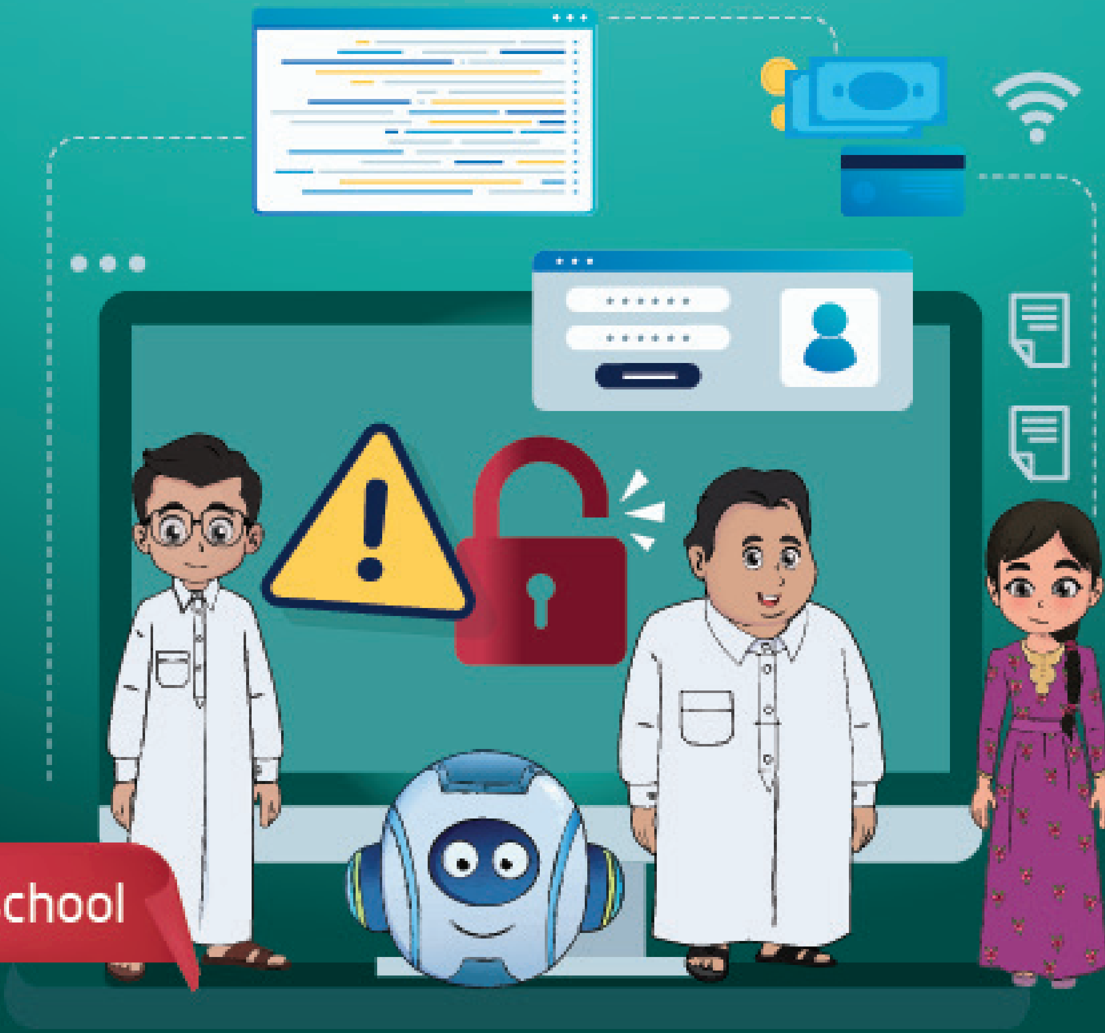
Forgery and online fraud

Presentation Slides

Training Kit

CyberEco

معًا لدعم السلامة الرقمية
Together to support digital safety



Middle School

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

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

Content of The Training Kit

Time Table for the Lecture

Content	Allocated Time
General introduction	5 minutes
The theoretical aspect	25 minutes
View Educational Videos	25 minutes
Short break	20 minutes
Implementation of Training games	25 minutes
Dialogue and discussion with students	15 minutes
Graduation project	5 minutes
Workshop duration	2 hours

Chapter One
The Concept of Forgery and Online Fraud and Its Types

First:

The Concept of Online Fraud

Online fraud

A type of deception and tricks carried out over the internet, often occurring in chat rooms, via e-mail, on forums or websites (the web). The goal of these crimes is to defraud customers and users by stealing money, important personal information, and other purposes.

Information fraud:

A concept related to the concept of online fraud, and it means deception or fraudulent manipulation of information processing systems, with the intention of wrongfully gaining access to services, money, or specific assets.

Online fraud or scam:

Seizing others' money through deceitful means, often involving the use of computers.

Second: Reasons for falling victim to online fraud

1. Lack of awareness about using social media and internet platforms.

2. Misuse of internet websites and access to unsafe websites.

3. Sharing personal information on social media and online platforms.

4. Weakness of electronic systems of enterprises and companies.

5. Fake online stores leading to financial losses.

6. Digital fraudulent currencies platforms.

7. Theft of sensitive information about individuals from companies and organizations without the company's management knowledge.

Third

Types and Forms of Online Fraud

E-mail

Among the more deceitful and cunning methods of online fraud is the act of sending a fabricated email that appears to originate from a friend or an official entity, whereas it’s just a phishing attempt.

Smartphone

Installing pirated (hacked) or unidentified applications, as well as clicking on links from unknown source, leads to the compromise of personal data such as images and files.

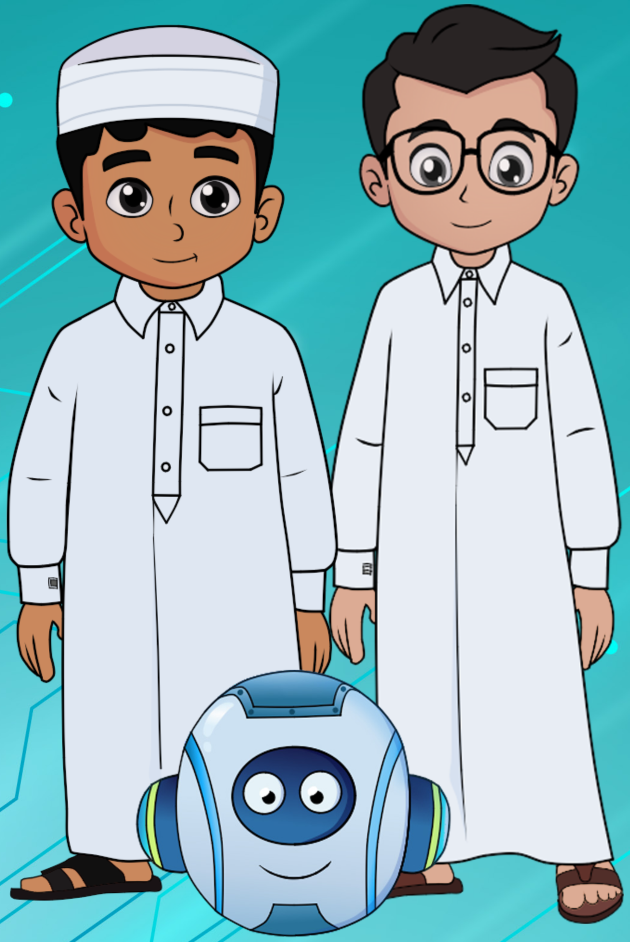
Computer

Hackers and scammers resort to infiltrating the computer using Malware and links, causing shutdowns, and then extorting victims to pay money to regain access.

13844 MAIN ST
PORTCITY
CALIFORNIA 12346
SHOP NAME
Mon 05/04/2018 11:25AM
16-586 Lorem ipsum x 2 $40.56
74-013 Or Sit Amet x 1 $3.99
18-578 Consectetuer x 1 $15.99
TOTAL: $ 90.54
Bank card# **** **** ***** 2345
Response: APPROVED
INV. 5775686 AUTH. 23405
Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh
BUY NOW

E- Commerce

Users can visit a fake website intending to purchase goods, only to become victims of fraud and online scams, paying money without receiving anything in return.



Exploiting Disasters:

During crises such as natural or health disasters like the "COVID-19 pandemic," cybercriminals organizing deceptive campaigns soliciting donations to aid victims. This deceit tricks individuals into disclosing private banking information, a clear instance of online fraud.

Chapter Two

How to Carry Out Online Frauds

First

vulnerabilities that help with online frauds

Definition of Security Bug

A 'Security Bug' is a term referring to vulnerabilities in computer operating systems and software. These weak points allow attackers to infiltrate the operating system, enabling them to modify it, leading to potential outcomes such as complete destruction, spying on the computer owner's private information, or what is known the victim's device.

Zero-Day vulnerability

One of the disadvantages of the electronic system. This describes a defect in software that can be taken advantage of by unauthorized individuals (hackers). Developers may be unaware of this vulnerability, haven’t created a remedy, or have chosen to overlook it. This type of security flaw leads to a critical breach in cybersecurity.

How Zero-Day vulnerabilities attack works

1

Identifying security vulnerabilities.

2

Creating an exploitation code.

3

Search for systems affected by security vulnerabilities

4

Planning the attack.

5

Infiltration.

6

Launch of Zero-Day vulnerabilities.

Non-targeted attacks of Zero-Day vulnerability

Non-targeted zero-day attacks are commonly launched against a large number of home users (ordinary individuals) who use a vulnerable system, such as an operating system or browser. The attacker's primary aim is often to breach these systems and utilize them to build extensive botnets for executing larger cybercrimes later.

Second

Personal Data Security and Online Fraud

Information security

Refers to a set of security measures and tools that widely protect sensitive information from misuse, unauthorized access, or disruption or destruction.

Data Theft

It is the act of stealing digital information stored on computers or mobile devices to obtain confidential information or violate privacy, such as bank account details, internet passwords, passport number, medical records, online subscriptions, etc.

In the realm of the internet, the term used for “theft” is often “data breach” or “data leakage.”

Third: Digital Footprint and Online Fraud

The term “Digital footprint” or “Digital shadow” or Electronic footprint”, refers to the trail of data and information left behind when using the internet. This encompasses the websites visited, the emails sent and received, and the information provided online.

For instance, actions like social media posting, subscribing to newsletters, leaving reviews online, or shopping online all contribute to the “Digital footprint”.

There are two types of digital footprint; active and inactive

Inactive digital footprints

Generated when information is collected about the user without their awareness.

Active digital footprints

Intentionally sharing user information by posting or sharing on social platforms sites or online forums.

The Negative Effects of the Digital Footprint

1

It creates relatively permanent data that becomes available for public or partial access.

2

The digital footprint shapes individuals' online reputations, similar to what occurs in real life.

3

Words and images published by an individual online can be misinterpreted or altered, causing unintended offense.

4

Content intended for a specific group can spread beyond it, potentially damaging relationships between individuals.

5

Cybercriminals can exploit your digital footprint for purposes such as identity theft, accessing accounts, or creating fake identities using your personal data to deceive others.

Examples of Digital Footprint

Among the ways users contribute to their digital footprint are:

- Online shopping.
- Register to create an account on a specific website.
- Downloading and using applications.
- Signing up for newsletters from brands.
- Online banking services.
- Subscribing to printed and blogs.
- Using social media on your devices.
- Logging into other websites using social media credentials.
- Communicating with friends and contacts online.
- Sharing information, data, and images with acquaintances.
- Subscribing to online news sources.

Digital Footprint Protection

- Using search engines to verify the digital footprint.
- Reduce the number of information sources, for example, Websites may contain more information than one wants to display, such as phone numbers, address, and age, so users should remove personal information from them.
- Restricting the amount of data shared online.
- Check the privacy settings.
- Avoid over-sharing on social media.
- Avoid unsafe websites.
- Non-disclosure of private data on public Wi-Fi network.
- Deleting our old online accounts

- Creating strong passwords and using a Password Manager.
- Avoiding logging into websites and applications using Facebook credentials.
- Regularly update programs.
- Reviewing mobile phone usage by setting a device passcode.
- Thinking twice before posting.
- Act quickly after a data breach.

Chapter Three

How to React When Exposed to Online Fraud

First: Guidelines for protecting against online fraud

1. Downloading applications from well-known app stores.

2. Regularly updating the phone.

3. Avoiding unknown source links.

4. Be cautious about transactions involving third parties.

5. Employing anti-virus software.

6. Use strong passwords and change them regularly.

7. Refraining from shopping on unfamiliar websites.

Second: Data protection against online fraud

- Be vigilant for fraudulent activities when you are dealing with intrusive communications.
- If you’ve only met someone online, take the time to do additional research about them.
- Do not open suspicious texts, pop-up windows, or emails.
- Secure your personal details, such as putting a lock on your mailbox.
- Keep your phone and computer secure by using a strong password, constantly updating operating systems, and maintaining a backup copy of content.
- Secure your Wi-Fi network with a password.
- Review your privacy and security settings on social media platforms.
- Be cautious about any requests for your details or money.
- Beware of any requests regarding your details or money.

- Be careful when shopping online, especially with overly enticing offers.
- Change your online passwords if you suspect your computer or phone has been hacked.
- Bookmark essential websites you frequently visit.
- Remember that legitimate error messages from Microsoft or other major tech companies will never include phone numbers for you to call.
- Remember: Microsoft and other legitimate tech companies will never call you to inform you of a problem with your device.
- If your screen suddenly fills with scary pop-ups windows, immediately shut down your computer.

Third: How to React When Exposed to Online Fraud

- **First:** Do not engage with the scammer.

- **Second:** Close all active accounts upon receiving a warning message or if you suspect any of your accounts have been compromised, or upon receiving a threatening and extortionate message from an unknown source. Also, turn off the devices.

- **Third:** Retain the message sent, as it serves as evidence incriminating the intruder.

- **Fourth:** Report to a trusted individual, such as parents or a school authority.

- **Fifth:** Do not comply with the intruder; they are skilled at intimidating others. Do not succumb to their demands, such as sending money, as happens in ransomware attacks.

- **Sixth:** Do not believe what the intruder says and do not let them manipulate your emotions.

- **Seventh:** Provide any information or specific details about the intruder or any messages received to trusted individuals who can then pass it on to the department of cybercrime control at the ministry of Interior.

Examples of the most famous online frauds

First Example
Toyota Boshoku Company

In 2019, “Toyota Boshoku,” a company involved in supplying Toyota cars and providing some equipment, fell victim to an online fraud operation amounting to approximately 37 million USD. Online fraudsters convinced the company’s financial director to change the recipient’s bank account information, enabling them to obtain these funds.

Second Example

Digital Currencies

In 2017, many people lost thousands of dollars after losing digital currencies, specifically “Ethereum.” Hackers breached the currency wallets and transferred them to their own servers. Also in the same year (2017), the “WannaCry” virus, a ransomware attack, disrupted computers. To regain access, the hackers demanded a sum of money in (Bitcoin) to avoid detection and escape punishment.

BITCOIN · DECENTRALIZED DIGITAL CURRENCY · BITCOIN · DECENTRALIZED DIGITAL CURRENCY · BITCOIN · DECENTRALIZED DIGITAL CURRENCY ·

CyberEco

Third Example
Yahoo Inc

During the period between 2013 and 2016, Yahoo suffered a data breach affecting about 3 billion users. The intruders gained access to information and passwords that could be used to access other online services and accounts.

Fourth Example

Money Theft in Russia

In Russia between 2013 and 2014, one of the most prominent online fraud methods, where a fraudster contacts his victim, impersonates an employee of the victim's bank, and asks him for information related to the debit card, under the pretext of stopping suspicious financial transactions. After obtaining the card information, the fraudster used it to steal and transfer funds to their accounts.

BITCOIN · DECENTRALIZED DIGITAL CURRENCY · BITCOIN · DECENTRALIZED DIGITAL CURRENCY · BITCOIN · DECENTRALIZED DIGITAL CURRENCY

Fifth Example

$600 Million Theft in a Massive Cryptocurrency Fraud Operation

Cyber pirates stole approximately 600 million dollars, marking one of the biggest fraud operations in the history of digital currencies. They exploited a security flaw in the currency system to pilfer funds belonging to tens of thousands of cryptocurrency community members.

Exercises and training

pay attention!

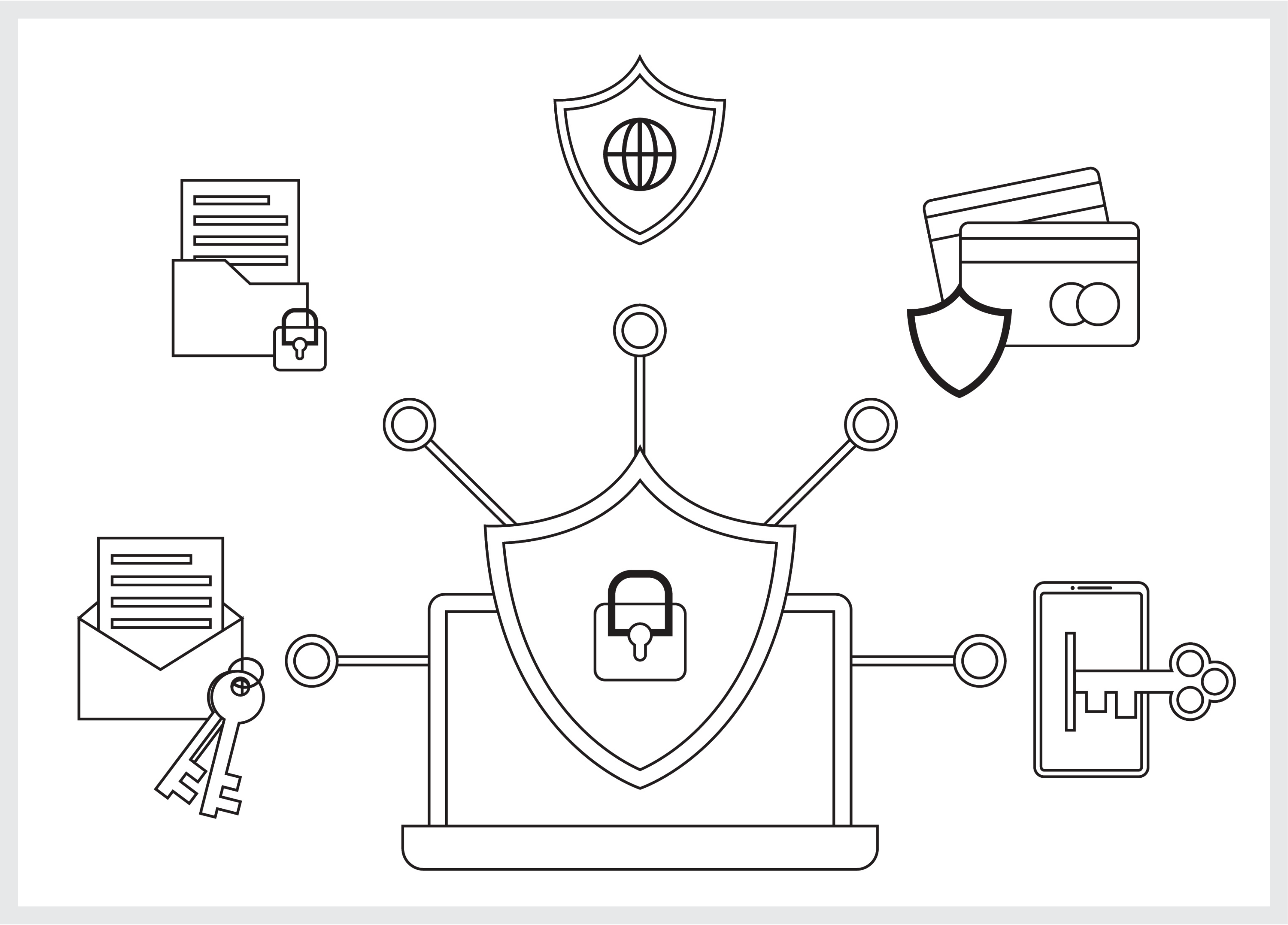
Online fraud

A type of deception and tricks carried out over the internet, often occurring in chat rooms, via e-mail, on forums or websites (the web). The goal of these crimes is to defraud customers and users by stealing money, important personal information, and other purposes.

First: In-Class Exercises

Do you know that...?

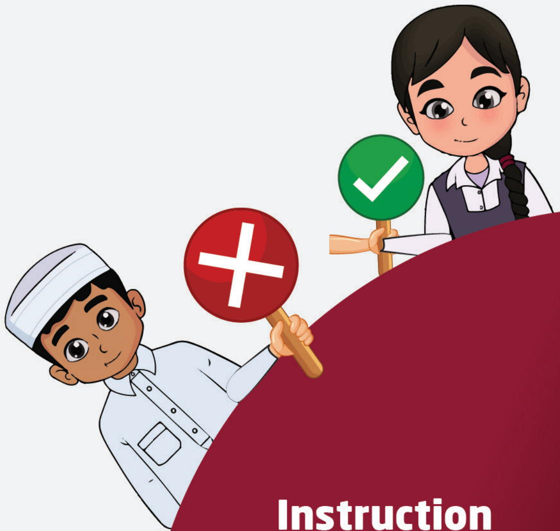
The majority of prizes and gifts received online for no reason are the beginning of an online fraud process.



Exercise 1

Mark (✓) next to the correct statement,

and (✗) next to the incorrect statement



Instruction

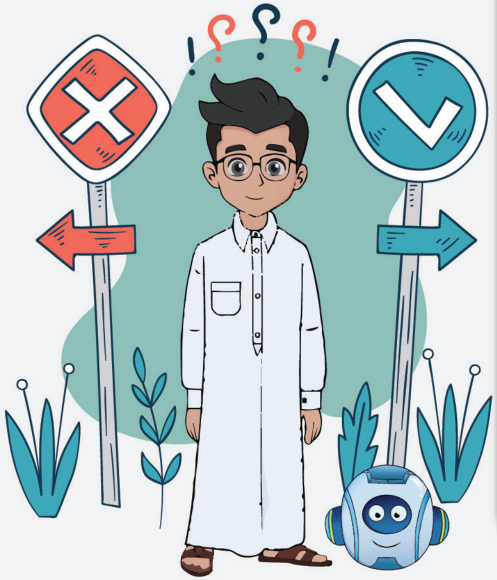
Read the sentences below carefully, then determine whether the sentence is true or false. An example provided below.

1 Online fraud is a deliberate manipulation of information and data on the computer. ✓

2 Online fraud is the authorized access in order to obtain information and data on the computer. ○

3 Unauthorized access to devices or systems to gain illegal profit or cause harm is a type of online fraud. ○

4 Modern technology assists online fraud perpetrators in committing crimes only on a local scale. ○



5 Online fraud is the use of authorized systems and devices to deceive others. ○

6 Information fraud involves cheating and deceiving by manipulating information processing systems unjustly, to obtain services, money, or assets. ○

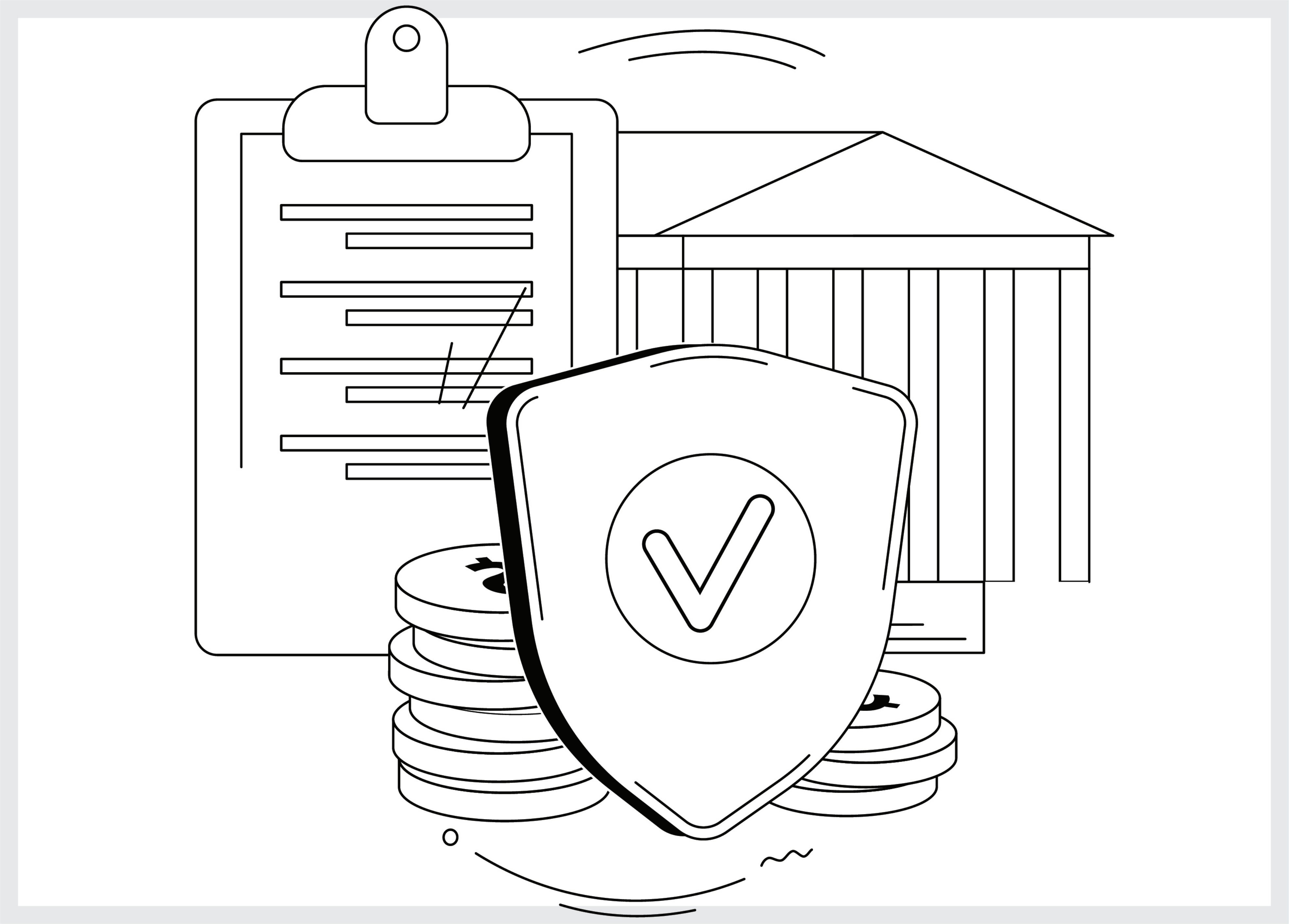
7 Online fraud is gaining money through illegal means only from outside the country. ○

8 Criminals in online fraud use technologies in a legitimate way and without any manipulation. ○

pay attention!

Cyber Fraud

Seizing others' money through deceitful means, often involving the use of computers.



Do you know that...?

Your digital footprint defines your online reputation, much like in real life.

Exercise 2

Match the terms from column (A) with their corresponding from column (B):

Column (A)

- SMS fraud ○
- Ad fraud ○
- Ransomware viruses ○
- Traditional online fraud ○
- Voice fraud ○
- Online shopping fraud ○
- Fundraising fraud ○
- Shopping fraud ○

Column (B)

- ● A type of cyber fraud in which the victim is threatened with data destruction or payment of a ransom.
- ● It relies on deceiving others through voice alteration software to convince victims to share personal data and information.
- ● It occurs during the victim's shopping experience, where after paying for a product, they either receive nothing, or they might receive a wrong or counterfeit product.
- ● It exploits fake charitable organizations' names to obtain money by eliciting sympathy from others.
- ● A link is sent via text message, and once clicked, the fraud is initiated.
- ● It deceives the seller into thinking that the buyer has made the payment, but after sending the product, the money is not added to their balance.
- ● It involves purchasing credit card data and using it to buy products online.
- ● Malicious ads loaded with viruses are used to steal information and data.

Exercise 3

Complete the sentences with the appropriate words:

Instructions:

Carefully read the sentences below and choose the suitable words to fill in the blanks, making the sentence meaningful. An example provided below:

1 Identity theft is considered the most dangerous form of online fraud; where the criminal steals personal ...**data**..., such as name, date of ...**birth**..., address, **banking** account details, and all other important information.

2 This information is used to steal .... and the identity can be exploited to open a bank.. obtain .... cards or loans, or to register .... lines.

3 Online fraud criminals can steal personal .... to take over existing bank ... accounts.................................... of the person by using their personal ....

4 It is essential to avoid giving any personal .... to others, and you must delete any document or file containing confidentia .... or .... card numbers before disposing of it.

5 Ask your bank to send you a notification or .... you in case there is any suspicion of unusual or unauthorized transaction on your bank ....

6 You must be very careful in your dealings with commercial .... , or with others, whether through the phone or .... , or the Internet in general, especially .... platforms.

7 Avoid opening any suspicious .... , and disable pop-up .... Ensure the authenticity of the .... of the person you are communicating with online.

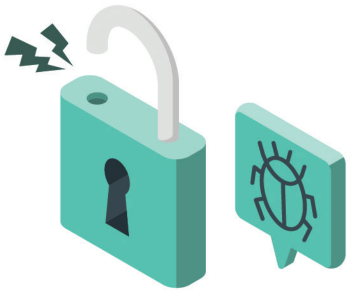
8 Use a strong ....for your phone and personal accounts, do not share it with others, and remember to keep ....of your data. Avoid using public....................................networks, especially when accessing any banking-related applications.

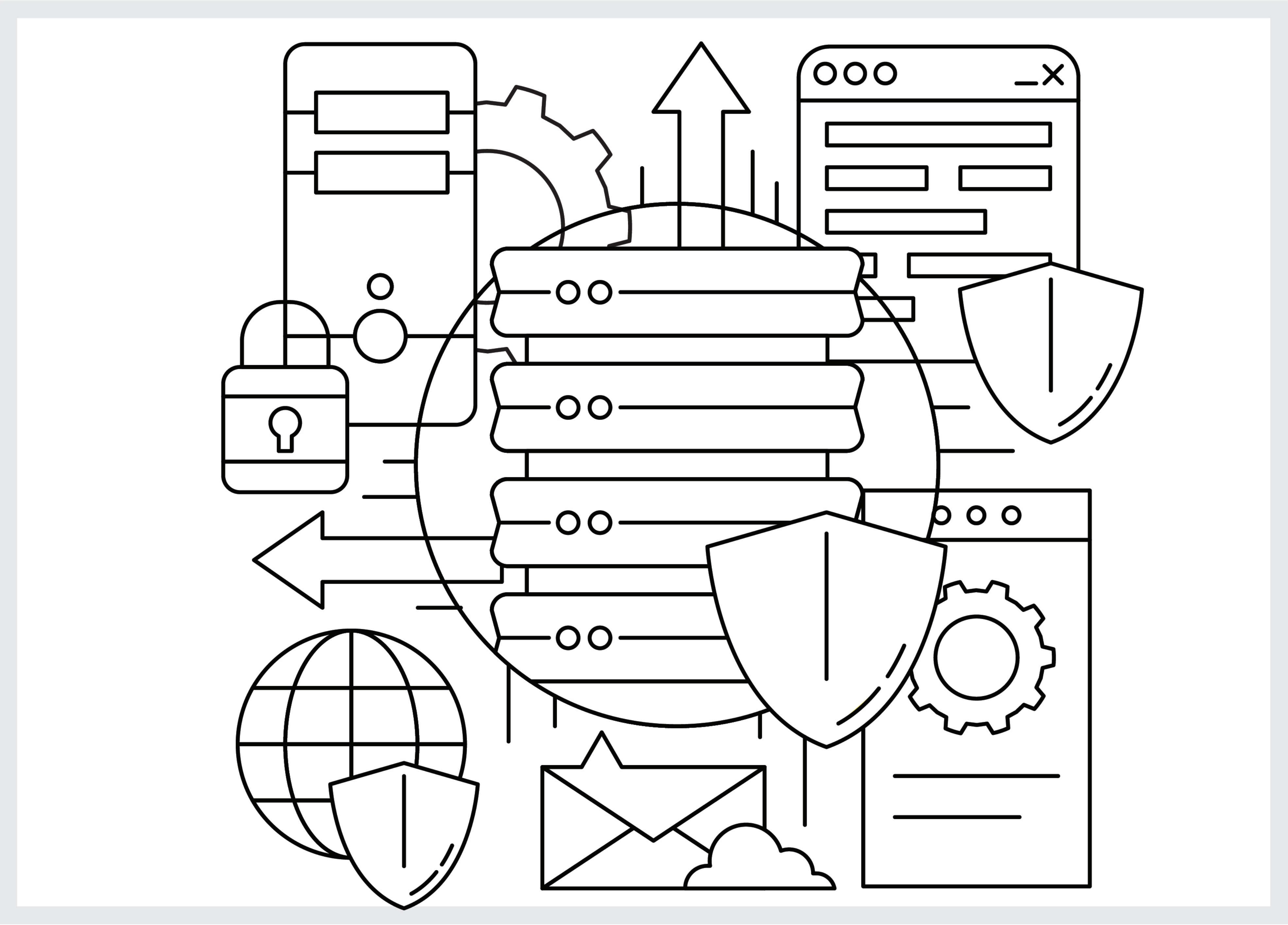
9 If you want to shop .... , you need to make sure that the store is trustworthy, read reviews and ratings from others, and it's better to deal with well-known and secure stores.

pay attention!

Information fraud

Deception or fraudulent manipulation of information processing systems, with the intention of wrongfully gaining access to services, money, or specific assets.





Exercise 4

Put the word (true) or (false) in front of the phrases that are essential for protection against online fraud crimes:

Instructions:

Carefully read the sentences in the table and determine whether the sentences represent accurate information or misinformation in the field of online fraud protection. If the sentence is correct, place the word (true) next to it, if it's incorrect, place the word (false). An example provided below.

1	It is necessary to use legal versions of banking applications.	**True**
2	You can download applications from any website.	
3	You should not disclose your confidential information or personal details during phone calls.	
4	It's okay to click on any links sent by friends, whether in text messages or through email.	
5	Using a third party in financial transactions may expose you to fraud or money laundering.	

6 Using antivirus software is an essential factor in protecting yourself from online fraud.

7 You can repeat your name or using your date of birth as a strong password for your accounts and devices.

8 You should be careful when shopping online, and it is preferable to deal with well-known websites.

9 Writing your banking card details on any electronic shopping application is acceptable.

10 Avoid using modified or pirated (hacked) versions of smartphone applications.

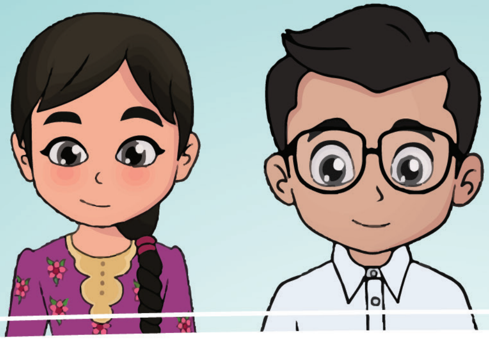
pay attention!

Reasons for falling victim to online fraud

- Lack of awareness about using social media and internet platforms.
- Accessing unsafe websites.
- Sharing personal information on social media and online platforms.
- Dealing with fake online stores.
- Impersonation of well-known personalities such as government employees, experts, executives, or technicians by hackers.
- Exploiting of emotions like during emergencies to attract the sympathy of targeted victims online.

Exercise 5

Place the appropriate word in front of each sentence:



Instructions:

Carefully read the sentences in the table, think of a word or phrase that expresses the meaning of the sentence. And write it in the second column, an example provided below.

• The impact you leave behind and the information you leave behind after each use of the internet.	**Digital footprint**
• Fraud and data theft using technology and the internet.	
• Programs that help you protect your devices and fend off fraudulent attacks.	
• A set of letters, symbols, and numbers used to secure your accounts.	
• Using an intermediary to transfer money from one party to another.	

pay attention!

Security Bug

A 'Security Bug' is a term referring to vulnerabilities in computer operating systems and software. These weak points allow attackers to infiltrate the operating system, enabling them to modify it, leading to potential outcomes such as complete destruction, spying on the computer owner's private information, or accessing the victim's device.

Second:
Non-classroom Exercises

pay attention!

The Zero-Day loophole

This type of security vulnerability is present in computer programs and can be exploited by hackers; these security vulnerabilities pose a high level of risk to cybersecurity.

Exercise 1:

Extract the following words from the table:

Instructions:

Carefully read the words listed below and search the table for consecutive letters that form these words. Below is an example for the word "Thieve" and how its letters were found in the table:

h	a	r	m	~~s~~	~~c~~	~~a~~	~~m~~	b	n	e	t
i	n	s	t	r	u	c	t	i	o	n	s
r	f	c	h	w	l	h	s	l	o	c	c
i	r	r	t	o	i	a	e	e	r	h	r
g	a	i	t	r	e	r	c	g	d	e	i
h	u	m	p	k	s	m	u	a	e	a	m
t	d	e	d	a	t	a	r	l	r	t	i
p	r	i	v	a	c	y	e	j	s	i	n
d	c	c	e	p	t	i	o	n	n	n	a
b	n	n	k	r	u	p	t	c	y	g	l
m	n	n	i	p	u	l	a	t	i	o	n
t	c	c	h	n	o	l	o	g	y	t	i

Fraud - ~~Scam~~ - Manipulation - Data - Instructions - Orders - Technology - Harm - Http

Criminal - Crime - Deception - Cheating - Bankruptcy - Right - Work - Privacy - Secure - Legal - Lie - net

Exercise 2

Determine the correct and incorrect statements:

Instructions:

Read the sentences below carefully, and think carefully about whether the sentences are correct or incorrect. An example provided below.

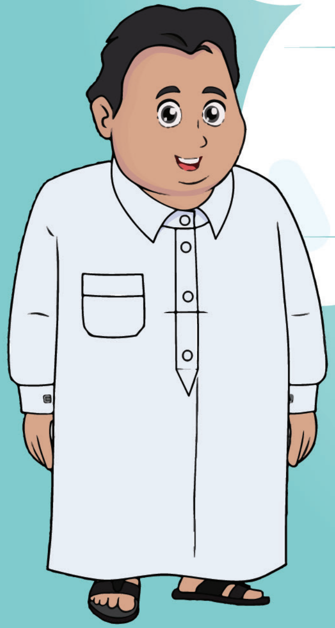
1 Online fraudsters exploit people’s trust to steal their money and data. **Correct**

2 Cybercriminals study the victim to know their weaknesses; to gain trust before committing their crime.

3 Large companies are never exposed to any form of online fraud crimes.

4 Online fraud crimes cannot enter into any other areas other than stealing money and data.

5 Online fraudsters seek only to obtain money.

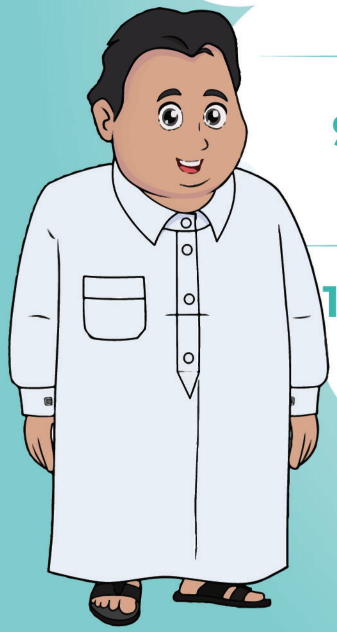


6 Using illegal applications helps online fraudsters.

7 Applications can be downloaded from any website on the Internet without fear.

8 It is okay to share confidential data and information with others over the phone.

9 You do not need to use antivirus software.



10 Use numbers 1 to 8 as the password for your accounts and devices.

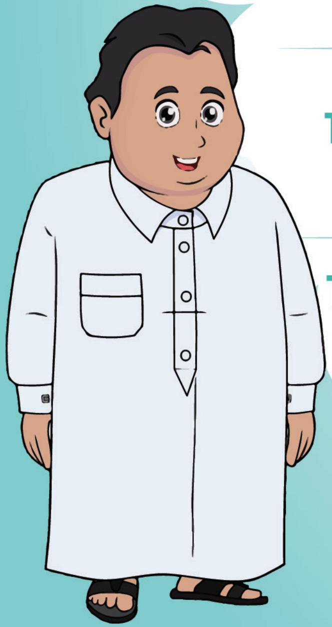
11 You can shop from any online store and share your bank card data without fear.

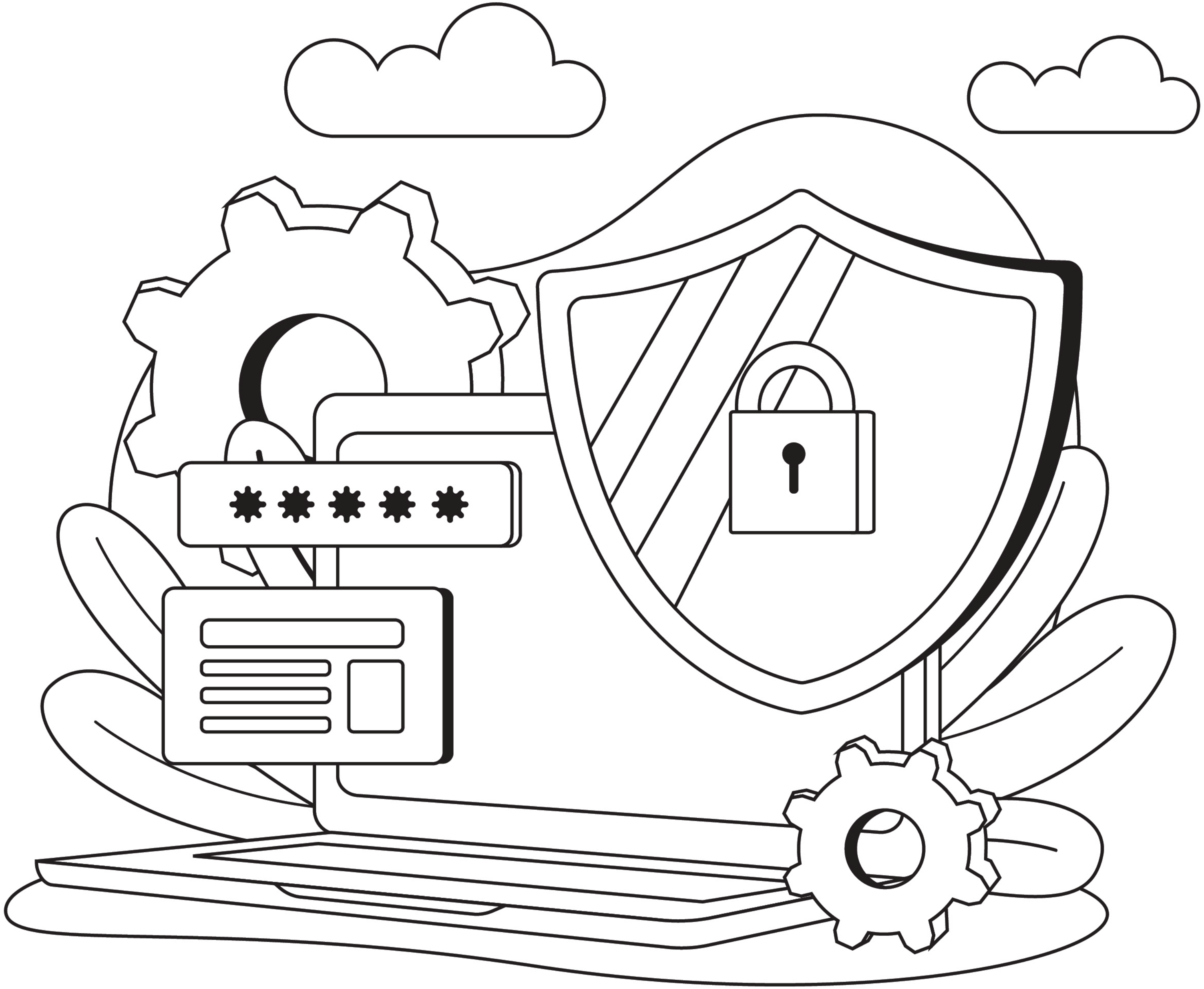
12 Fraud cannot occur in the name of charitable or volunteer institutions.

13 E-commerce is one of the primary targets of online fraudsters.

14 Clicking on malicious links without awareness may lead to the theft of your data and accounts .

15 Ransomware viruses cannot cause any harm to your devices or data.





Exercise 3

Complete the following sentences:

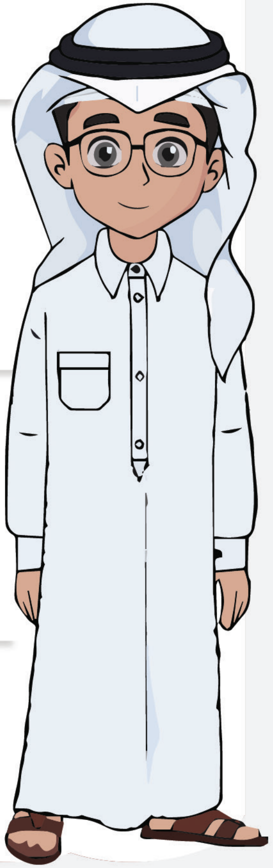
Instructions:

Carefully read the following sentences and proceed to fill in the blanks with the appropriate words to give the sentence a meaningful context. An example provided below.

1 **Digital footprint** is the digital shadow and refers to the trail of data left when using the internet

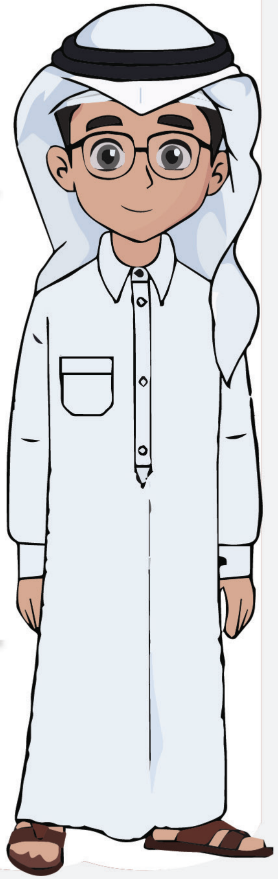
2 Digital footprintαng includes visits to ……………………………, messages from ……………………… and the information you are looking for.

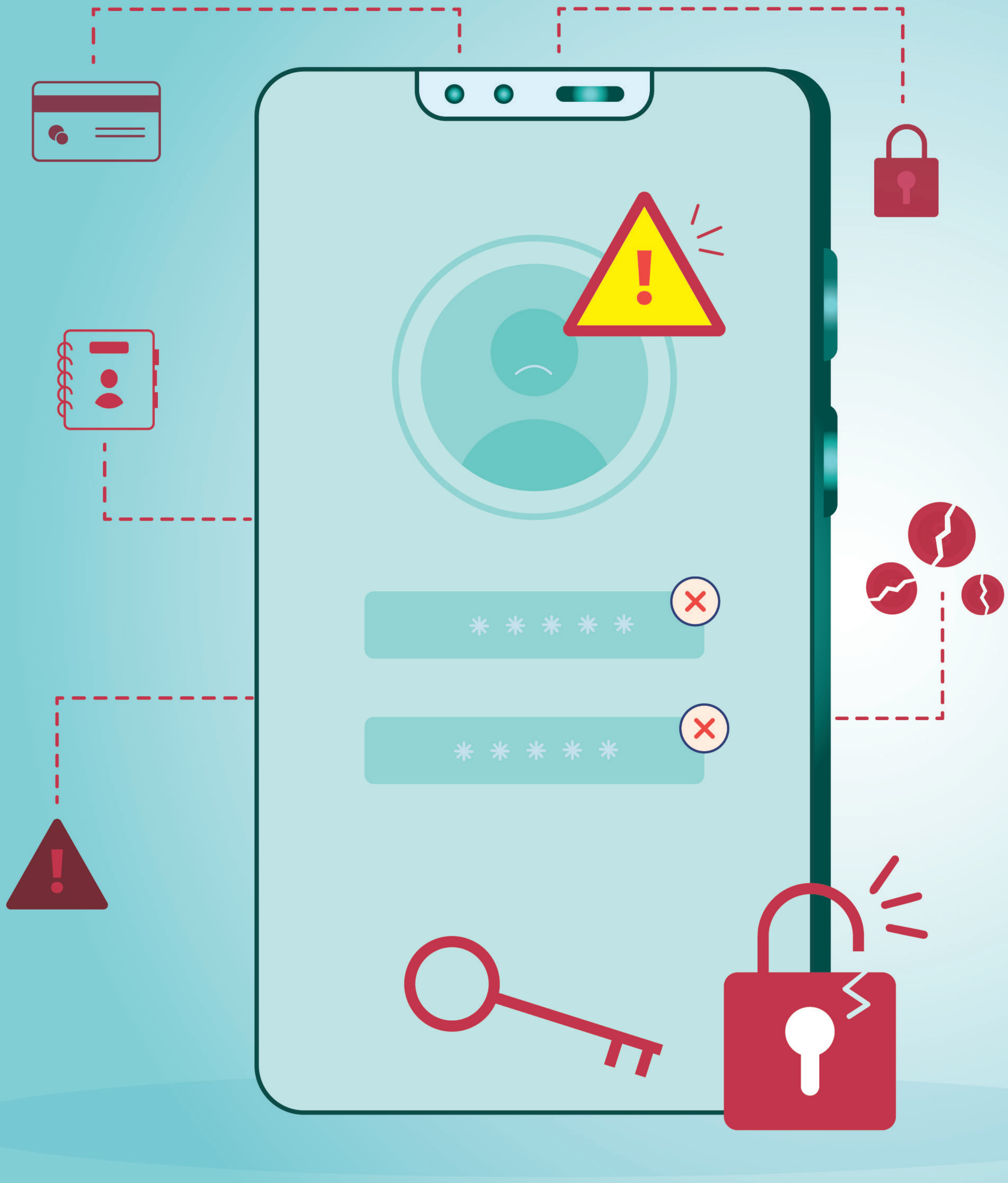
3 The ……………………… digital footprint is when you deliberately share information about yourself by participating in ……………………… sites or forums.



4 The .... digital footprint occurs through gathering information about the user without their knowledge, either from their website visits or the information they search for and use with their .... address.

5 The digital footprint is very important, especially since it is considered .... data, and it determines the .... reputation of the person. Some employers resort to tracking the digital .... of potential employees and some words or .... shared online can be misinterpreted, affecting your reputation or digital ....





Do you know that...?

Using a strong password protects you from online fraud.

Exercise 4

How can you protect yourself from online fraud? Place a word true or false:

Instructions:

Carefully read the following sentences, and carefully consider whether the sentences are true or false, and an example provided below.

1.Downloading legitimate applications from official stores.	True
2.Using modified and leaked versions of mobile phone applications.	
3.Use anti-virus software and firewalls.	
4.Sharing personal data on social media platforms.	
5.Sharing data through phone calls.	
6.Shopping only from trusted stores.	
7.Avoid sharing bankcard information on websites.	
8.It's okay to click on links from unknown sources.	
9.Be careful of using third-party services during money transfer or withdrawal.	
10.Choose a strong password consisting of uppercase and lowercase letters, numbers, and some symbols.	

Exercise 5:

Identify the mistake made by each victim in the following online fraud incidents:

Hamad received an email with a gift of an iPhone 14. So he immediately opened the link provided but found nothing.

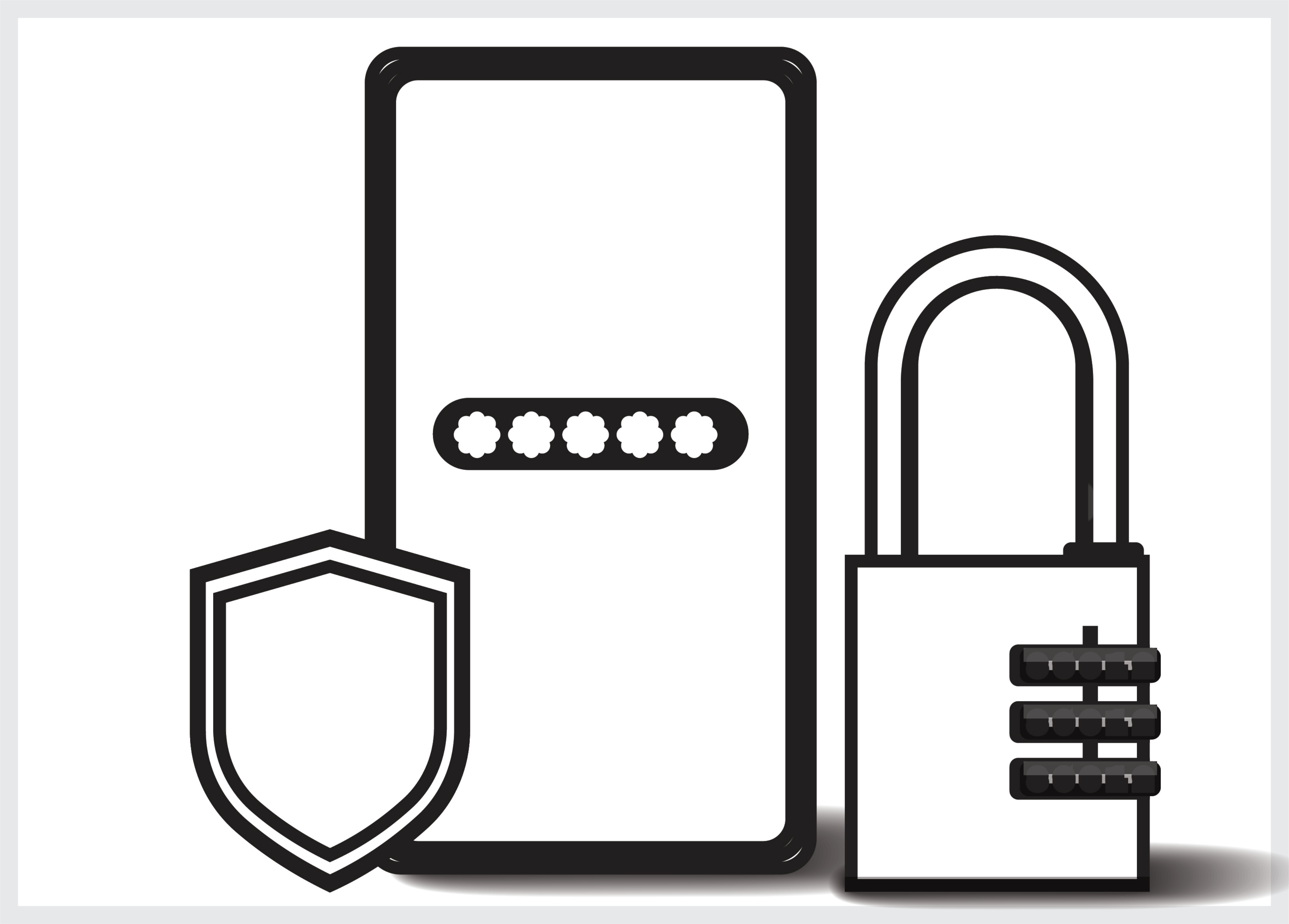
Hala received a message from an international number asking her to send her Facebook account password. Once she sent it, she couldn’t access her account again.

A bank customer service representative contacted Abdullah to verify the accuracy of his card and bank account information. After that, Abdullah received a message informing him of a withdrawal of 50,000 riyals from his account .

Mona saw a sponsored ad on Facebook for a charity collecting donations for Sudanese refugees. She sent them some money, and when she tried to confirm receipt of the amount, no one responded to her.

Do you know that...?

Logging into certain websites using your Facebook account details might expose you to online fraud.



The digital footprint is formed through

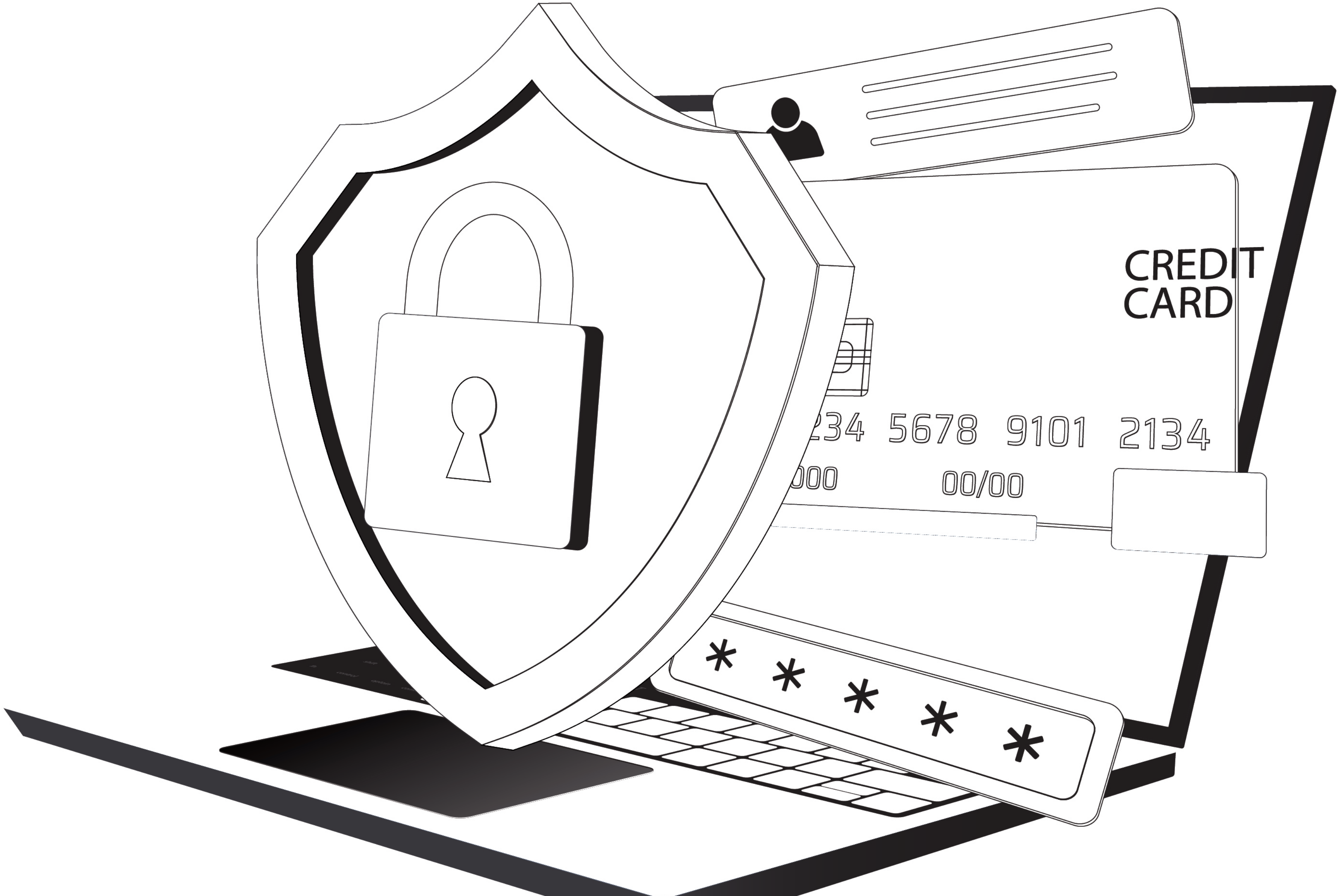
1. Online shopping.
2. Register to create an account on a specific website.
3. Downloading and using applications.
4. Using social media on your devices.
5. Logging into other websites using social media credentials.
6. Communicating with friends and contacts online.
7. Share information, data, and images with acquaintances.

Digital footprint protection methods

1. Verifying our information using search engines.
2. Removing personal information from websites.
3. Restricting the amount of data shared online.
4. Checking social media privacy settings.
5. Avoid unsafe websites.
6. Being cautious when using public Wi-Fi network.
7. Deleting our old online accounts.
8. Creating strong passwords.
9. Avoiding logging into websites using Facebook credentials.
10. Regularly update programs and applications.
11. Setting a password for the mobile phone.
12. Act quickly after a data breach.

Online fraud protection guidelines

1. Downloading applications from well-known app stores.
2. Regularly updating the phone.
3. Avoiding unknown source links.
4. Be cautious about transactions involving third parties.
5. Employing anti-virus software.
6. Using complex passwords.
7. Refraining from shopping on unfamiliar websites.

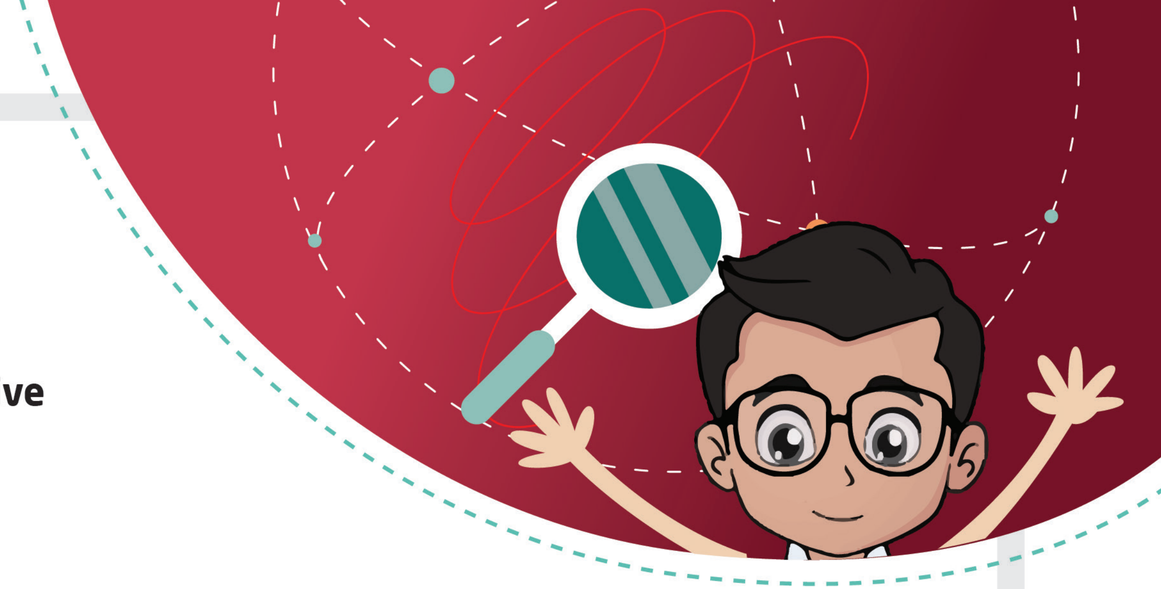

CREDIT CARD
234 5678 9101 2134
000
00/00
* * * * *

pay attention!

Information security

Refers to a set of security measures and tools that widely protect sensitive information from misuse, unauthorized access, or destruction.

Competitions



Choose the correct answer

1. Which of the following is an example of an active digital footprint

□ Posts on social media platforms.

□ Applications using geolocation.

□ Websites installing cookies without user notifying.

2. One of the most important sources of personal information is the identification links related to applications and websites.

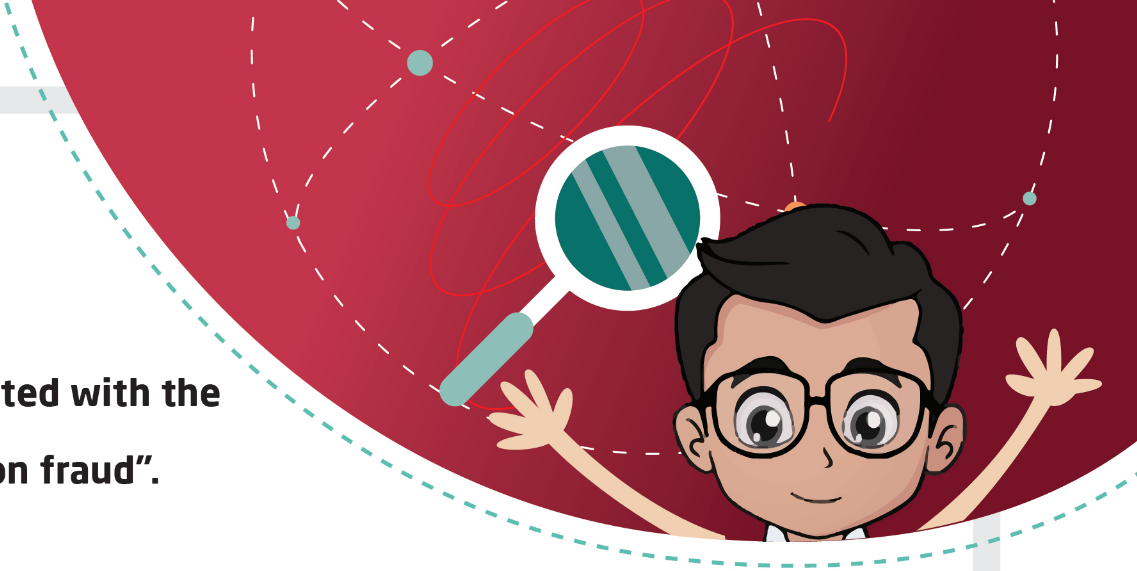
□ True.

□ False.

3. Online fraud is usually carried out when individuals visit websites, chat rooms, online stores blogs or smart applications.

□ True.

□ False.



4. **Deception or informational cheating is associated with the concept of online fraud; it is called "information fraud".**

□ True.

□ False.

5. **Online fraud is the act of seizing others' money through deceit, using computer devices.**

□ True.

□ False.

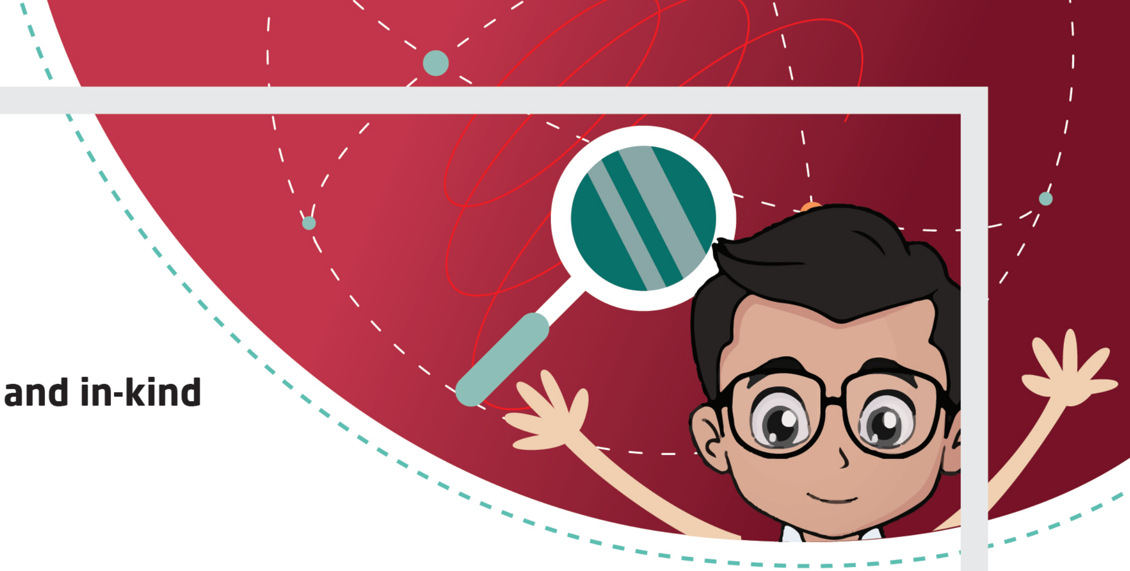
6. **Causes of online fraud include:**

□ Misuse of internet sites.

□ The spread of fake online stores..

□ Exploitation of emotional compassion.

□ All of the above.



7. **Emails containing links to attractive financial and in-kind prizes are forms of online fraud.**

□ True.

□ False.

8. **A security vulnerability is a term used for weak spots in computer operating systems and software.**

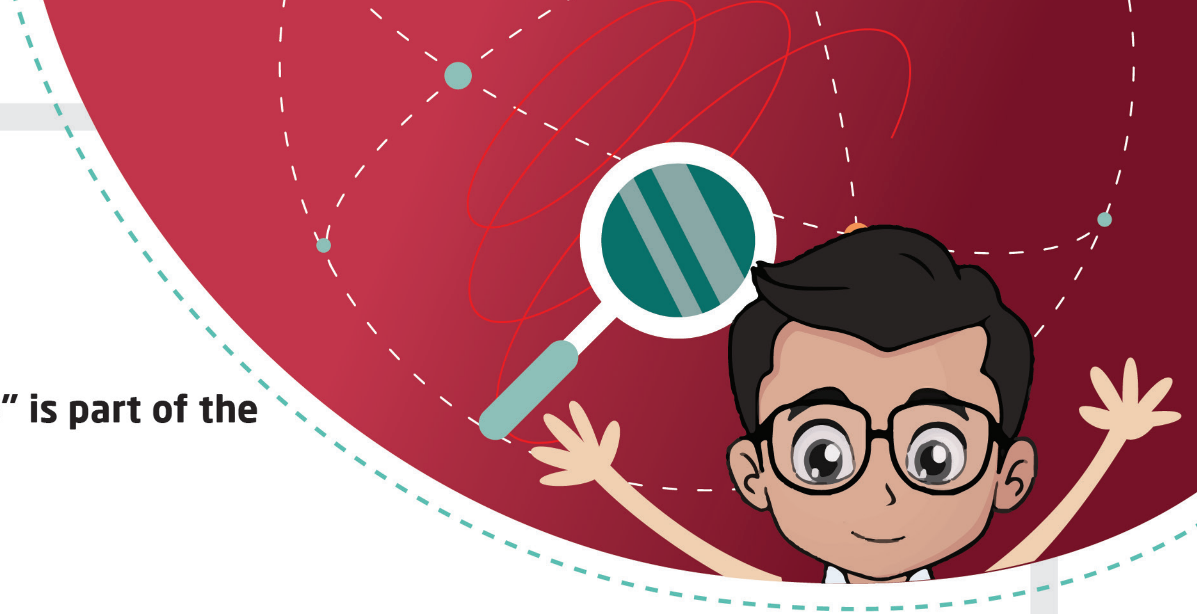
□ True.

□ False.

9. **The Zero-Day loophole does not represent a threat to cybersecurity**

□ True.

□ False.



10. **The step of "Creating an Exploitation Code" is part of the Zero-Day loophole attack mechanism**

□ True.

□ False.

11. **In the online world, the term "theft" is referred to as...**

□ Data violation.

□ Data leakage.

□ All of the above..

12. **......... can be used to track anyone's activities online.**

□ Facial recognition.

□ Handprint recognition.

□ Digital footprint.

Find the matching item

Match the sentences from column (A) with the corresponding ones from column (B)

Column (A)			Column (B)
Causes of online fraud	○	●	Exploitation emergencies such as the COVID-19 pandemic
Fake e-mail messages	○	●	One form of online fraud
Examples of online fraud crimes	○	●	Cryptocurrency theft in recent years, such as Bitcoin
One of the security vulnerabilities that infects software	○	●	Zero-Day
A set of security measures and tools that protect sensitive information from misuse	○	●	Information security
Theft of digital information stored on computers or phones for the purpose of privacy violation	○	●	Data theft
A synonym for the word “theft” in the internet	○	●	Data breach

Place the word or phrase synonymous with the following sentences:

An attack that disables our online accounts, and in exchange for reusing them, we have to pay a sum of money. ....

Fake messages offering financial rewards and gifts arrive via email or messenger with the aim of deceiving and stealing our data. ....

Vulnerable areas that lead to infiltrating our devices, whether computer or phone, putting us at risk. ....

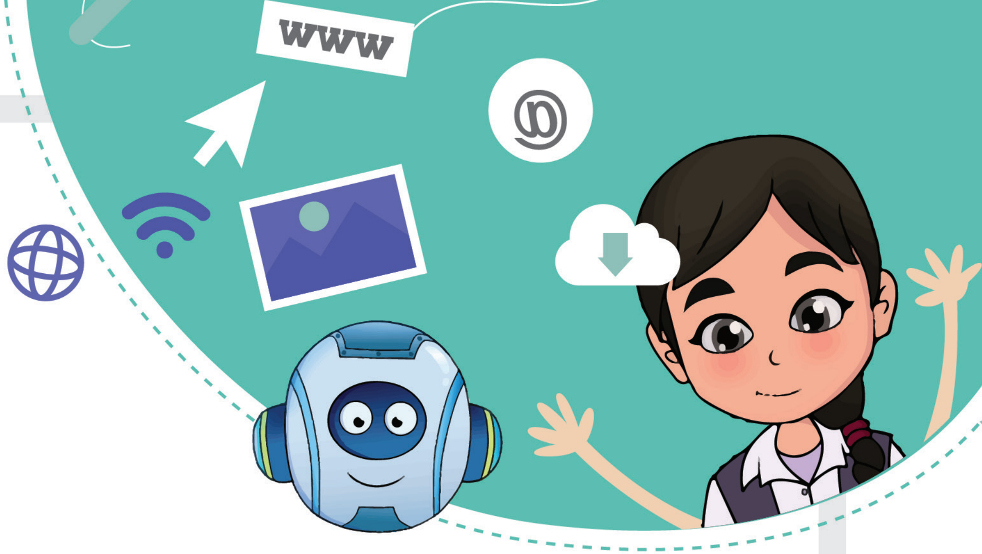
Tools that safeguard our sensitive information from unauthorized access, disruption, or destruction. ....

A specific type of theft targeting our personal data online, punishable by law. ....

Online footprints used by attackers to exploit sensitive information and deceive both us and others. ....

It consists of 12 letters, symbols and numbers, and aimed at protecting us online. ....

Complete the following sentences with the correct answers:



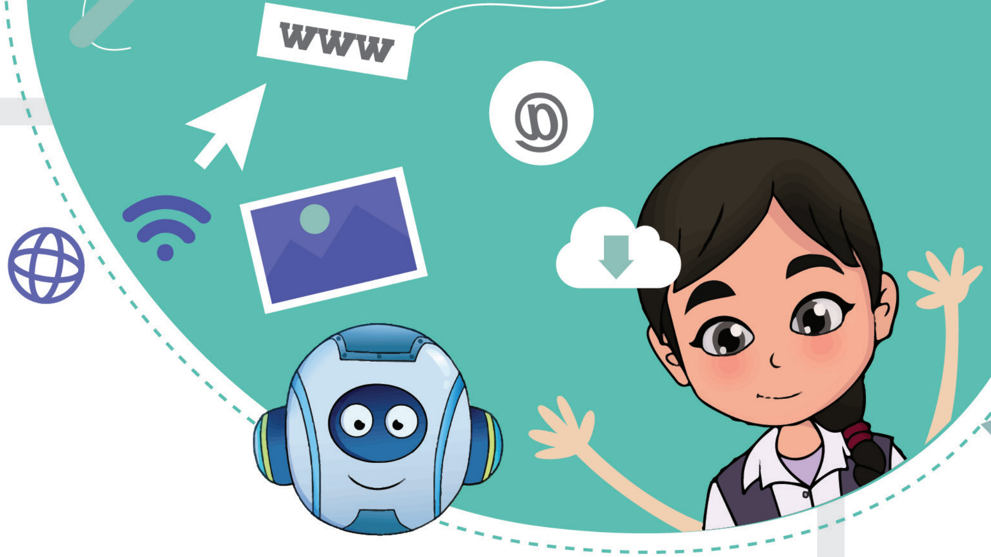
1 .... digital footprint refer to intentional sharing of user information.

2 .... digital footprint involve collecting user information without their knowledge.

3 Cybercriminals can exploit digital .... for purposes like identity theft.

4 Among the ways users add to their digital footprint is by downloading ....

5 Restricting .... is among the methods of safeguarding the digital footprint.



6 Verifying privacy settings is a way to protect ....

7 Avoiding clicking on .... is among the guidelines for protection from online fraud.

8 It is preferable to use passwords consisting of .... to protect against online fraud.

9 In case of exposure to an online fraud, it's advisable to report it to

....

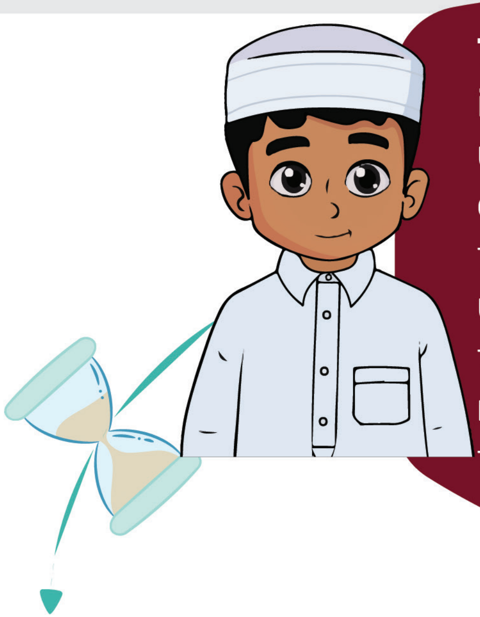
10 If your screen suddenly fills with creepy pop-ups windows, then ....

pay attention!

Digital footprint

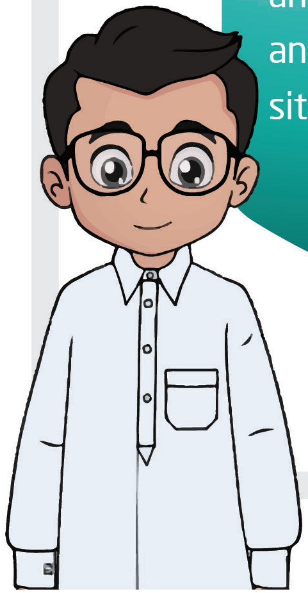
Refers to the trail of data and information left behind when using the internet. This encompasses the websites visited, the emails sent and received, and the information provided online.**The digital footprint** shapes individuals' online reputations, similar to what occurs in real life.

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 was experiences an attempted online fraud, and how he dealt with the situation.



The student takes on the role of a trainer and writes general guidelines to his colleagues or parents, explaining the necessary steps to protect themselves from the risks of forgery and online fraud.

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency