Phishing attack

Student exercises and trainings

Training Kit

Middle School

CyberEco

معًا لدعم السلامة الرقمية

Together to support digital safety

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

Phishing attack

Student exercises and trainings

Intellectual Property rights

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

00974 404 663 78

00974 404 663 62

Dear Student

This booklet is specifically for you, and you must have it with you when you attend training sessions. Your trainer will guide you on how to use it. This booklet contains a collection of fun and useful exercises, which you will answer either during class or at home.

The booklet also contains a set of educational competitions and cards, as well as general information in which you will find useful and enjoyable. Your trainer will guide you on how to deal with these competitions, and at the beginning of each exercise or competition, we will provide you with general instructions on how to answer.

Dear Parents

This booklet is specifically for the student and will accompany them during the training they will receive at school. It contains a collection of exercises, training activities, competitions, training games, and training cards, all of which revolve around concepts related to Phishing attack and how to confront it.

The purpose of this booklet and and it's included mental exercises and activities is to reinforce and solidify the information that the student receives during the training session with the primary goal of enhancing the student›s ability to use the internet and technology effectively and safely.

All the exercises and training in the booklet will be accompanied by general instructions on how to answer them. As for the training competitions, the trainer will provide guidance on how to solve them. The booklet also includes some non-classroom exercises, which the student will answer at home. These exercises will also be accompanied by trainer for the solving. We kindly request your indirect supervision as the student interacts with this booklet. If the student has any question or inquiry about any of the exercises or training activities, please read the specific instructions for each exercise and provide assistance to student in light of these instructions.


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!

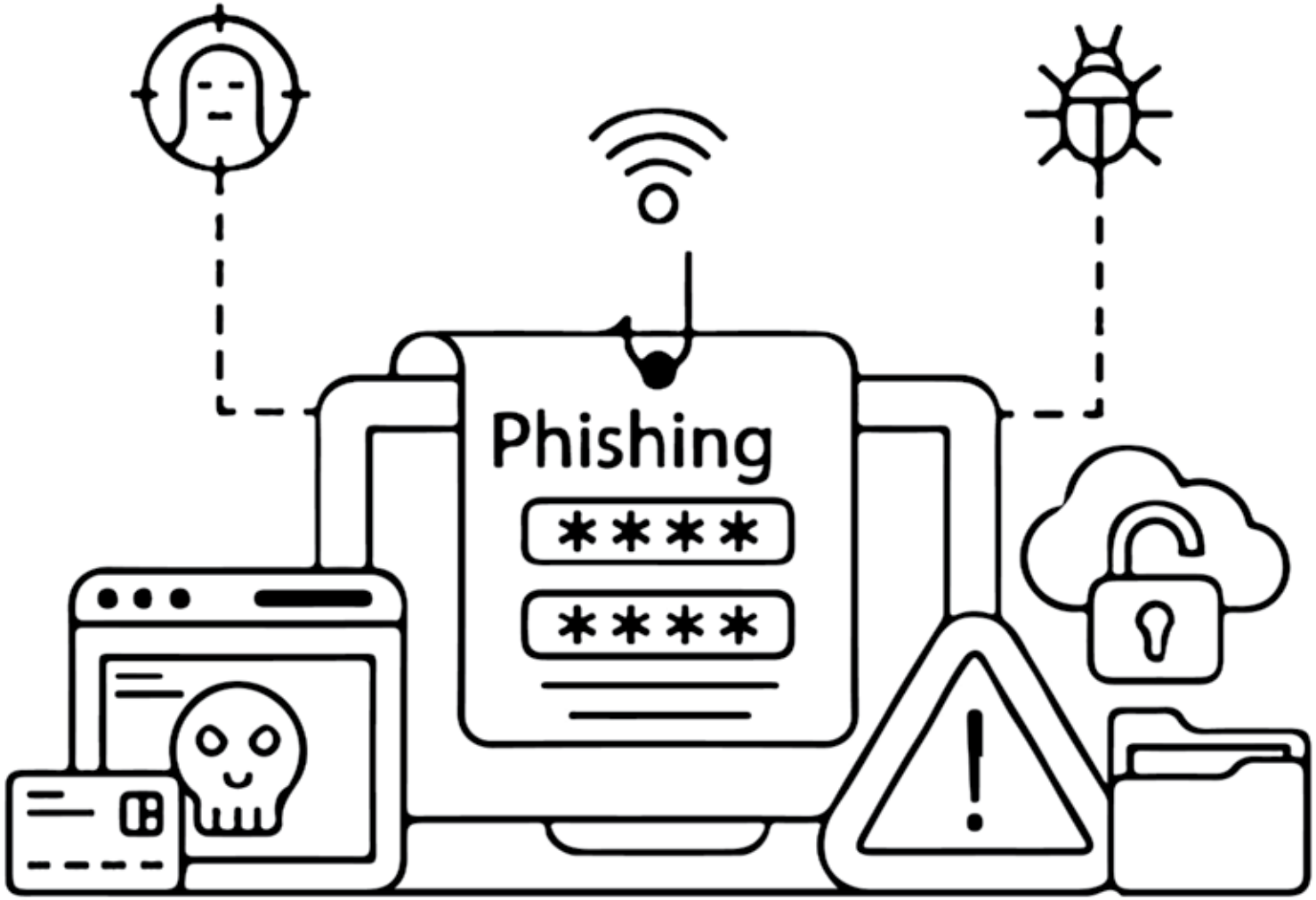
Email phishing

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.	


Phishing
****
****

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

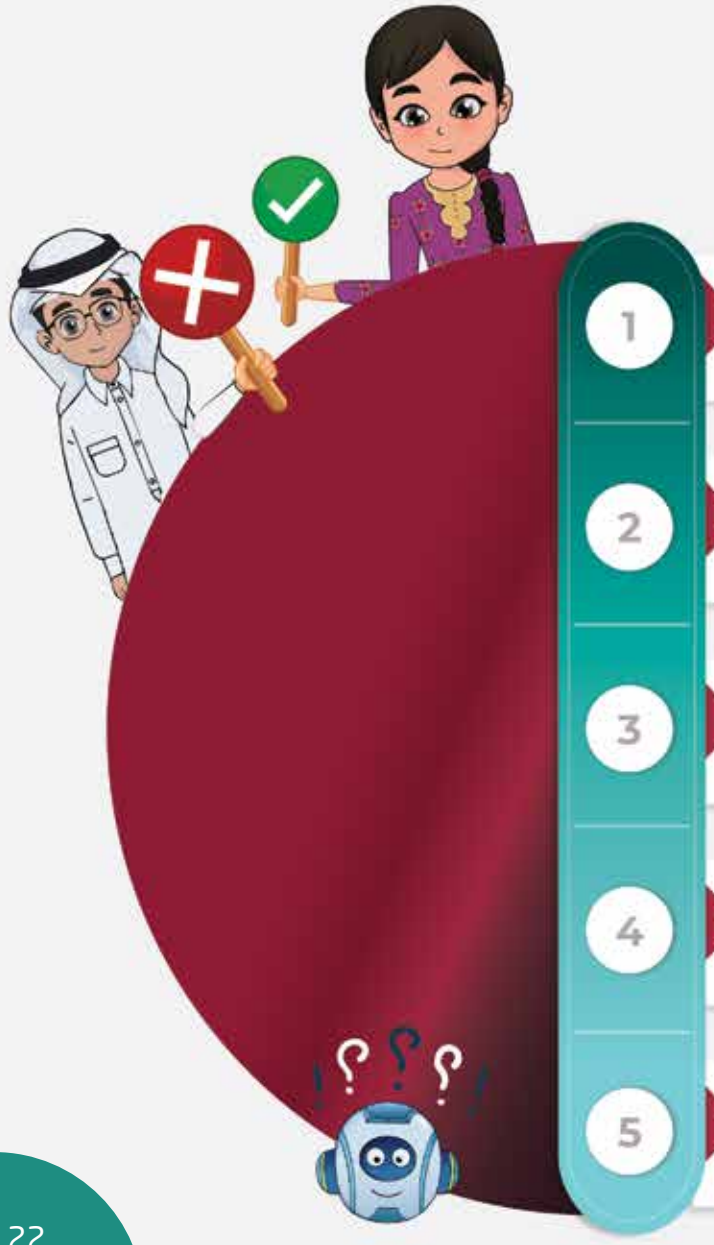
Arrange the following steps in a logical order to show what to do in case of exposure to a phishing attack:

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. pen 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

	True
E-procurement.	
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.


Second:
Non-classroom
Exercises

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?


01001110
01110100
0111011101
11110001011

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.


Competitions

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.

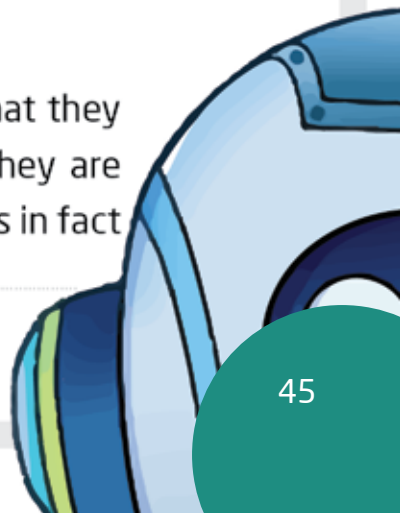
- It is an attack that causes the appearance of fraudulent messages to users while they are browsing the Internet. Where attackers infect original websites with malware; Which causes these pop-up messages to appear when you visit it..

- 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.

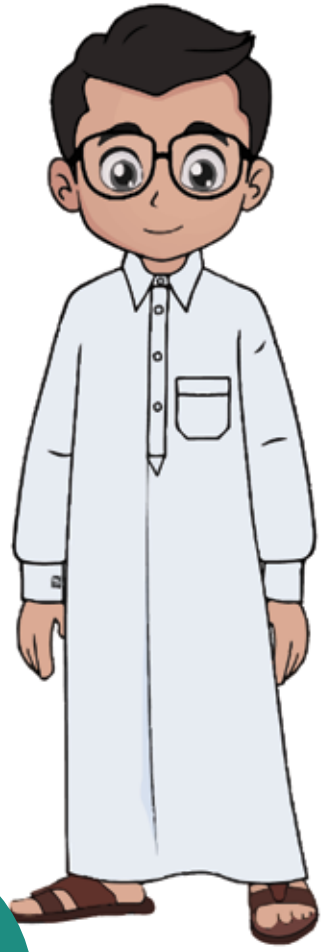


Complete the following sentences:

- _____ 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 faced a phishing attack, and how he or she acted in that situation.
- 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

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency