a fraudulent attack targeting senior executives in global institutions, disguised as a familiar email, and is designed to incentivize its victims to perform actions such as transferring money or sending personal data. ....
- It means that a hacker makes an exact copy of a message that the recipient has already received. It might include something like "resend this" and include a malicious link in the email. ....
- It is a fraudulent attack in which the attackers use deceptive technology to pretend that they are working with a real company, such as Apple, to inform the targeted users that they are actually being subjected to a cyber attack, to push them to click on a specific link, but it is in fact malicious. Which causes their computers to be infected. ....





## Complete the following sentences:

- ..... is one of the most widespread cybercrimes in the world.
- In phishing, artificial intelligence can be used to innovate ..... to use it on the phone to circumvent the victims.
- It is difficult to distinguish between phishing messages and real messages sent to users, but there is a sign that is many ..... in them.
- The goal of phishing attacks is to steal ..... or ..... from the targeted users, and ..... on users' devices, and pushing the victim to log into ..... on the Internet.
- One of the ways for cyber attackers to hack targeted users' devices is to send ..... containing ..... that include ..... When clicking on it ..... are allowed to crawl your computer.



- Receiving email notifications about ..... even though the user has not done, the ..... device, and the high ....., and the delay in the commands received from the user.
- The appearance of ..... containing annoying messages claiming that your electronic device is infected with viruses is one of the signs that the device is exposed to hacking.
- Among the mistakes that Internet users commit are: browsing on the ..... network, and not updating ..... and ..... on devices, in addition to sharing a lot of ..... on social media.
- ..... is data path left by the user when using the Internet.
- One of the ways to protect data from hacking: using ..... It represents the first line of defense against fraudulent attacks.



Mark (✓) or (✗) in front of the following sentences



**One of the mistakes that an Internet user makes while performing his tasks or browsing on the global network is**

- ▶ Browsing on a public Wi-Fi network without taking the required security precautions.
- ▶ Updating the browser and applications on devices.
- ▶ Sharing a lot of personal information on social media.
- ▶ Different passwords for a number of the user's personal online accounts.
- ▶ Installing software updates automatically.
- ▶ Opening links from emails without checking their authenticity.
- ▶ Not taking advantage of your privacy settings on social media.



## 2- Ways to form a digital fingerprint

- ▶ Registering for email newsletters on websites and newsletters.
- ▶ Restricting posting on social media.
- ▶ Stay away from online financial transactions such as shopping.

## 3- The difference between phishing and spear phishing

- ▶ Phishing attacks are highly targeted attacks that target a specific victim.
- ▶ Spear phishing attacks take more time and effort to execute.
- ▶ Spear phishing attacks are widespread attacks targeting sensitive data of users in general.

## Graduation project

The graduation project is an assignment that you undertake on your own or in collaboration with one or two of your colleagues, under the supervision of the trainer. Through it, you are required to perform one of the following assignments:

- Write a short story about a student who asked his colleagues to explain what web bots are and how the student conveyed the information to his colleague.
- The student takes on the role of the trainer and writes general guidelines for his colleagues or parents, explaining phishing and how to combat it.









**CyberEco**



**الوكالة الوطنية للأمن السيبراني**  
**National Cyber Security Agency**