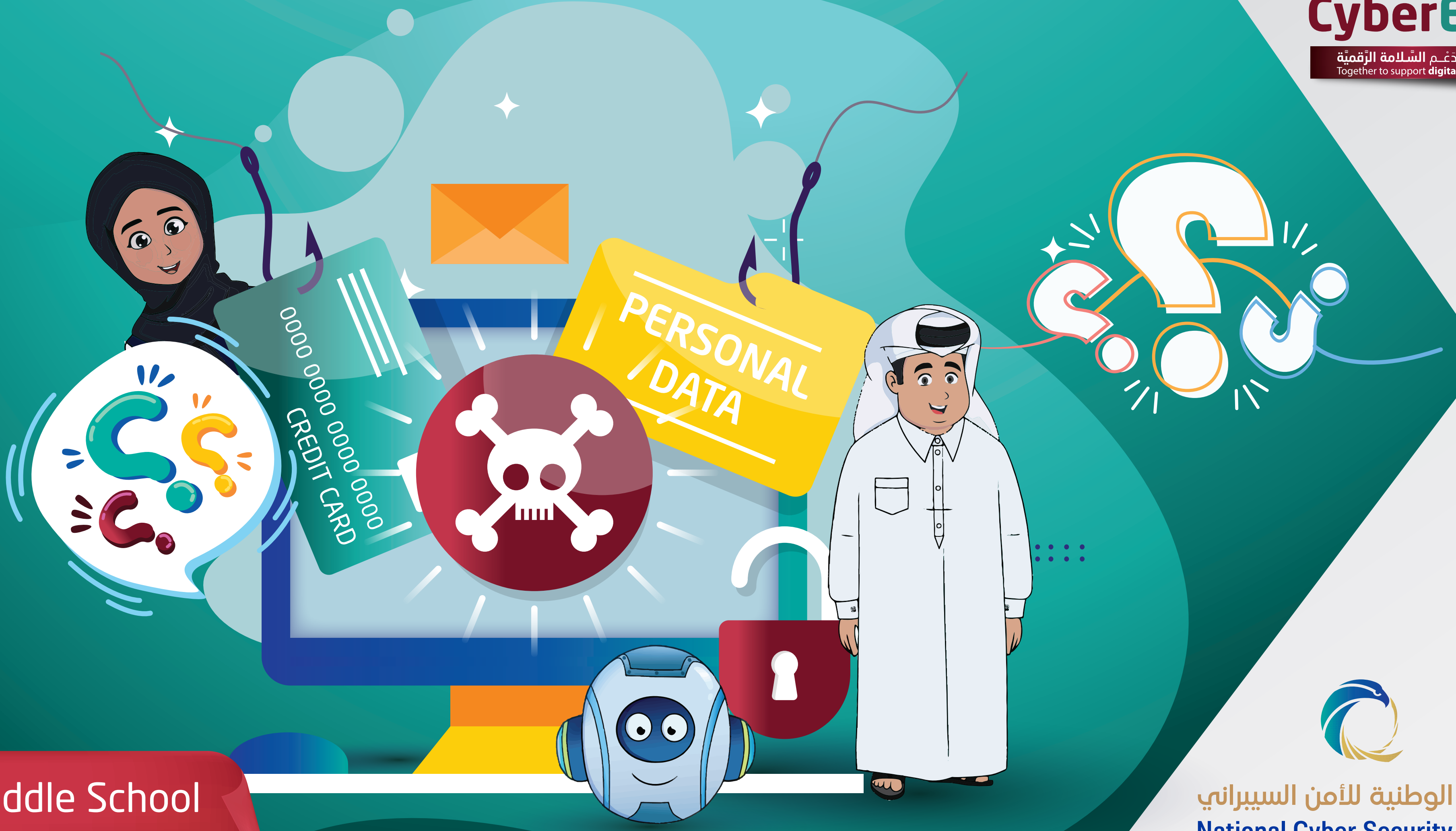
Phishing Attacks

Training kit

Trainer’s booklet



Middle School

CyberEco

معًا لدعم السّلامة الرّقميّة
Together to support digital safety

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Phishing attack

Middle School

Training material

Trainer’s Book

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

General content of the Kit

First: General Introduction to the training kit

Second: Scientific content

First: General Introduction to the Training Kit

Below is an explanation of some details relevant to the objectives of the training kit, along with general guidelines for the trainer on how to handle this kit, while providing him with the scientific content that will be relied upon during the training.

The general idea

The concept of this training kit is to equip the trainer with tools and training resources, making it easier for him to deliver information to the trainees. In general, each training material consists of two parts: One part for the trainee and another for the trainer. The training kit serves as a general guide and support for the trainer, and its scientific content is the same as that of the trainee, but here the training content is presented differently. Additionally, the kit equips the trainer with training tools and methods that support him in the training process.

Objectives of the training kit

1. Providing the trainer with training tools that help him deliver the training content to the students.
2. To present information and training content in an easy and simple manner.
3. To offer training content on phishing attack along with multiple training tools and methods.

Contents of the Training Kit

The training kit includes several training tools, as detailed below:

1. **Presentation files.**
2. **Training games,** such as crossword puzzles and quizzes”, which the trainer presents to the students to ensure their interaction with the training content.
3. **Educational videos.**
4. **Competitions,** Contests in the form of inferential questions presented by the trainer to encourage interaction between the students.
5. **Training cards**, comprising general information accompanied by illustrative images, presented by the teacher to the students.
6. **Sketches**, including information about the main topics in the training content.

Content of the Training Kit

Chapter One:

Chapter Two:

Chapter Three:

WorkShop Timetable

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

Trainer's Guidance Manual

The following is an explanation of some general guidelines for the trainer, revolving around how to use this training kit.

1. The scientific content of the kit may exceed the student's ability to comprehend, especially in terms of general concepts. Therefore, the trainer must simplify these concepts and present them in a way that is understandable to middle school students.
2. The trainer presents slides for each point discussed. For example, when talking about the concept of the Phishing attacks, the corresponding slide is presented, and the same applies to all scientific content.
3. After explaining of the first and second chapters the scientific material, a simple test is given to them, such as "Mark (✓) or (✗) for each sentence.
4. During the explanation of the first chapter, specially designed images for the "Did you know that..?" section are distributed.
5. The trainer displays "Sketches" while the students solve the exercises.
6. At the end of the training, the trainer presents the quiz questions mentioned at the end of the document.
7. During the presentation of the scientific material for each chapter, a portion of the allocated time is used to present several links related to the content of the chapter.
8. The trainer displays the videos - mentioned in a separate file - to the students at the end of each chapter, or in the place he deems appropriate.
9. Mention examples of phishing incidents that occurred during the presentation of scientific material.
10. Please initiate discussions with the students at times considered appropriate by the trainer.
11. Regarding exercises directed towards students; a file with exercises will be attached at the end of this kit. These exercises are divided into two parts: a part to be given to students during training, which are classroom exercises, and the other part assigned for students to answer at home, which are non-classroom exercises. This division will be explained at the end of this kit.

Graduation Project

The graduation project is a task carried out by the student, aimed at achieving several goals, Here is an explanation of the most important ones:

- Ensure that the student has absorbed the information and ideas presented and is capable of applying them in their daily life.
- Consolidate the information and ideas that were presented to the student.
- The project serves as a link between theoretical information and practical real-world application.

Regarding the mechanism for assigning students to the project, and how to implement it, the following guidance can be provided:

- The graduation project can be individual or group-based, In case of a group project; the number of students participating in one project should not exceed three students.
- The students choose the project topic, and the trainer can provide some assistance or ideas in this field.

- The topic of the graduation project must be consistent with the training content that was presented to the students.
- The graduation project can be within one of the following scenarios, which are non-binding concepts. The trainer can choose other concepts that he find suitable. Here are some suggestions:
    - Writing a short story that revolves around a student who was exposed to a phishing incident, and how he dealt with this situation
    - The student takes on the role of the trainer and writes general guidelines to his colleagues or family members, explaining to them the concept of phishing attacks and how to protect against these attacks.

Second: Scientific Content

Chapter One

The concept of phishing

- First: the concept of phishing.
- Second: Types and forms of phishing.

0 1

First: the concept of phishing

Phishing is one of the most common types of digital crimes. In this type, the Internet is exploited to deceive targeted victims by stealing their personal data, such as passwords and credit card numbers, through several methods and tools, including creating a fake website to lure the victim. The link is sent via e-mail or messenger messages to be clicked on, thus allowing hackers, without the user's knowledge, to illegally enter the victims' accounts and devices and install malware help them steal data.

Attackers rely on psychological pressure tactics to persuade victims to act without thinking, by impersonating a familiar persona, then creating a false sense of need, exploiting feelings such as fear and anxiety to get what they want. In this case, people tend to make quick decisions when they are informed that they are at risk of losing money, or that there is a legal problem they may face, or that they will not be able to access one of the important resources for them later.

This is done by sending a message asking the user to "take immediate action." this is a fraudulent trick by cyber attackers.

In general, phishing means that digital attackers masquerade as a known entity - such as a well-known company with a good reputation, 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 so on [1].

Phishing is one of the most widespread cybercrimes in the world, because deceiving individuals into clicking on malicious links contained in fraudulent emails is easier to do than carrying out a hacking attack on computer security. According to the report issued by Cisco on cybersecurity threats for the year 2021, it revealed that phishing is responsible for 90% of data security hack in the world. In IBM research in 2022, phishing was linked to 550 cyber attacks that cost an estimated 4.9$ million in losses [2].

[1] Phishing, Alexander S. Gillis, Technical Writer and Editor. On site: https://cutt.us/5jBhs

[2] What Is Phishing? On site: https://cutt.us/PbZ3Y

In this type of cyber attacks, the attacker impersonates another person through e -mail, or any of the means of communication such as “Messenger”, or the messages of the service of short messages (SMS), For the purpose of obtaining sensitive information about the victim user,, In order to do this , the attacker uses opened sources to obtain personal information about the targeted victim., and one of these sources is “social media such as Facebook,” where this information is later used when drafting a fraudulent email message to deceive the victim and thus hack his cybersecurity.

In this type of attacks the user victim get a message that seems outwardly that it is affiliated with a trusted authority with the same as the world institutions “Microsoft” or “Google” ... and others. As soon as the user clicks on the files attached to the message - which is often a hyperlink linking him to a malicious website - the attack begins by installing malware on his device or directing him to fake websites, to begin the process of collecting sensitive information, such as passwords and bank card numbers, etc.

What increases the credibility of these phishing messages is the attackers’ use of artificial intelligence tools such as chat bots to overcome the poor format of the messages.

And it does not stop the chat bots, but the artificial intelligence can also be used to create a voice to exploit it through the phone to follow the victims, through their delusion that the voice belongs to one of the important stakeholders that the victim deals with or associates with an interest to begin the process of deception and obtaining personal information from him..

In general, it is difficult to distinguish between phishing messages and real messages sent to users, but the most apparent sign in phishing messages is the large number of spelling and grammatical mistakes in them, as well as the cyber attacker’s use of two e-mail addresses that are different from the original ones to the authorities whose identity has been impersonated; When looking at the style used in writing phishing messages, we find that they are filled with phrases that make the user feel afraid and want to make an immediate decision. To overcome this fear and anxiety resulting from its content.

In general, the aim of phishing attacks is the following points:

- Stealing information or money from targeted users.
- Creating a gateway to carry out other operations t to destroy the systems of targeted institutions.
- Installing malware on targeted users' devices.
- Push the user victim to log in to a fake website to complete the fraudulent attack plan.

Thus, we find that phishing results in a number of damages at the level of individuals and institutions; For institutions, phishing attacks can cause the organization's internal operations to be destroyed, thus causing major financial losses. In addition to harming the institution's reputation, customer data becomes at risk of being stolen and manipulated; This puts institutions in confrontation with executive regulations aimed at protecting data within countries.

As for individual, phishing attacks result in the theft of their bank data and personal information and their re-exploitation, causing greater damage that amounts to distorting reputations, fabricating lies, and identity theft.

Types of phishing

- **Email phishing:** Relies on techniques such as fake hyperlinks to deceive email recipients into stealing their personal data. The attacker often masquerades as a large account provider such as Microsoft and Google, or a co-worker or student.

- **Ransomware Phishing:** Attackers "insert malware disguised" as a trusted attachment such as a CV or bank statement in an email, and once the victim opens it, the entire system crashes.

- **Spear Phishing:** In this type of attack, attackers target specific people by exploiting information collected by researching their jobs and social lives that they share via social media.

- **Whaling Attack:** This cyber attack targets important figures in societies, such as artistic celebrities, businessmen, and politicians. In-depth research is conducted on their targeted victims in order to exploit the appropriate moment to steal their bank information and important personal data.

- **Phishing via SMS:** The cyber attack sends text messages disguised as trusted contacts from companies known to the victim user, such as: Amazon, Google, etc.

- **Vishing:** Attackers who seek to deceive people into providing sensitive data over the phone impersonate people in specific jobs of interest to the victim.

Second: Forms of phishing

Phishing often occurs in several forms, and the following is an explanation of the most important of these forms:

- **Spear phishing**

Spear phishing means targeting an individual within a specific institution for the purpose of stealing 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.

The difference between phishing and spear phishing

The difference here is that spear phishing attacks, as the name suggests, are dedicated to a specific target. Phishing attacks are large-scale attacks that target sensitive data of users in general. In this type of fraudulent attack, the email message is deceptive, but it is not designed to suit specific individuals, and here the attacker relies on quantity, not quality. Meaning that it sends fraudulent messages to a list of mailing addresses, perhaps a group of them will fall into the trap.

This is unlike spear phishing, which are very specific attacks that target a specific victim and emails appear more credible. Because they carry addresses related to the victim, and therefore this type of phishing attacks require more time and effort [1].

[1] What is spear phishing? Definition and risks. On site: https://cutt.us/riHDD

- **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. Vishing can also be carried out by playing on the victim's desire to achieve material gains, such as luring him with huge purchasing offers at nominal prices, or offering a fake competition with a large financial return and other tempting tricks used by the cyber attacker.

Therefore, the user must be careful not to inform others via the phone of his important information because if the caller is from the bank, he will not ask for personal information such as credit card numbers on the phone. You should also evaluate the number calling you first before answering it, and it is preferable to call it from another number. To ensure its credibility.

It is not preferable to respond to emails, text messages, or social media messenger messages that request personal information such as your phone number, as this is often a proactive step before receiving a vishing call later [1].

[1] Vishing – a growing threat. On site: https://cutt.us/q3aSU

- **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:

1. Writing style

Spelling and grammatical mistakes are also hallmarking of fraudulent messages. 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.

2. Grammatical and spelling mistakes

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.

3. 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.

4. 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. Here, one must be alert to this issue, not fall under the pressure exerted, and take time to think before taking any action.

5. 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.

This type of malware attachment carries extensions such as scr, exe, zip... and other unfamiliar extensions. Therefore, attachments must be scanned before opening them with Anti-virus programs[1].

6. 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 and you should not respond to these commands.

7. The recipient did not initiate the conversation

In most scams, the victim receives an e-mail that prompts him to respond 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.

8. 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.

9. 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.

[1] 10 Most Common Signs of a Phishing Email. On site: https://cutt.us/MJiQZ

- **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. Fraudulent HTTPS websites are a preferred port of call for attackers who have the ability to deceive victims into believing they are a trusted source. This type of fraudulent attack is described as low risk and high reward.

- It is noted that 91% of all cyber-attacks begin with a phishing email sent to unexpected victims, luring them to the sites via a link in the message sent from a legitimate address, such as a known company or well-known person. The most widespread example of this type of fraudulent attack is Sony Pictures, which in 2014 was exposed to an attack via fake emails during which the attackers were able to hack the company and steal passwords and important data from it as a result of employees clicking on fake links sent to them via email [1].

- **Phishing attack known as pharming**

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. These fake websites aim to collect personal information about the victim, such as passwords, bank account numbers, etc. Or it attempts to install malware on victims’ computers, especially those working in the financial sector such as banks or online commerce sites, for the purpose of identity theft; **The cyber attacker carries out his fraudulent operation through two methods:**

- Sending malicious code in an e-mail message for the purpose of installing a virus or Trojan horse on the target user’s computer; as this malicious code directs traffic towards a fake website even if the user types the correct website address, the goal of this malware is to divert him to the fake website without him being aware of it.

[1] HTTPS Phishing Attacks: How Hackers Use SSL Certificates to Feign Trust. On site: https://cutt.us/20AV8

- Using a technique called "Domain Name System Poisoning," the attacker makes modifications to the "Domain Name System" (DNS) with the aim of unintentionally diverting the targeted user to fake websites instead of the correct ones. Here, the attacker begins installing viruses or Trojan horses on The user's computer or collect personal and financial information for use in identity theft [1].

After obtaining personal data, attackers either use it for other fraudulent purposes or sell it to other attackers.

- **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. What increases the danger of this type of phishing message is its reassuring content to users. They provide a fraud warning to visitors to these sites about the security of their electronic devices and ask the visitor to download some software to fix the problem, such as anti-virus, but in reality they are malware whose goal is to hack the devices of website visitors and defraud the device owners.

To avoid pop-up phishing attacks, it is recommended to follow the following:

- If you see pop-up messages on some websites you visit, it does not necessarily mean that your device is infected with malware. The malware may be present on the website you are browsing, and if you have installed a good anti-malware program, it will not be able to infect your device.
- You should not give anyone remote access to your computer.
- If you are unsure of the authenticity of the messages you see, you should contact the website owner or your support team directly[2].

1. What Is Pharming and How to Protect Yourself. On site: https://cutt.us/BGtUI
2. Scam Alert: What You Need to Know About Pop-Up Phishing. On site: https://cutt.us/3pHtA

- **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: The following is an explanation of the most important ones:

- 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 [1].

[1] What is an Evil Twin Attack? On site: https://cutt.us/jsBji

- **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.

This type of attack aims to achieve the following goals:

- Paying victims to click on links to websites containing malware.
- Request to transfer funds to the cyber attacker's bank account.
- Requesting data related to institutions or individuals in order to launch further attacks, such as a ransomware attack.

In general, the damage resulting from whale attacks includes the following aspects:

- **Data loss:**

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

- **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.

These phishing attacks have become more difficult to detect recently. Because of the adoption of fake mailing addresses that appear as genuine, contrary to commercial terms and the combination of many fraudulent methods that executive officials fail to detect, and thus become victims of whaling attacks, whaling attacks can also use e-mail with phone calls to push the target victim to Satisfaction with the request sent Through the mail, and therefore it is a double attack, and social media is also a common way to carry out phishing attacks. It provides professional and personal information about the targeted people[1].

[1] Whaling: how it works, and what your organization can do about it. On site: https://cutt.us/H9RNo

- **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 malware which causes their computers to be infected.

- **Clone Phishing**

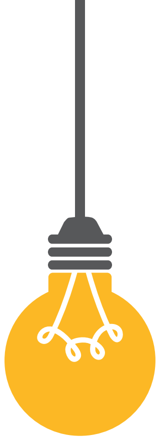
It means that a hacker makes an exact copy of a message that the target has already received. It may include something like “Resend this,” with a malware link in the email [1].

[1] How Does Clone Phishing Work? On site: https://cutt.us/x7Gwg

Chapter Two

How to carry out phishing attacks

- First: The loopholes that perpetrators of phishing attacks exploit.
- Second: Mistakes committed by Internet users.
- Third: Digital fingerprinting and phishing.



02

First: The loopholes that perpetrators of phishing attacks exploit

Attackers can access users' devices at home, at work, and anywhere the victims of cyberattacks are, by hacking into the users' Wi-Fi network, remotely taking over the computer, or hacking passwords through phishing attacks. This requires securing personal devices, and attackers penetrate networks and devices by exploiting weak points in the security systems built into them, with the aim of gaining unauthorized access to personal information. As a result, victims of phishing attacks lose their privacy and become threatened with identity theft for life.

There are several methods that cyber attackers exploit to penetrate their target users' devices, and the following is an explanation of the most important of them:

- **Sending fake text messages or emails containing links that contain malware**: when clicked on, devices are infected; This allows hackers to hacking into the user's computer to obtain important data or to place spaying on the device.
- **Fraud by claiming to provide technical support:** They contact the target user via emails or chats claiming that the device has been hacked, and the names of well-known institutions in this field are often used to convince the user.
- **Users' failure to update programs and applications makes them an opening for attackers to in hacking personal devices:** Therefore, we must pay attention to the importance of updating programs as soon as possible. To benefit from the repairs made by technical companies to secure them.
- **Utilising weak passwords that are easy to guess:** or they can be guessed on the user's devices and Wi-Fi network, contributes to exposing the user to the risk resulting from phishing attacks.
- **Clicking on unknown or untrusted links by users:** This helps attackers hack their devices and control them remotely or transfer them to a fake website that contributes to the theft of personal data such as passwords, names, and other personal details.

In general, there are many indicators that indicate the possibility of electronic devices being hacked, **as follows:**

- 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[1].

[1] Warning signs you’ve been hacked and what to do next. On site: https://cutt.us/rd84U

Second: Mistakes committed by Internet users

Cyberattacks can be mitigated through a content security policy, such as protecting against Cross-Site Scripting (XSS) attacks. This assists website owners in distinguishing between safe and unsafe resources. These policies also enable webmasters to establish their own rules tailored to their site's specific needs, in addition to preventing unauthorised access to sensitive information. Furthermore, the implementation of a Content Security Policy (CSP) is complemented by the provision of reporting and analytics tools that seek out security vulnerabilities.

There are several mistakes that the Internet user makes while performing his tasks or browsing on the World Wide Web, which are represented in the following points:

1. Browsing on public Wi-Fi without taking the required security precautions, which makes them more vulnerable to hacking and falling victim to phishing attacks; The user becomes monitored by the attacker to monitor his movements on the Internet and obtain passwords and sensitive data, so it is preferable to avoid conducting private transactions over the Internet when using a public Wi-Fi network.
2. Not updating the browser and applications on the devices makes it an opportunity for attackers to hack through the security vulnerabilities in old versions, which technology companies are constantly updating.
3. Sharing personal information on social media gives attackers the opportunity to exploit that information to carry out phishing attacks against the user.
4. The similarity of passwords for a number of online accounts, resulting in increased chances of users being exposed to fraud and theft because accessing any of them means accessing the rest of the accounts.
5. Use passwords that are easy to guess, which facilitates the process of hacking them. There are two types of simple passwords that the attacker can hack, the first: consecutive words, numbers, or symbols such as (123456, ABC), and the second: common terms that are easy to guess quickly.

6. Not installing program updates automatically, which increases the chances of viruses hacking the system. For example, Microsoft provides a continuous update for its Windows computer system, and here it is preferable to set the user's computer to "automatic update" to ensure obtaining every update for the Windows system automatically[1].
7. Opening links from emails without checking their authenticity enables viruses and hacks to hacking devices.
8. 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, in addition to the word "fraud" or "review" to ensure that no complaints have been received previously.
9. Ignoring basic security features, including two-factor authentication, as these steps ensure that passwords are protected in the event that a hacker tries to hack your accounts; The user then receives a notification stating this on his phone or another email.
10. Shopping online from untrusted sites increases the user's chances of being hacked; Especially if he uses his personal bank cards. Therefore, it is preferable to use a card with a limited capacity of money, and to set a strong password that is difficult to guess to overcome fraud attempts that occur.
11. There are many tempting tests spread on social media - especially Facebook - such as "If you were not a lawyer, imagine what you would be?" As soon as the user visits these pages that implement the tests, he becomes a prey to fraud and theft.
12. Do not take advantage of your privacy settings on social media, so all photos, information, and shares become available to everyone, from those close to the user as well as strangers [2].

[1] Which 7 Online Mistakes Will You Make Today? On site: https://cutt.us/z25Nk

[2] 10 mistakes people make online. On site: https://cutt.us/4XQ7A

Third: Digital fingerprint and phishing

The term 'digital footprint' refers to the trail of data left by a user when navigating the internet. This includes the websites visited, email correspondence, online shopping activities, conversations (chats), and all movements made by the user across various accounts, regardless of whether these actions are positive or negative. Websites can contribute to shaping a user's digital footprint by installing cookies on their devices. Furthermore, applications can collect users' data without their knowledge, especially if permission is granted to access stored files, be they text, videos, photos, or other types.

There are two types of digital fingerprints: the active fingerprint and the passive fingerprint… The active digital fingerprint is known as:

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. In addition, others [1].

As for passive digital fingerprinting, it means 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[2].

[1] What is a digital footprint? And how to protect it from hackers. On site: https://cutt.us/bObsJ

[2] digital footprint. On site: https://cutt.us/P2gI8

The digital fingerprint has clear importance in several areas; the following is an explanation of the most prominent of them:

- It is permanent and it is difficult to control how others use it.
- It determines the user's digital reputation as well as offline.
- Employers and universities can verify the digital fingerprints of potential employees and students, especially through social media, before making an employment decision or accepting university admission papers.
- Words, images and videos shared can be misinterpreted.
- Harmful to social relationships between individuals as a result of sharing the contents of private groups on the Internet in general.
- Hackers can exploit the digital fingerprint in phishing operations or to create fake identities based on the data collected from the fingerprint[1].

The user can contribute to his digital footprint through the following digital practices:

- Online shopping.
- Registration for newsletters on electronic websites.
- Financial transactions over the Internet.
- Social media.
- Joining websites.
- Subscribe to newsletters.
- Subscription to different applications.

[1] Importance of Digital Footprint: Complete Guide [2023]. On site: https://cutt.us/DCq7d

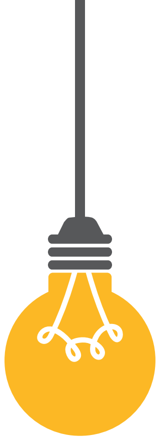
In general, the user should protect his digital fingerprint, and there are several ways to do this, the most important of which are as follows:

- Verifying our digital fingerprint through search engines. This is done by entering the name and searching for it on the engine to see what appears in the search results.
- Removing personal information from unimportant sites, such as fitness sites, to reduce the circulation of that information on the Internet.
- Controlling the amount of information that is shared via social media and other websites.
- Adjust your privacy settings, so that you restrict who can see your data or like and comment on your posts and see your photos.
- Verifying which websites are visited, or whose links are received via e-mail; because it may be for phishing or for stealing sensitive data, you should make sure that the site address begins with https, as the letter “S” here indicates the security of the site.
- Do not use public Wi-Fi networks when conducting financial or personal transactions.
- Deleting old accounts is one of the ways to reduce the information circulated about users on the Internet.
- Create strong and different passwords for accounts.
- Do not log in to websites or applications using Facebook data.
- Updating programs and applications, to benefit from the security fixes that technical companies make on them as soon as possible.
- Set a password for the smartphone, so that the data on it is not exploited if it is lost, hacked, or stolen.
- If you are hacked, you must change the passwords for all accounts immediately[1].

Chapter Three

How to act if exposed to phishing

- First: Instructions for protection against phishing.
- Second: Protecting data from hacking.
- Third: What do I do if I get phished?



03

First: Instructions for protection against phishing

Cyber attackers use email or text messages to try to steal users› passwords or bank account numbers. They launch thousands of phishing attacks, the majority of them succeed in achieving their goal. To avoid such fraudulent attacks, the user should avoid clicking on links or attachments sent in emails from unknown or unexpected sources, and 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. In general, there are signs that distinguish fraudulent e-mail messages; **the following is an explanation of the most important ones:**

- The messages contain exaggerated kindness.
- Messages invite the user to click on a link to update their account details.
- Many spelling and grammatical mistakes in mail messages.

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:

- **Use security software to protect computers,** while setting automatic updates for programs and applications to be able to confront cyber threats.
- **Set a password for the smartphone,** and set automatic software update on it.
- **Use two-factor authentication to provide additional security for accounts,** whether by passwords, answering a question, or fingerprint and face.
- **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].

[1] How to Recognize and Avoid Phishing Scams. On site: https://cutt.us/0VwNx

Second: Protecting data from hacking

With the increase in security breaches of electronic devices in the world and the theft of data and accounts, the need to provide security for them has increased. Methods of protecting data from theft can be summarized as follows:

- Use anti-virus software, as it represents the first line of defense against fraudulent attacks, as it protects devices from intrusion and deals with malware that attackers hack to access data and files.
- Activate two-factor authentication, as it is the best way to protect accounts from unauthorized access and data theft, whether this is done using codes, fingerprint and face, or by answering questions. All of these things make the hacking process difficult.
- 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, as these gaps provide the gateway for hackers to enter the devices and then to the accounts and files stored on the devices.
- 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. Cloud computing can be used here, but it is also preferable to keep another copy in another place.
- 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[1].

[1] 18 Ways to protect your data from hackers. On site: https://cutt.us/3M0uz

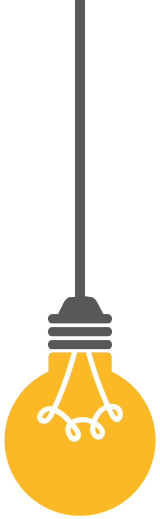
Third: What do I do if I get phished?

In the event of exposure to phishing, one of the following procedures can be taken, and one can resort to a number of authorities that can provide assistance in this area. **The following is an explanation of the most important of these procedures:**

- 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.
- 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.
- 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.
- It is necessary to update its operating systems, reset all passwords, activate two-factor authentication, scan the device, and start the installation again.
- 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.
- 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.
- 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.
- It is preferable to communicate 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[1].

[1] What to Do If You Give Your Personal Information to a Phisher. On site: https://cutt.us/axv7k

Exercises and trainings



Exercises are a major part of the training process, and they achieve several goals and aims, as follow:

- Exercises are an effective tool to assess students' utilization of the training content and its impact on their cognitive inventory.
- They serve as a vital means to reinforce information and knowledge, constituting a rapid review of the training content.
- They help to identify knowledge gaps among students.
- They act as a form of feedback for the trainer, providing information on the effectiveness of the training kit and the training method.

Approach to Dealing with Exercises:

The exercises mentioned in this section are comprehensive of the training content in this kit, here's an outline of the proposed methodology for dealing with them:

- During the training, after introducing an idea, the trainer will request students to open their respective booklet and answer the specific question, directly related to the presented idea or subject.
- The exercises are carefully selected to be simple, easily understood, and solvable by middle school students. The trainer may offer support to students in answering some exercises if necessary, at their discretion.
- The exercises are divided into two parts; one for in-classroom use, called classroom exercises, and another is non-classroom, to be completed at home by the students.
- The answers for each exercise are provided, highlighted in a different color.

Below is an explanation of exercises specific to Middle school students, arranged according to chapters and classified as in-classroom and homework exercises (Non-classroom Exercises). These exercises, in the form presented here, are the same as those in the students' booklet.

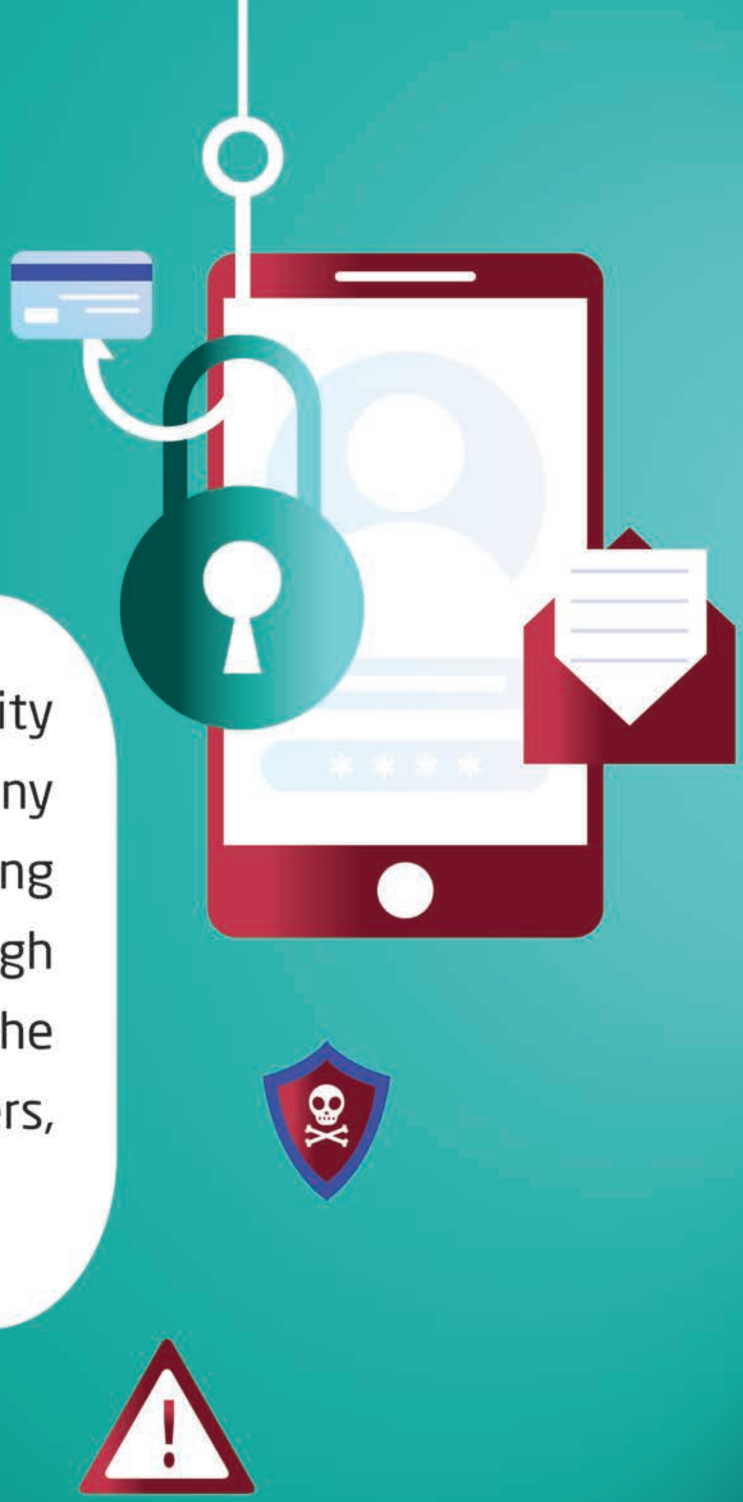
First:

in-classroom Exercises

The exercises here are accompanied by the answers, while in the student's booklet they are written without a solution, and are accompanied by guidance for the student on how to solve, when necessary.

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...?

Vishing is one of the types of phishing attacks, carried out via telephone calls with the intent of obtaining victims' money or other personal information.

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

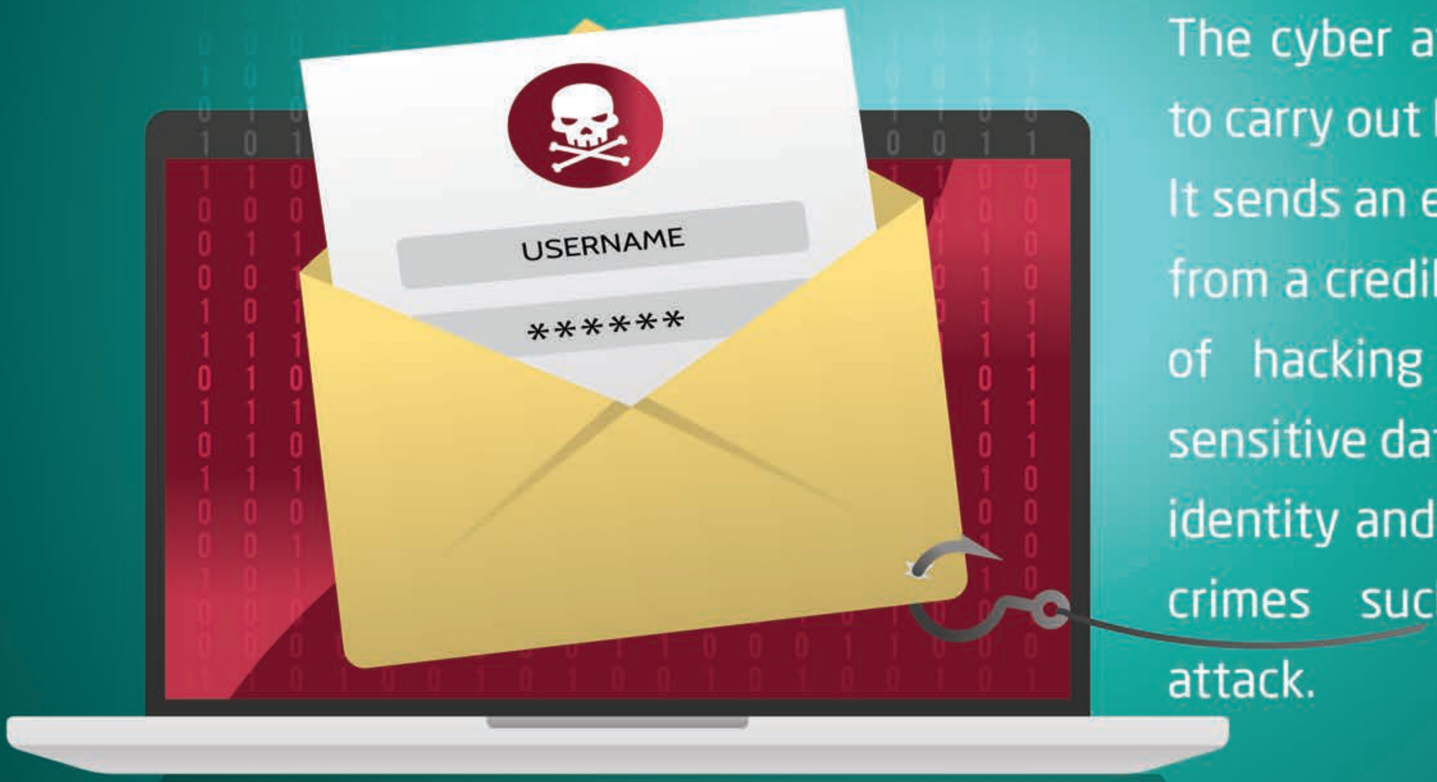
Determine what is **true** and **false** about phishing.

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.	fasle
Phishing depends on revealing confidential information, which includes credit card numbers, passwords, and banking information.	true
Sometimes websites carry out phishing frauds.	true
A phishing attacker does not impersonate a friend or family member.	fasle
Fake messages are used in phishing frauds.	true
Suspicious links are one of the most prominent methods of phishing.	true
Phishing criminals cannot take advantage of bank information or credit card numbers.	fasle
Phishing criminals don’t care about identity.	fasle
You cannot protect yourself from phishing no matter how hard you try.	fasle

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!

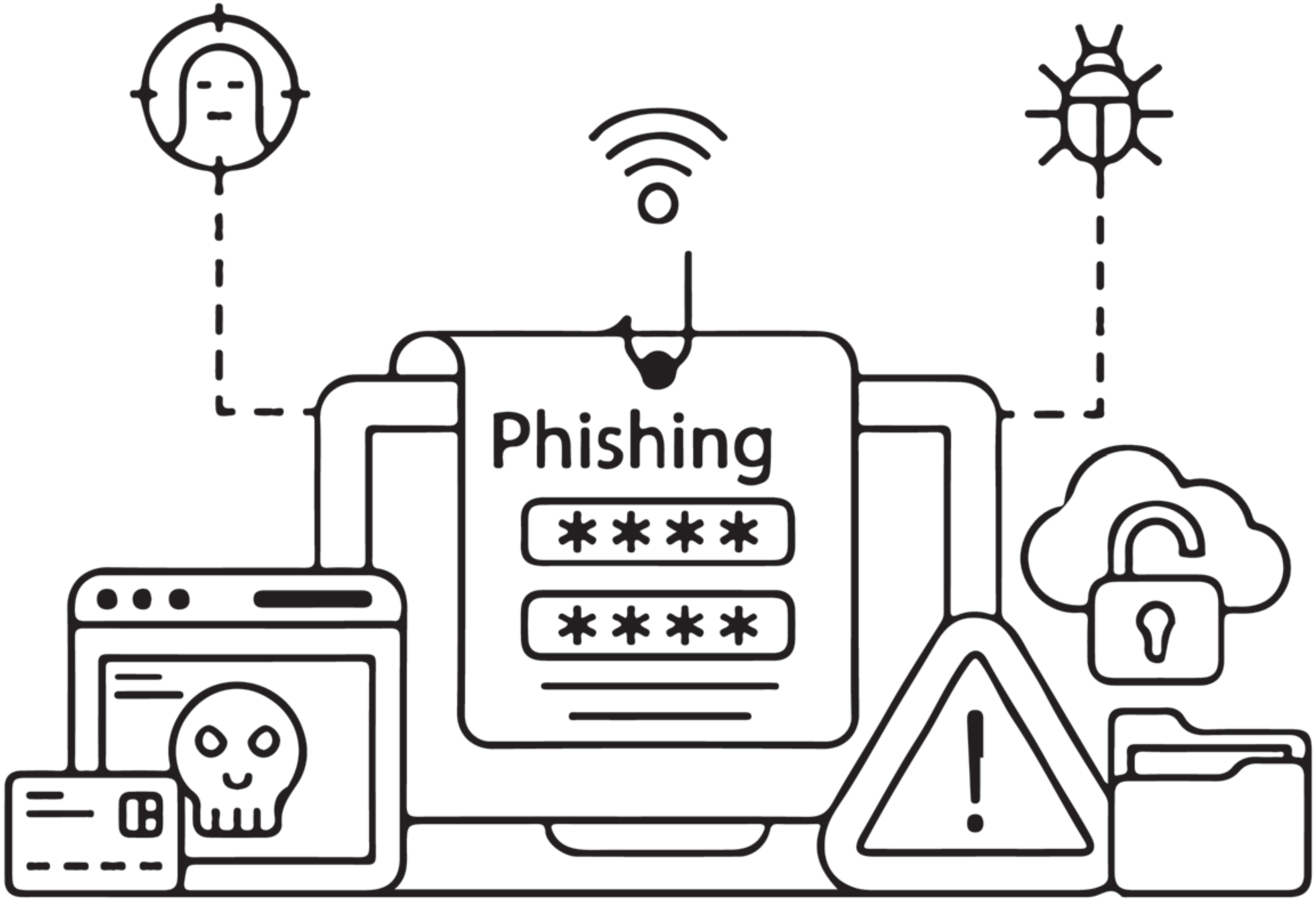
Email phishing

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	**Virus software**
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.	**Spear phishing**
SMS messages are used disguised as trademarks or large, trusted websites to deceive the user into opening the link or text sent.	**Phishing via SMS**
Voice is used to push the victim to provide sensitive and personal information over the phone by impersonating personalities close to the victims.	**Vishing**


Phishing
****
****

Do you know that...?

Spear phishing attacks are targeted, large-scale campaigns aimed at accessing sensitive user data.

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

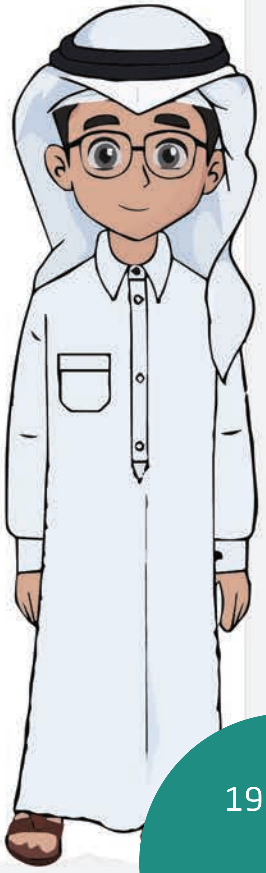
Complete the following sentences:

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

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

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

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



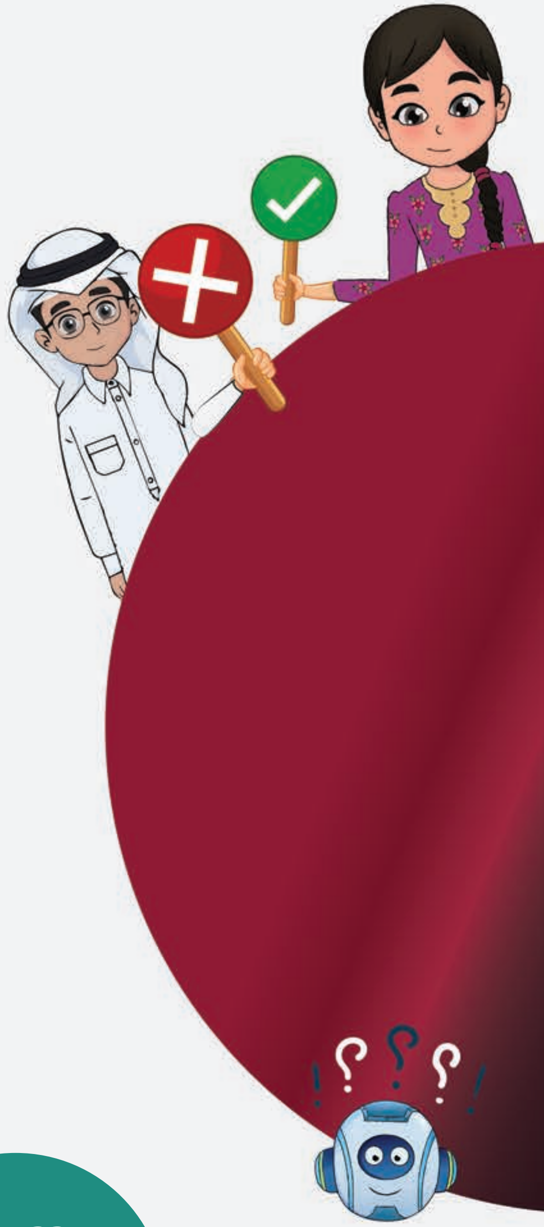
Exercise 4

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

1. 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.
2. Stop all types of communications with this scammer who tried to deceive you.
3. If bank account or credit card data is stolen, contact the bank immediately to stop any transactions on your account.
4. Go immediately to the Cybercrime Unit to report what happened to you, especially in the case of the theft of money.
5. If the phishing is through a job advertisement, you must immediately report the suspicious advertisement.
6. 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.
7. Write posts explaining how you were exposed to phishing; So that no one else falls into the same trap.

Exercise 5

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



1. Opening 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.	True
Download apps from app stores.	True
Talking on the phone.	Fasle
Registration in general bulletins.	True
Go for a walk.	Fasle
Buying and selling stocks.	Fasle
Subscription to electronic journals.	True
Opening a bank account.	Fasle
Social media posts.	True
Watching television programs.	Fasle
Share information and photos with friends.	True
Republish the articles and information you read.	True
Subscribe to health blogs.	True
Publishing videos via social media platforms.	True

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:

Read the words below carefully, and search in the table for consecutive letters that form these words.

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?

The answer is considered correct if the student mentions information about the need to confirm who sent the message, and not to open the message if there is suspicion that it is fake, in addition to mentioning information about ignoring questionable messages and not opening them.

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?

If the student answers that he knows someone who has been exposed to attack, to a phishing attack, his answer is considered correct if he mentions information about how to act correctly, including stopping communication with the scammer, informing the bank or institution whose name is being exploited, informing the official authorities responsible for cybercrimes, or any information intersect directly or indirectly with this information.

01001110
01110100
0111011101
1111000010110

Exercise 4

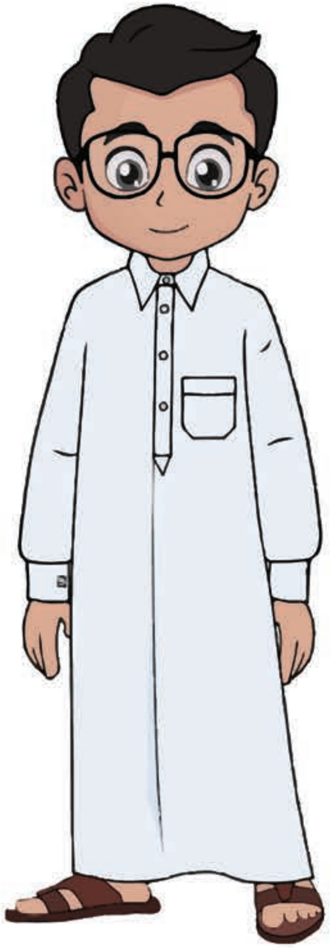
Mark (✓) or (✗) in front of the following phrases:

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:

1. Do not share your personal data with any party.
2. Do not access suspicious websites or links.
3. Make sure to update your device's drivers.
4. Make sure to install anti-virus software.
5. Contact the official authorities responsible for cybercrimes if you are exposed to a phishing or electronic fraud.



Exercise 6

Define the following terms:

Social engineering A modern technology that relies on natural human instincts such as trust or fear...and other feelings that cyber attackers exploit to influence victims to push them to make a specific decision that leads to achieving the attacker's goal, such as stealing money or sensitive information.

Password A set of letters and symbols that are used to protect e-mail, bank accounts, and social media so that no one other than the owner of these accounts is allowed to use them or view their content.

Phishing One of the most common types of digital crimes. In this type, the Internet is exploited to deceive targeted victims by stealing their personal data, such as passwords and credit card numbers, through several methods and tools, including creating a fake website to lure the victim; Sending the link via e-mail or messenger messages to click on, thus allowing hackers, without the user's knowledge, to illegally enter the victims' accounts and devices and install malware that help them steal data.

Digital fingerprint data path left by the user when using the Internet, such as the websites visited, emails shopping, conversations (chats)... and all the movements that the user makes through his various accounts, regardless of whether those movements are 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, photos, etc.

Cyber fraud Cyber attackers masquerade as a known entity, such as a well-known, reputable company or 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 victim's data, such as login credentials, bank account numbers, or personal family or work information.

Goals of phishing attacks

1. Stealing information or money from targeted users.

2. Installing malware on targeted users' devices.

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

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

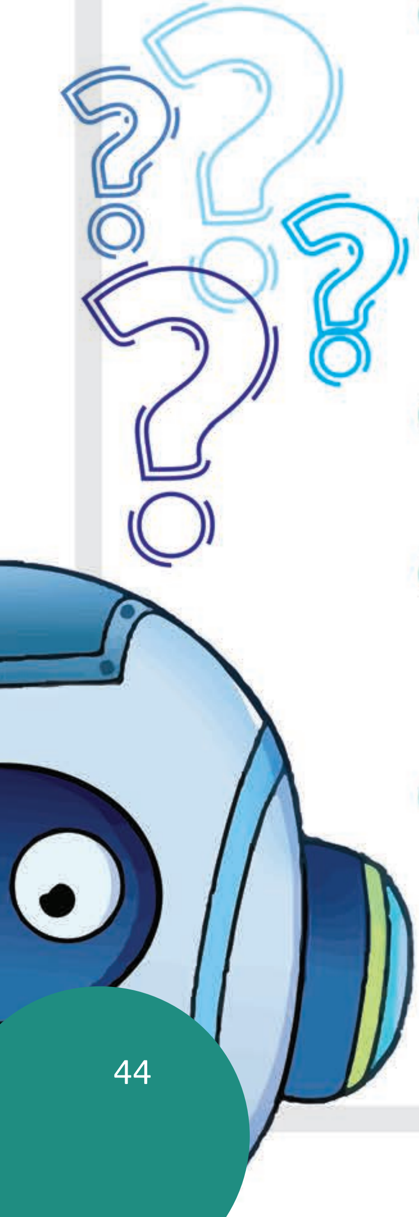
It is a cyber attack that deceives targets into connecting to a fake Wi-Fi network that looks like the real one, and when it comes to connect, the attacker begins to hack the victims' devices to steal all their data and files.

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?



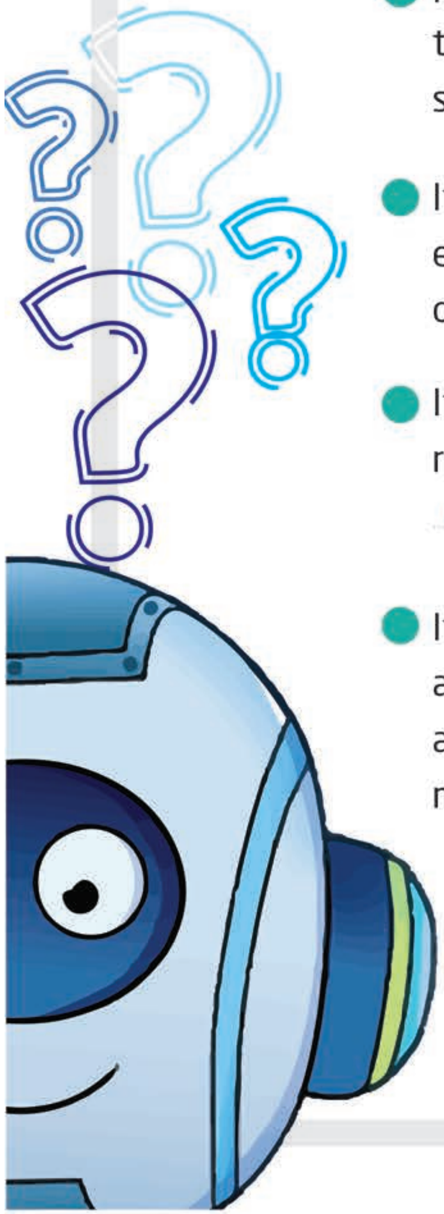
- It is an attack that cyber attackers masquerade as a known entity or a reputable person in an email or any other form of communication. **Phishing**

- It is a fraudulent attack targeting an individual within a specific institution. With the aim of stealing his login credentials. **Spear Phishing**

- 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. **Vishing**

- 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. **HTTPS Phishing**

- 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.. **Pop-up 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. .... **Evil twin phishing** ....

- 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. .... **Whaling** ....

- 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. **Clone Phishing** ....

- 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. .... **Deceptive Phishing** ....

Complete the following sentences:

- ....**Phishing**........ is one of the most widespread cybercrimes in the world.

- In phishing, artificial intelligence can be used to innovate ....**voice**........ 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 ....**Spelling and grammatical mistakes**........ in them.

- The goal of phishing attacks is to steal ....**information**.... or ....**money**........ from the targeted users, and ....**installing malware**........ on users' devices, and pushing the victim to log into ....**a fake website**........ on the Internet.

- One of the ways for cyber attackers to hack targeted users' devices is to send **fake text messages or emails** containing ....**links**........ that include ....**malware**........ When clicking on it........**hackers**........ are allowed to crawl your computer.

- Receiving email notifications about **attempts to log in to your accounts** even though the user has not done, the **slow** device, and the high **overheating** , and the delay in the commands received from the user.

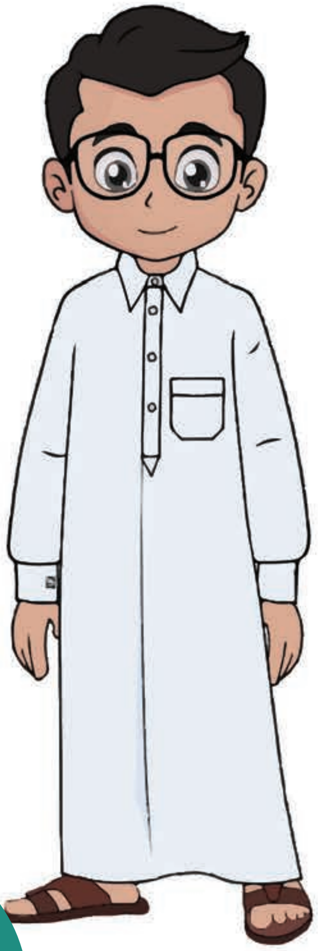
- The appearance of **pop-up windows** containing annoying messages claiming that your electronic device is infected with viruses is one of the signs that the device is exposed to hacking.

- Among the mistakes that Internet users commit are: browsing on the **Public Wi-Fi** network, and not updating **browser** and **apps** on devices, in addition to sharing a lot of **personal information** on social media.

- **digital fingerprint** is data path left by the user when using the Internet.

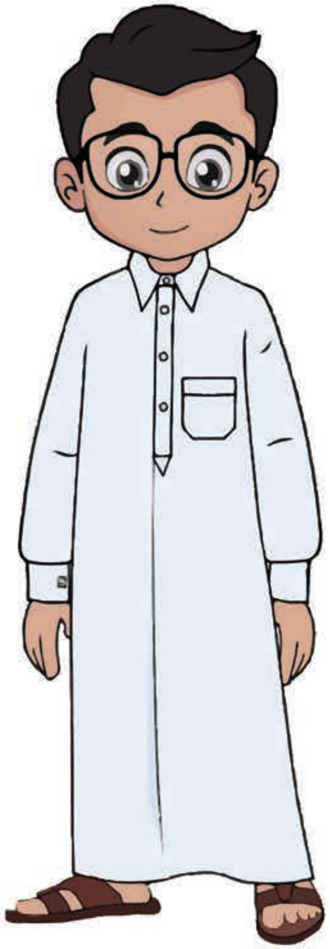
- One of the ways to protect data from hacking: using **Digital footprint** It represents the first line of defense against fraudulent attacks.

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



1- 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

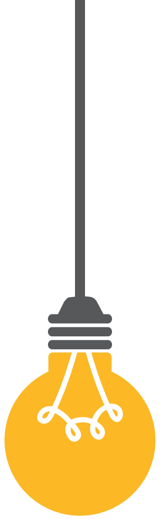
- Phishing attacks are highly targeted attacks that target a specific victim. ✗
- Spear phishing attacks take more time and effort to execute. ✓
- Spear phishing attacks are widespread attacks targeting sensitive data of users in general. ✗

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 dealt with the 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.

References



1. 10 mistakes people make online. On site: https://cutt.us/4XQ7A
2. 10 Most Common Signs of a Phishing Email. On site: https://cutt.us/MJiQZ
3. 18 Ways to protect your data from hackers. On site: https://cutt.us/3M0uz
4. digital footprint. On site: https://cutt.us/P2gI8
5. How Does Clone Phishing Work? On site: https://cutt.us/x7Gwg
6. How to protect your digital footprint. On site: https://cutt.us/0ksRZ
7. How to Recognize and Avoid Phishing Scams. On site: https://cutt.us/0VwNx
8. HTTPS Phishing Attacks: How Hackers Use SSL Certificates to Feign Trust. On site: https://cutt.us/20AV8
9. Importance of Digital Footprint: Complete Guide [2023]. On site: https://cutt.us/DCq7d
10. Phishing, Alexander S. Gillis, Technical Writer and Editor. On site: https://cutt.us/5jBhs
11. Scam Alert: What You Need to Know About Pop-Up Phishing. Onsite:https://cutt.us/3pHtA
12. Vishing – a growing threat. On site: https://cutt.us/q3aSU
13. Warning signs you've been hacked and what to do next. On site: https://cutt.us/rd84U
14. Whaling: how it works, and what your organization can do about it. On site: https://cutt.us/H9RNo
15. What is a digital footprint? And how to protect it from hackers. On site: https://cutt.us/bObsJ
16. What is an Evil Twin Attack? On site: https://cutt.us/jsBji
17. What Is Pharming and How to Protect Yourself. On site: https://cutt.us/BGtUI
18. What Is Phishing? On site: https://cutt.us/PbZ3Y
19. What is spear phishing? Definition and risks. On site: https://cutt.us/riHDD
20. What to Do If You Give Your Personal Information to a Phisher. On site: https://cutt.us/axv7k
21. Which 7 Online Mistakes Will You Make Today? On site: https://cutt.us/z25Nk

CyberEco

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency