Cybersecurity Risks

Presentation Slides | Training Kit

CyberEco

معاً لدعم السلامة الرقمية

Together to support digital safety

Primary 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

Workshop Time Table

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

Content of The Training Kit

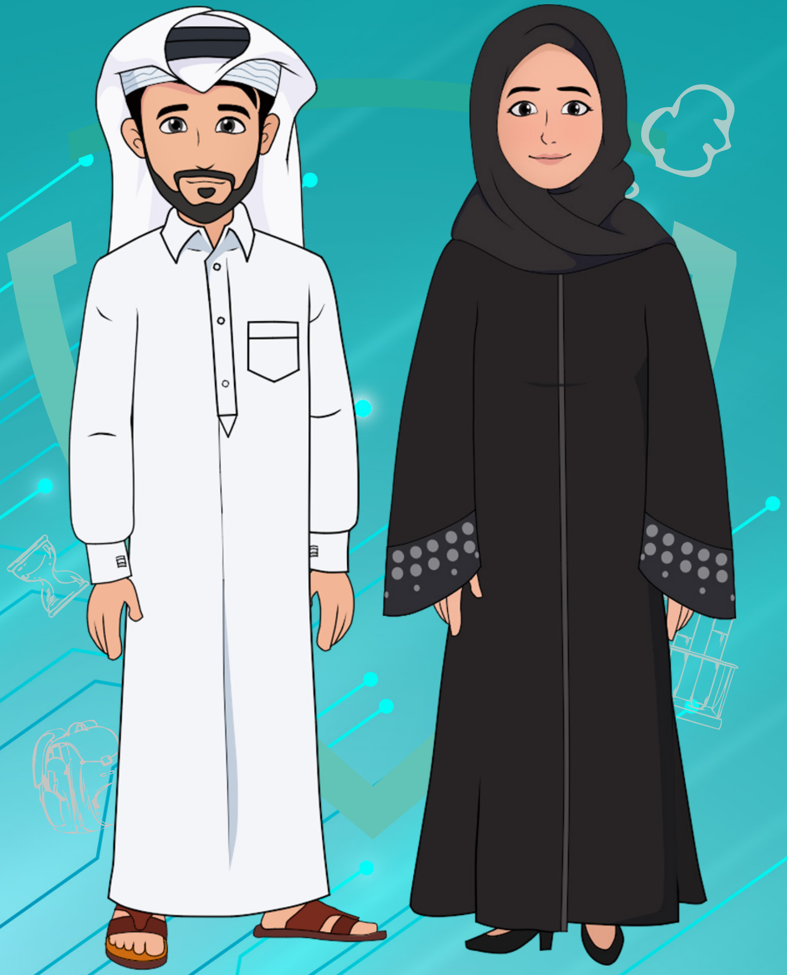
Chapter One

The Concept of Cybersecurity and Digital Safety

What is cybersecurity ?

What is cybersecurity?

Cybersecurity is the protection of networks, information technology systems, operational technology systems, and their components, including devices, software, services offered, and the contained data, from any hacking, disruption, alteration, entry, utilization or exploitation.



The importance of cybersecurity

Cybersecurity is considered one of the most important branches of technology that aims to protect all critical information concerning individuals and both public and private entities from Cyber-attacks that ultimately violate the privacy of these entities or even individuals.

Types of cybersecurity

There are several different types of cybersecurity, which are:

01

The first type

Network Security

02

The second type

Cloud Security

03

The third type

application security

04

The fourth type

operational security

Characteristics and tasks of cybersecurity

01 Data Protection

Cyber-attacks often cause significant concern for many companies. So, cybersecurity tools are employed to maintain the confidentiality of all data.

02 Protection of Intellectual Property

There are various types of protection, such as trademarks, trade secrets, copyright, and others.

Characteristics and tasks of cybersecurity

03 Protection against Money Theft

Many internet criminals (hackers) seek vulnerabilities to steal money from both small and large businesses. Updating software, utilizing strong passwords, and encrypting critical data.

04 Protection against Espionage

Espionage increases the chances of personal data and credit card numbers being stolen due to online purchasing transactions. Without sufficient security measures, devices can be infiltrated and breached.

Characteristics and tasks of cybersecurity

05 Enhanced Customer Trust

Cybersecurity aids in building customers' trust in institutions and companies they engage with by providing secure measures such as: detection systems and intrusion prevention systems, in addition to encryption systems, ensuring high protection of customers' confidential data.

06 Business protection

Cybersecurity aids in secure internet browsing and conducting work safely without fear of potential threats across networks.

Characteristics and tasks of cybersecurity

07 Protection of personal data

Cybersecurity helps protect all customer data from theft or manipulation, as any virus penetrating electronic devices.

08 Security Provision and Productivity Maintenance

Viruses breaching company-operated devices hinder employees from performing their tasks, sometimes leading to complete work stoppage.

Characteristics and tasks of cybersecurity

09 Website protection

Companies and institutions owning websites rely on security programs to reinforce cybersecurity, preventing breaches or disruptions that might affect the functionality of the website In case of any virus entry.

10 Recover leaked data

Cybersecurity not only focuses on data maintenance but also aids in swiftly recovering stolen and leaked data.

The Difference between Information Security and Cybersecurity

Information Security

It concerns the preservation of the confidentiality of information and data that internet users link to various social media platforms and online platforms from any attempt of hacking or electronic espionage.

What are the basic types of information security?

01 Software and application protection systems.

02 Operating system protection systems.

03 Entry and exit protection systems for applications.

04 Software and electronics protection systems.

The Risks Addressed by Information Security

01 Using low-security technologies and devices.

02 Issues in encryption.

03 Data corruption, whether digital or non-digital.

04 Relying on weak or undeveloped security program, especially when dealing with extensive data.

What are the Fundamental principles of information security?

Confidentiality. 01

Non-repudiation and denial. 02

Integrity. 03

Accountability. 04

Safety or Integrity. 05

Information Accessibility. 06

Key Measures Employed by Information Security Specialists

Strengthening passwords. 01

Two-factor or multi-factor authentication; such as linking the website to the phone. 02

The ability to control access to data. 03

Encryption. 04

Legal responsibility. 05

Cultural awareness. 06

Similarities between cybersecurity and information security

Information security and cybersecurity share an interest in the security of electronic or cyber information.

Cybersecurity concerns itself with securing everything in the cyber realm, including information security, while information security focuses on preserving information, even when it's online.

What are the differences between cybersecurity and information security?

Cybersecurity

- The app prevents itself from spying on you, blackmailing you, and tracking you.
- An electronic system that protects devices themselves and spy routers on the Internet from receiving any type of virus.
- It can track the hacker, know his personal identity and collect information about him.
- Cybersecurity can pinpoint the user›s location, activity, and interaction with the external environment. By connecting to more than one digital platform.
- It assists you in accessing all data and hobbies that legally or illegally access your information.

Information Security

- Information security safeguards all your data upon agreeing to the terms of using the electronic application.
- Information security is susceptible to breaches when using surveillance, hacking, and virus systems.
- Information security can alert you to an attempted online breach of any of your platforms or data you possess.
- The role of information security ends if the user stops granting permission to use their provided information at the outset of using the application.
- Information security can protect the images and data of publicly classified individuals on social networking platforms for the user.

Chapter Two

Risks associated with Cybersecurity

Cybercrimes (Internet risks)

Cybercrime

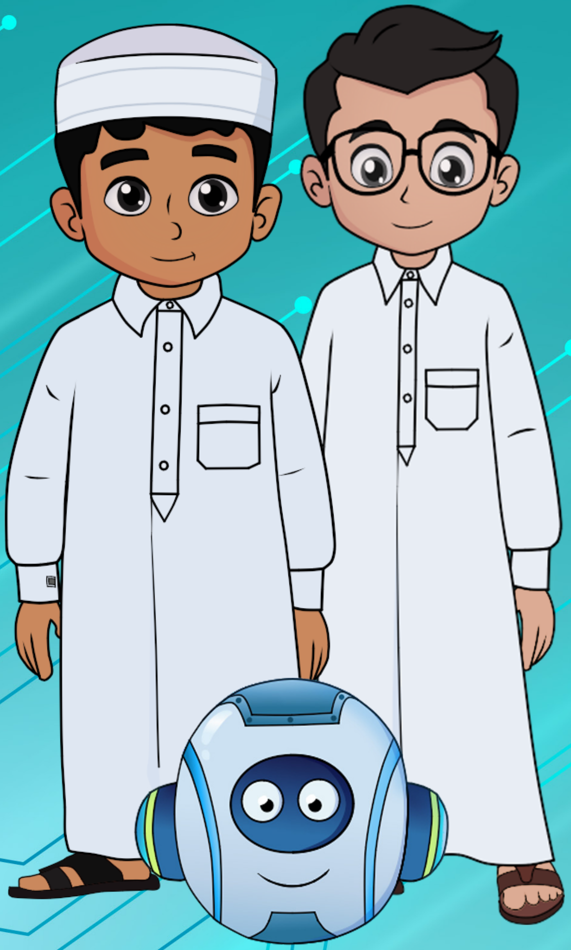
Cybercrime is an advanced form of cross-border crime that occurs in the realm of cyberspace, Perpetrators and victims of cybercrimes can be spread across different regions, and the effects of the crime can extend across communities around the world.

Types of cybercrimes

- Email and internet fraud.
- Identity theft

  (stealing personal information and using it)
- Theft of financial data or card information.
- Stealing company data and selling it.
- Electronic blackmail

  (demanding money to prevent attacks against individuals or institutions)



- Ransomware attacks (a form of electronic blackmail).
- Cryptojacking; (where hackers mine crypto currencies using resources they do not own).
- Cyber espionage (where hackers accessing individual, governmental, or corporate data).
- Interfering with systems in a way endangers the network.
- Copyright infringement.
- illegal gambling.
- Selling illegal goods online.

Cybercrimes include two main activities:

- Criminal activity using computers to commit other crimes such as extortion (Blackmail).
- Criminal activity targeting computer devices using viruses and other forms of malware.

How hackers operate

Perpetrators of cybercrimes, known as "cybercriminals," infect targeted computers with malware to damage or disrupt them. They may use this malware to delete or steal data.

Cybercrime perpetrators often engage in both activities simultaneously: they target computers with viruses first, and then use them to spread malware to other computers or across the network.

Common mistakes made by internet users

1

Using the same password for all personal accounts.

2

failing to follow latest changes made by different websites to protect users.

3

Neglect to update their smart device systems .Whether laptops or phones, which expose them to dozens of vulnerabilities that hackers may exploit for data theft and device breaches.

4

Clicking on any unknown link causes personal accounts to be hacked.

5

Accepting friend requests from people you do not know and have no relationship with is risky. It grants them the authority to breach your privacy and access your personal information.

6

Sharing personal information.

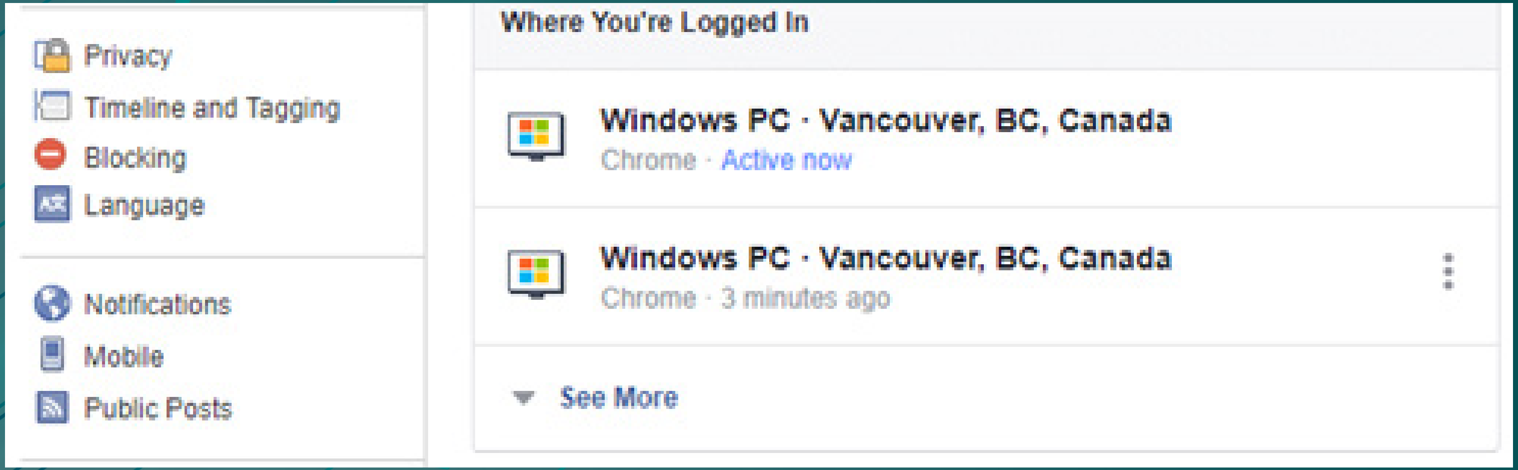
Dealing with a Personal Account Breach on Social Media:

If you suspect that your social media account password has been leaked, or that your account has been hacked; you must act quickly; hackers can prevent you from accessing your account and disturb your friends and family. Therefore, you must secure your account quickly or restore it before it is too late.

How do you know that your account has been breached?

If a hacker gains access to your account, they will leave a trace, and this can be known by:

- Click on the arrow in the top right corner.
- Selecting “Settings” from the menu.
- Go to (Security and Login).
- At the top, you will see a list of devices through which you were most recently logged in to your account, and when they were active.
- Click See More to open the list and review past sessions.



Where You're Logged In

Windows PC · Vancouver, BC, Canada
Chrome · Active now

Windows PC · Vancouver, BC, Canada
Chrome · 3 minutes ago

If you notice any suspicious activity in your login records, you should do the following:

- Change the password.
- Reporting the breach.
- Remove suspicious apps.
- Damage control.

If you are currently unable to access your account; contact your friends on Facebook, through other social media platforms, via email, or ask a mutual friend to inform them through Facebook.

How do I protect myself from cybercrime?

1. Keep software and operating system updated.
2. Use anti-virus software and keep it updated.
3. Use strong passwords.
4. Ignore attachments in spam emails.
5. Contact companies directly regarding suspicious requests.
6. Refrain from providing personal information, unless you feel safe.
7. Avoid clicking on links in spam emails or on untrusted websites.
8. Pay attention to the URLs of websites you visit.

Dealing with online abuse through social media platforms (Cyberbullying)

What is cyberbullying?

- Cyberbullying is bullying using digital technologies.
- It's a repeated behavior aimed at intimidating, angering, or defaming the targeted individuals.

Examples of such cyberbullying include:

- Spreading rumors or posting embarrassing pictures of someone on social media.
- Sending harmful or abusive messages, images, videos, or making threats through messaging platforms.
- Impersonating someone, and sending offensive messages to others in his name, or through fake accounts.

How can you tell the difference between joking and cyberbullying?

Friends often tease each other, but If the words upset you or you believe that the other person is mocking you instead of joking with you; then the joke has gone too far. And it becomes cyberbullying.

How to deal with cyberbullies

1. Talk to someone you trust, like a friend, family member, school counselor, or another trusted adult.

2. If the cyberbullying occurs on social media, you should consider blocking the person engaging in cyberbullying and reporting their behavior to the relevant social media platform.

3. Gathering evidence like text messages or screenshots containing offensive content posted on social media against you, and reporting it can be helpful.

4. Think twice before posting or sharing anything online; it might remain on the internet forever, and could be used against you later.

5. Do not give any personal details such as your address, phone number, or school name.

6. Learn about the privacy settings on your favorite social media apps

Chapter Three
How do I protect myself from digital threats?

Using a password to protect data

A strong password performs several functions:

01

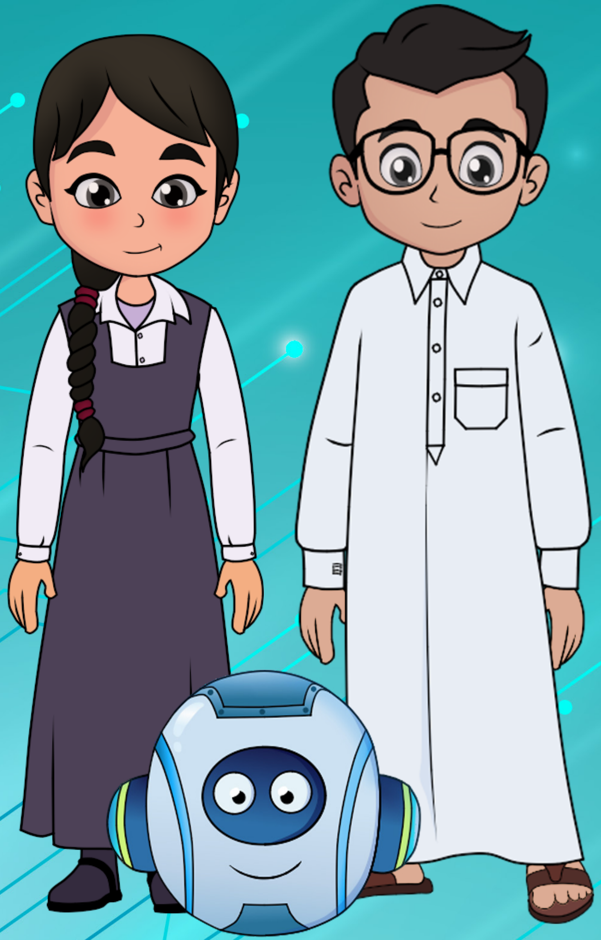
Keeping your personal data secure.

02

Protect your emails, files and other data.

03

Prevent anyone else from accessing your online accounts, such as social media pages.



How to create a strong password?

A password should consist of a combination of letters, numbers, and symbols (regular ASCII characters only), and cannot include diacritics or formatted characters.

You must avoid the following things when choosing a password:

- Very weak, such as “password123”.
- Previously used for your account.
- Starting or ending with a space.
- Easy to guess.
- Use one password for all your important online accounts.
- Reuse passwords on your important accounts.
- Less than 12 characters.

When creating a password you can use the following:

- Lyrics from a song or poem.
- A memorable quote from a movie or speech.
- A paragraph from a book.
- A sequence of words that are meaningful to you.
- An abbreviation: creating a password from the first letter of each word in a specific sentence.

Avoid choosing predictable or guessable passwords, such as:

- People who know you.
- Information available through your social media profile.
- Avoid using information that others may already know or can easily access, such as:

Your surname or initials.

Your pet’s name.

Birthdays or important years for you.

The name of the street where you live.

Digits from your address.

Your phone number.

- Simple words, phrases and patterns such as:

Obvious words and “phrases, like “password

Sequential letters or numbers such as ““abcd” or “1234

Keyboard patterns, like ““qwerty” or “qazwsx

Email protection

The most important steps that you must follow are:

- Choosing a strong password.
- Activating “Two-Factor Authentication
- Regularly changing passwords
- Using a different password for each account.
- Updating installed software
- Blocking spam emails with unknown content
- Tracking anonymous emails.

To track emails in Gmail, follow these steps:

1

Open your Gmail account, using any browser.

2

Open the email message you want to track.

3

Click the More icon (⋮) next to the word “Reply”, in the top-right corner of the message.

4

Select “show original” from the menu.

5

A new window will open containing the original message information; including: authentication results, sender’s IP address, creation date, and message identification number.

To track emails in other mailing services by:

01

In Outlook: click on “File,” then on “Characteristics.”

02

In Hotmail: Right-click the email, then select “View message source.”

03

In Apple Mail: Click View, then Message, and select All Addresses.

04

In Yahoo: Click “More”, then select Show original message.

What should i do when I am exposed to Digital threats?

If you are exposed to cyber blackmail... you must do the following:

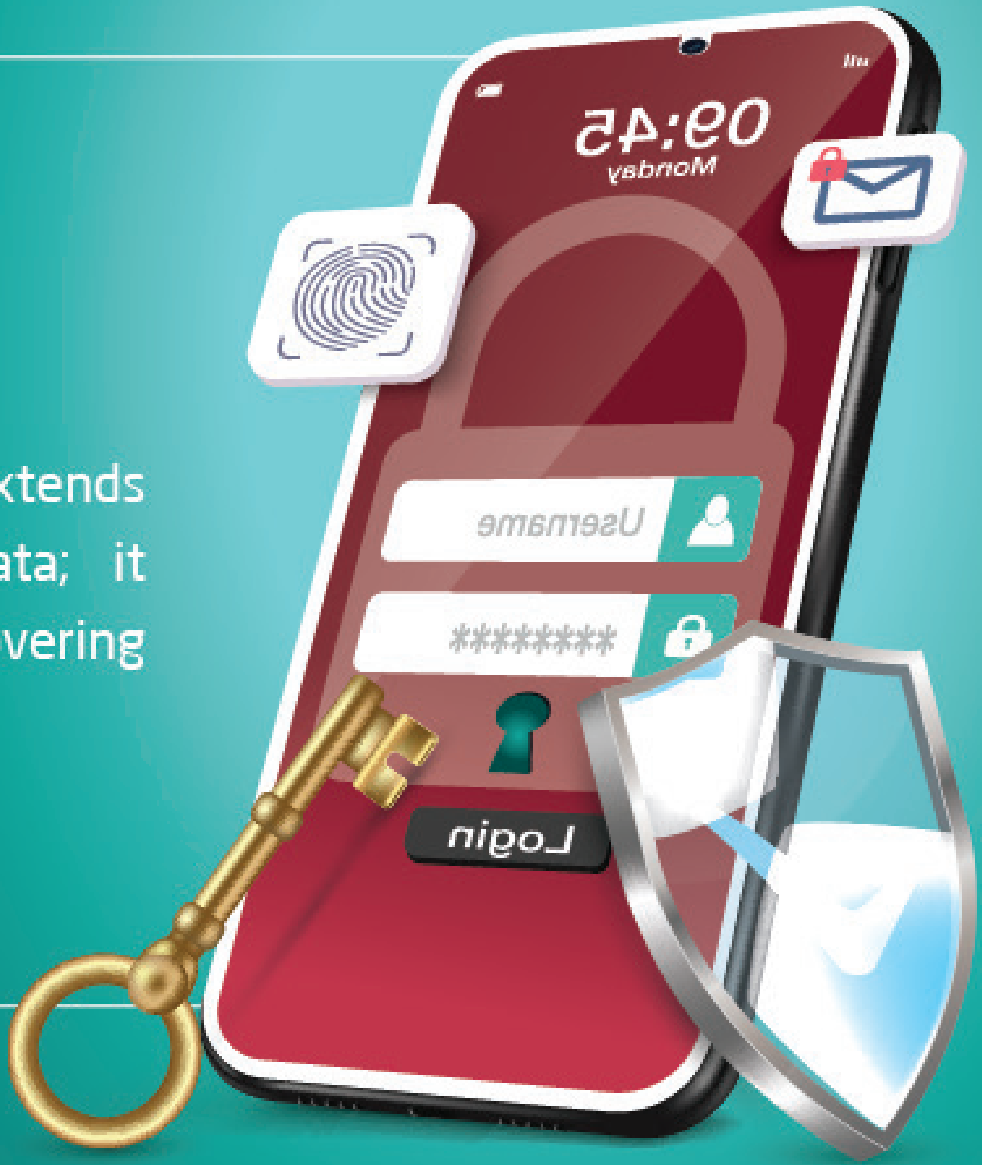
- Avoid responding to or trying to persuade the blackmailed person or not to publish your personal information and images. Doing so may give the impression that you are vulnerable or responsive to their demands, leading them to increase their demands or verify the authenticity of the information.
- Store the content with which you have been blackmailed, without deleting the threatening messages; it is evidence that can be used to convict criminals.
- Stop the blackmailer from following your accounts on social media sites, and change your passwords immediately. It is preferable to use different passwords that include numbers, letters, and symbols for your various accounts.
- Tell a trusted person about what happened to you, such as your father, mother, or supervisor at school; to provide you with psychological support, it is also preferable to seek psychological support from specialists, therefore, that blackmail does not affect your mental and psychological health.
- Contact the National Security Agency or the Cybercrime Department in your country.

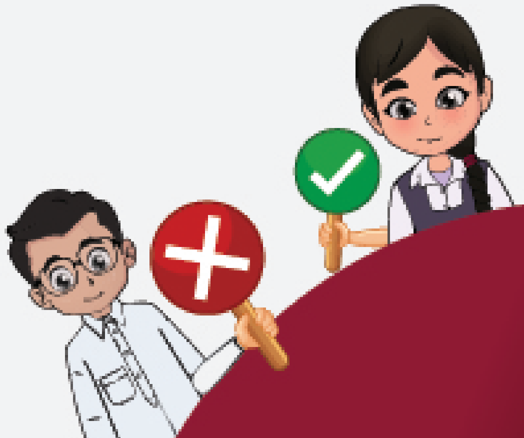
Exercises and training

First:
In-Class Exercises

Do you know ?

Cybersecurity's mission extends beyond safeguarding data; it also helps in quickly recovering stolen and leaked data.





Instruction

Read the sentences in the table carefully, and consider whether the information is true or false. If you find it to be true, write (Correct) next to it. If you find it to be false, write (Incorrect) next to it. Seek the trainer's help if needed.

Exercise 1

Identify the (✓) and (✗) statements in the following sentences:

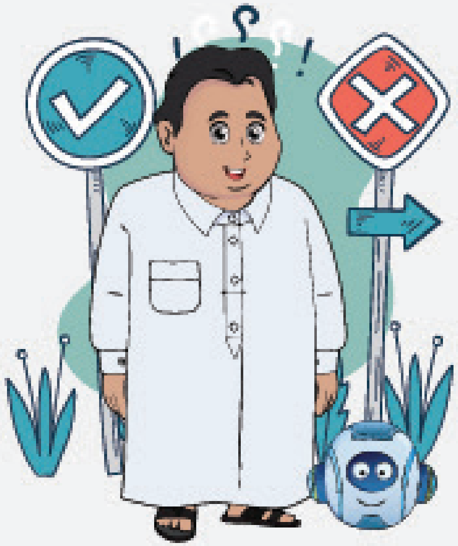
1 Cybersecurity is the protection of devices, networks, and applications from digital risks. ✓

2 Organizations are not responsible for securing their own data or the data of their clients. ○

3 Data protection builds trust between the organization and its customers. ○

4 Specialized measures and tools are necessary to protect data, especially unauthorized access. ○

5 Individuals need to understand the fundamentals of digital security to protect themselves and their private data from cyber risks. ○



6 Interest in cybersecurity has increased as most institutions and governments rely on digital and electronic services. ○

7 Hacking and data theft pose an easily solvable problem with Insignificant consequences. ○

8 Cyber-attacks have many advantages. ○

9 Cyberattacks have the potential to expose confidential data, facilitate its theft, or intentionally lead to its deletion. ○

10 Cyber-attacks do not happen intentionally, and anyone can execute them. ○

Pay Attention!

Setting a single password for all personal accounts and e-mails increases the chances of hacking your electronic devices.

01001110
01110100
0111011101
111100010110

Do you know?

Hackers, who infiltrate devices and data systems, seek vulnerabilities through which they can pilfer funds and private information. To mitigate such risks, it is imperative to regularly update software, employ robust passwords, periodically change them, and encrypt crucial data.

Instruction

Carefully read the sentences in the table, starting with the first sentence in column (A). Then, search in column (B) for the sentence that completes its meaning. Below is an example of linking two sentences.

Exercise 2

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

- Sitting online for long periods... ○
- Extended internet usage can lead to... ○
- You might be susceptible to privacy hacking through ○
- Privacy hacking ○
- Exposure to violent and inappropriate content for children ○
- You can suffer from internet addiction. ○
- The Internet threatens society's security ○
- The Internet threatens national culture ○

● Hacking attempts and data theft on websites.

● When you sit for long periods on the Internet without interacting with others.

● Leads to ethical, psychological, and physiological issues.

● Because openness to other cultures without controls may lead to adopting inappropriate elements conflicting with our religious and cultural beliefs.

● Because some terrorist groups resort to it to recruit young people and harm society.

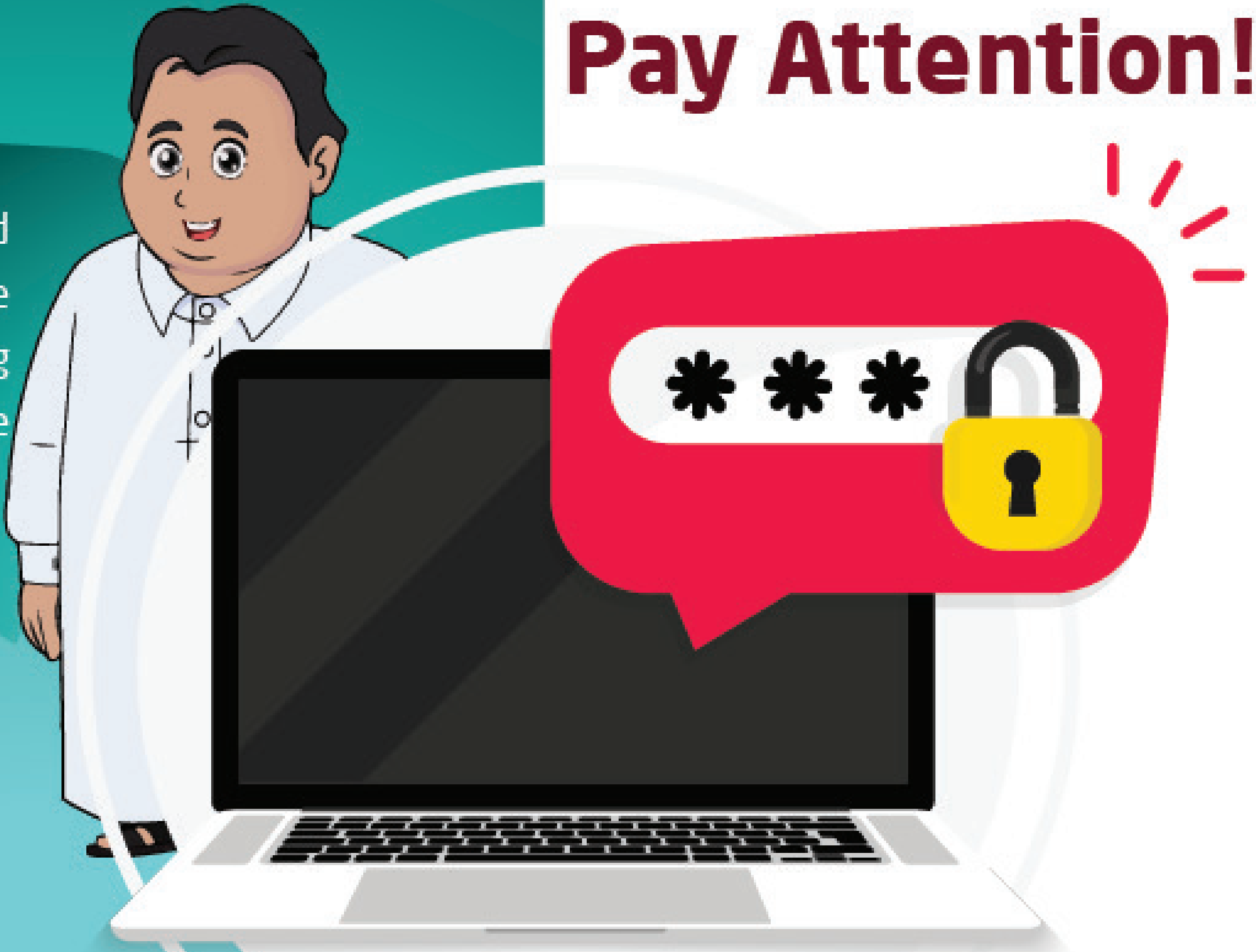
● Leads to social isolation.

● is a punishable crime by law.

● Depression and anxiety and stress.

Pay Attention!

Ignoring privacy settings and not keeping up with the latest changes in operating systems exposes you to the risk of being hacked.

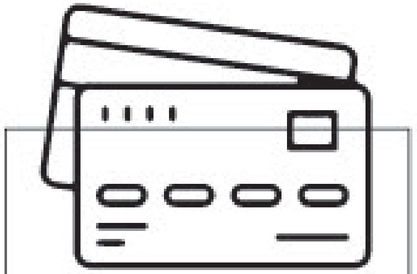


Exercise 3

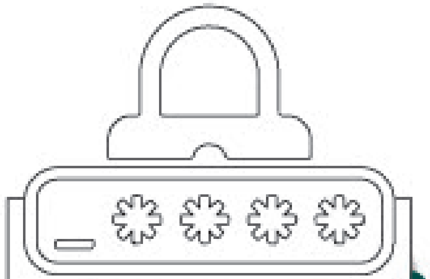
Read the following words carefully and consider whether these words represent something that can be stolen via the internet. For example, 'private photos and videos' are items that can be stolen through the internet. Color any item from the following list that can be stolen via the internet with one of the colors.

Information and documents on the computer

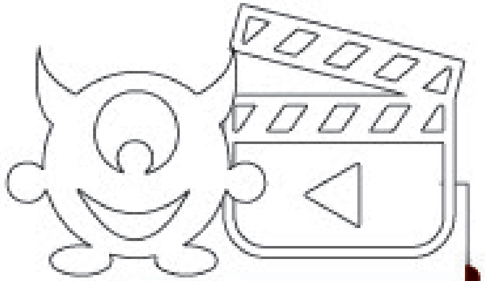
Bank account numbers



Credit card numbers

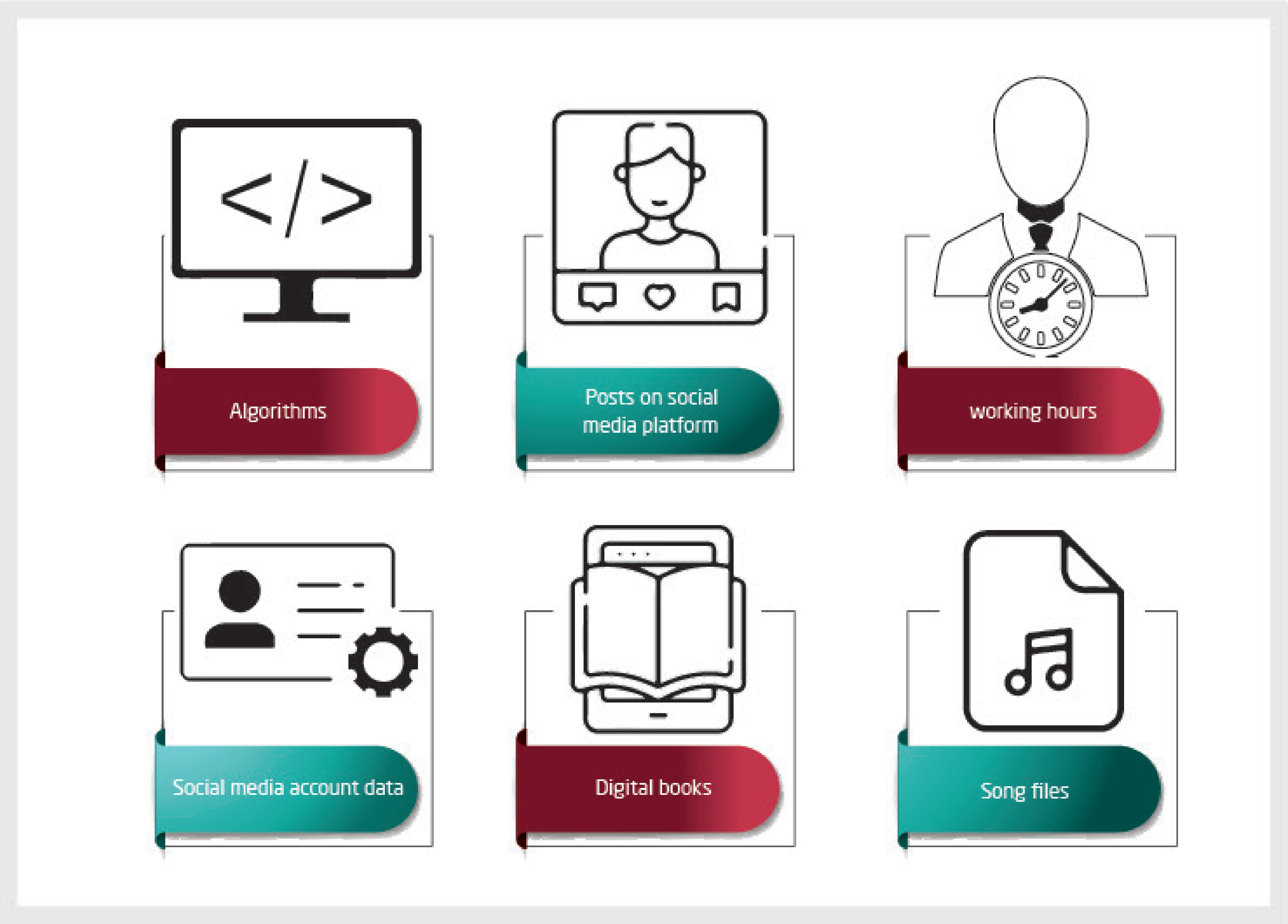


Passwords



Cartoon movie files

Official document data such as a license and passport



Algorithms

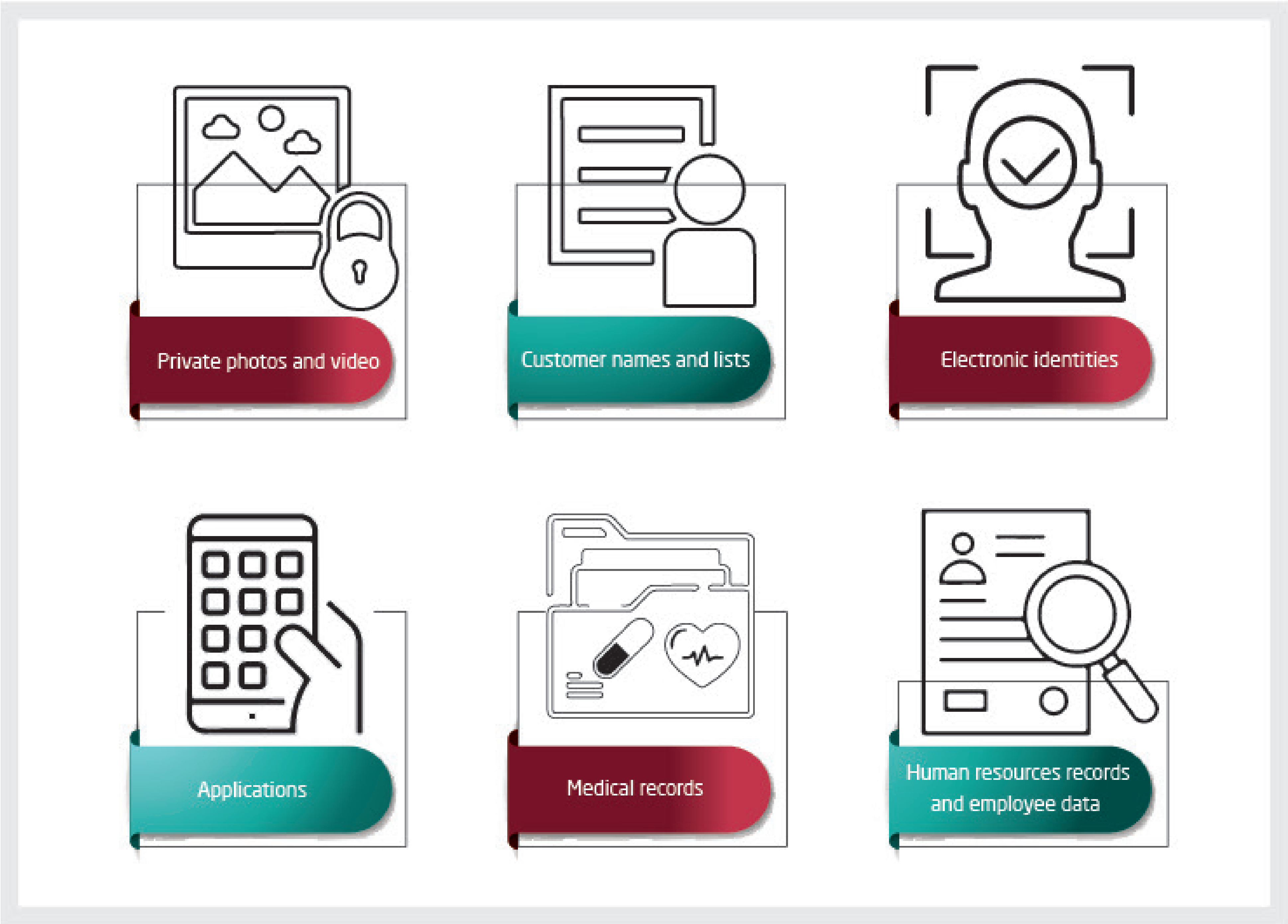
Posts on social media platform

working hours

Social media account data

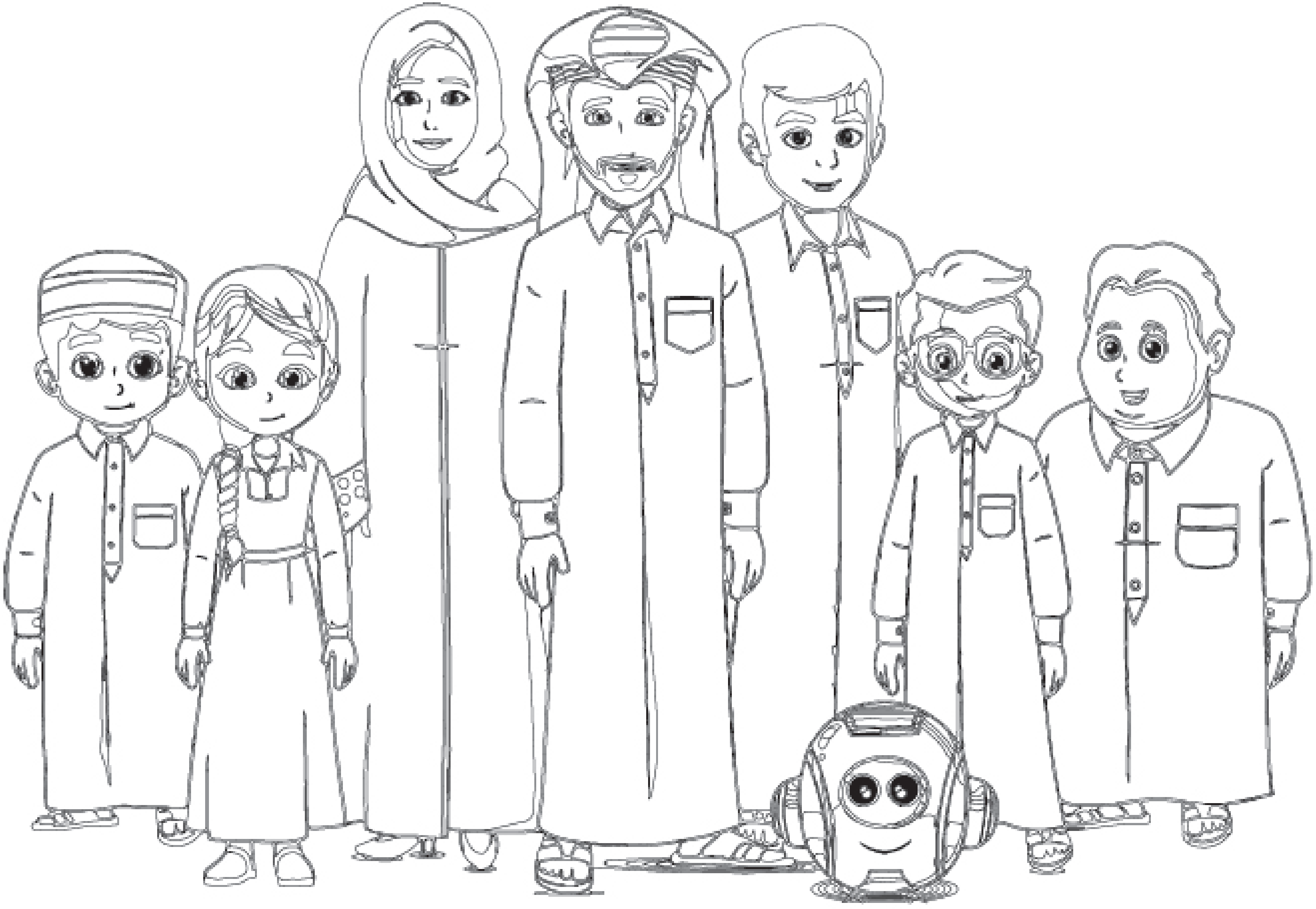
Digital books

Song files


Private photos and video
Customer names and lists
Electronic identities
Applications
Medical records
Human resources records and employee data

Pay Attention!

Failing to update the systems of smart devices, whether they be personal computers, phones, or tablets, exposes them to numerous vulnerabilities exploited by device hackers for data theft and device compromise.



Exercise 4

Carefully read the words provided, and consider whether these words reflect the digital impacts and risks. Then, proceed to shade the box containing the word or phrase.

Stress

Anxiety

Pride

Happiness

Distraction

Wanting to leave school

Avoiding friends

Ability to face

Low grades

Loss of self-esteem

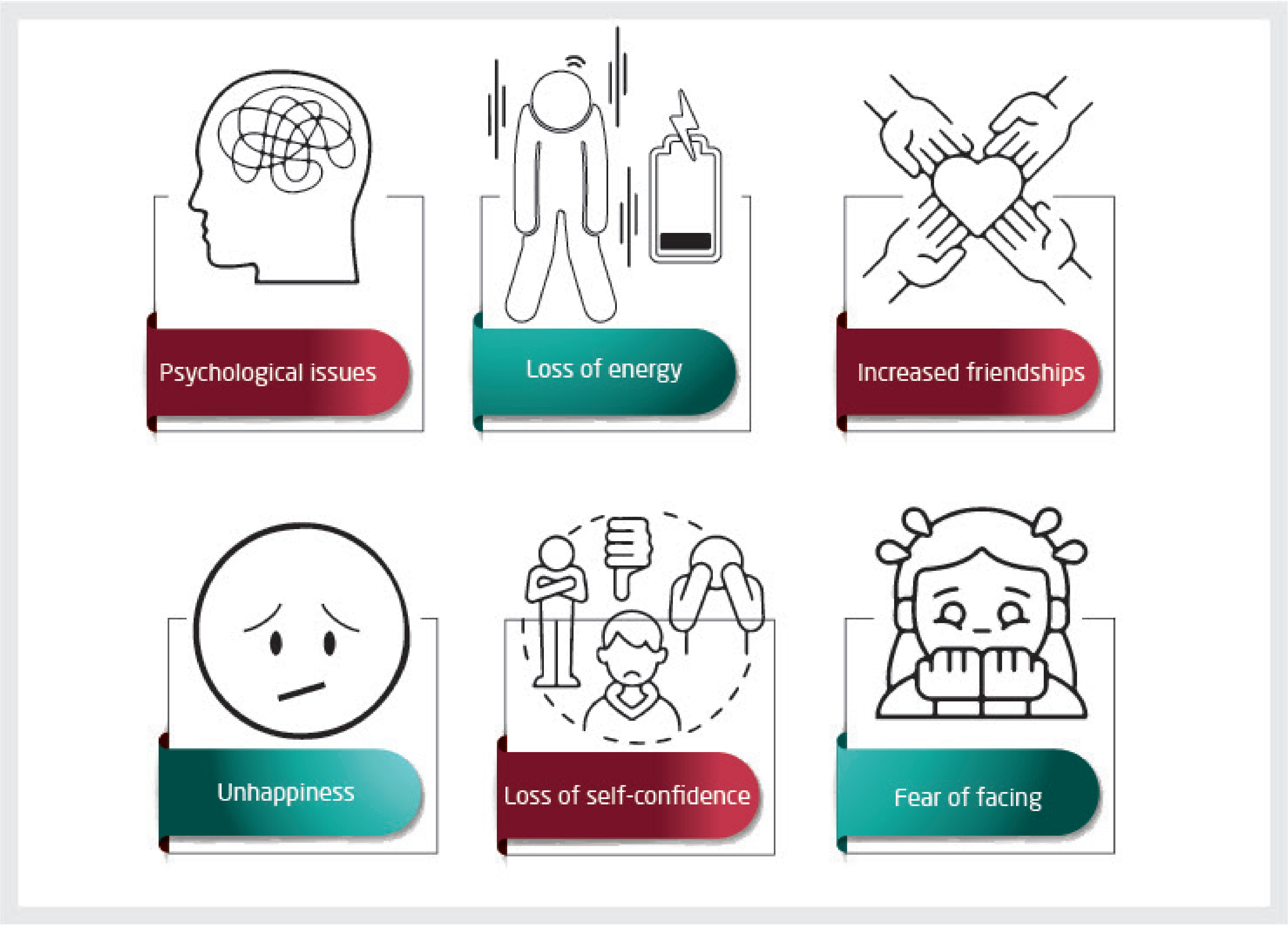
Sleep problems

Avoiding leaving the house

Wanting to engage in activities

Weight gain

Concentration



Psychological issues

Loss of energy

Increased friendships

Unhappiness

Loss of self-confidence

Fear of facing

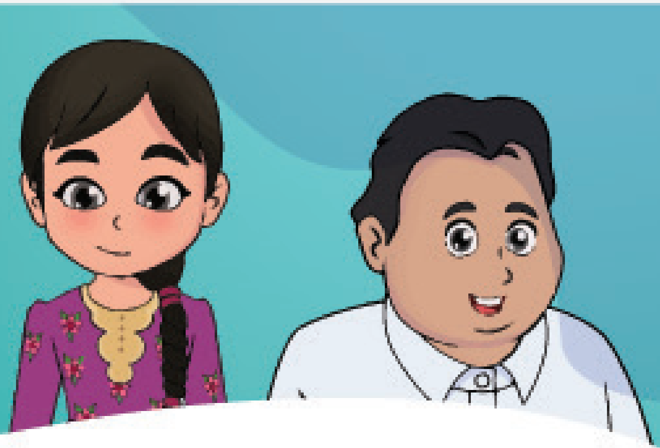
Do you know ?

Numerous advertisements are considered as one form of viruses on websites, which are transmitted to electronic devices with a simple click.

Exercise 5

Choose the best and strongest password to protect the data

Read the passwords below carefully, and think whether these words considered a strong password or not. Recall what the trainer explained to you about the criteria for choosing strong passwords. For instance, the password '123456' is not strong because it is easy to guess and consists of consecutive numbers



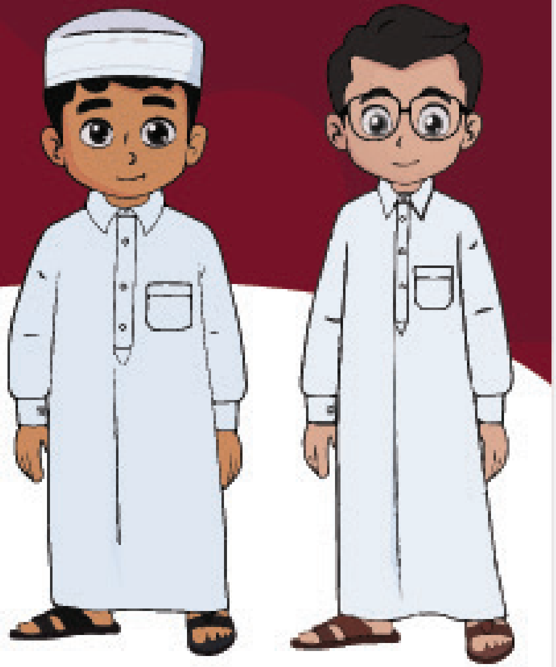
- □ Medo123
- □ 654321
- □ 2020MMeeDDoo$%
- □ Klmetser
- □ Password
- □ Penten
- □ 123medo
- □ 123456
- □ Me@12do
- □ Pass123

Pay Attention!

Clicking on any unknown or suspicious link will cause personal accounts breaches.

Exercise 6

Choose the correct answer:



1. **When I am exposed to a cybercrime, I should:**

□ Remain completely silent and not inform anyone.

□ Contact the police without my parents' knowledge.

□ Immediately go to one of my parents or my teacher at school.

2. **When I am exposed to cyber blackmail, the first thing I should do is:**

□ Threaten and provoke who blackmails me

□ Completely block them and report them to service providers.

□ Attempt to give them what they want so they don't harm me with what they know about me

3. **To protect myself online, I should:**

□ Tell everyone everything about me.

□ Never make any friends online.

□ Share regular, non- sensitive information that no one can use against me.

Second:
Non-classroom Exerclses

Pay Attention!

Sharing many details about our personal life, the nature of our work and our home on the Internet exposes us to hacking and theft.

Exercise 1

Extract the following words from the table

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:

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

Cybersecurity - Digital security - Attacks - Crime - Data - Confidentiality - Risks - Theft - Fraud

Services - Theft - Problem - Protection - ~~Thieve~~ - Disaster

Exercise 2

Read the phrases below carefully, read the words or phrases provided within parentheses: "...", and select any of the appropriate words. There is an example provided below.

" The Internet is an **International** ☑ **Local** □ network ".

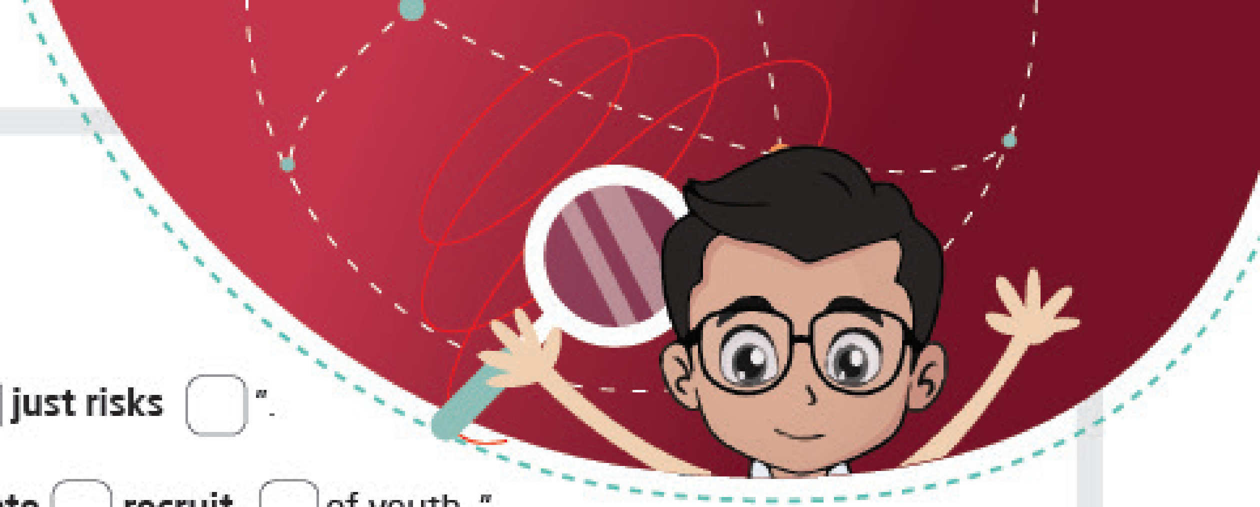
" The Internet is a means for **learning and entertainment** □ **entertainment and leisure** □ " .

"The Internet is important for transmitting and sharing "**data** □ **movies** □ and series ".

" Spending a long time using the Internet might make you **socially isolated** □ **sociable and loves gatherings** □ ".

" Research confirms that using the Internet for a long time can infect you with a lot of **promotions** □ **physical** □ and psychological diseases ".

" There is a link between being **thinness** □ **obese** □ and using the Internet for a long time ".



" The Internet is full of "benefits and **risks** □ **just risks** □ ".

" Terrorist groups exploit the Internet to **educate** □ **recruit** □ of youth ".

" Data theft and hacking of personal accounts is a **Crime** □ **Prize** □ in law ".

" One of the most prominent risks of the Internet is that all data is exposed to **Save** □ **Theft** □ and hacking ".

" Exposure to new cultures without controls may lead to **rejecting** □ **acquiring** □ customs that ".

" The Internet threatens societal culture because of its "**closure** □ **openness** □ to the world and its different cultures ".

" Children are most vulnerable to online problems due to **Violent** □ **Musical** □ content ".

" Internet addiction is a common problem that occurs due to **Using the Internet for a long** □ **Time using the Internet for two hours every day** □ ".

Exercise 3

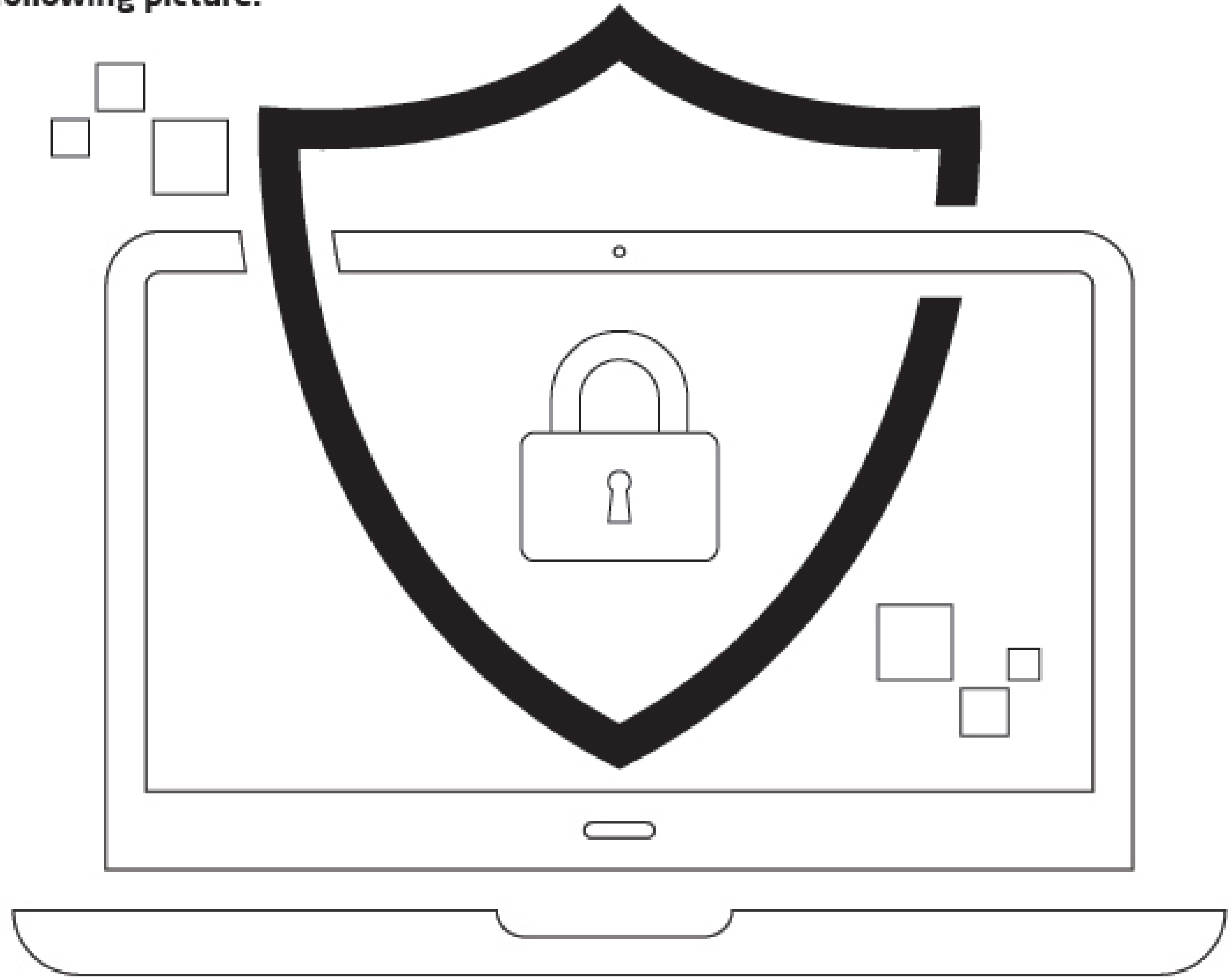
Read the sentences in the table carefully, and consider whether the information is true or false. If you find it to be true, write (**Correct**) next to it. If you find it to be false, write (**Incorrect**) next to it. Seek the trainer's help if needed

Hackers can steal users' data through fraud and pretending to be a trusted entity, such as banks or telecommunications companies?	Correct	
Weak passwords may be the easiest way to steal data?		
Sometimes the hacker sends a file or link via email, and by simply clicking on it, the device is easily hacked and the data is stolen?		
There is no problem with data theft.		
The hacker cannot benefit from the data he stole.		
You should choose simple passwords that can be easily guessed.		

You must make sure that there are no security gaps in your computer system or suspicious applications on your phone to avoid the risk of data theft.		
No human error can lead to data theft.		
Downloads are always safe, and devices cannot be hacked or have data stolen through them.		
Problems in databases or servers can result in data theft and make it easy for hackers to access networks or devices.		
The person himself may lead to the theft of his data without realizing it, just by disclosing a lot of information through social media platforms.		
Sometimes theft of phones or computers causes data leakage.		
Using public Wi-Fi networks or computers or tablets in public places such as libraries or Internet cafés may expose data to the risk of theft.		
Companies or organizations do not need to secure databases or servers in order to protect customer data.		

Exercise 4

Color the following picture:



Exercise 5

Place the word **"correct"** in front of the statements that can help you create a strong password:

Instruction

Carefully read the phrase below and think whether these phrases represent the conditions for creating a strong password. Remember what the trainer explained to you about the criteria for choosing strong passwords

I use the same letters as the username.	
I use a diverse set of letters and numbers.	
I use my birthday.	
I use a combination of uppercase and lowercase letters and some symbols.	
I use a word I can't remember.	
I use a word similar to old passwords.	
I use the word "password".	
I use my cat/dog's name.	
I use a date that is special to me.	
I use a word that is easy for me to remember and difficult for others to guess.	Correct

Pay Attention!

Accepting friend requests from unknown individuals is risky, as it allows them to breach your privacy and acquire personal information.

Training Games

Discuss the following questions with your colleagues

01 Cybersecurity is also called

(Number of letters 16) (________________________________)

02 Length of strong password

(Number of letters: 9 letters) (________________________________)

03 People who cause serious harm to our electronic devices

(Number of letters 7 letters) (________________________________)

04 One of the types of cybersecurity

(Number of letters: 13 letters) (________________________________)

05 One of the examples of intellectual property rights

(Number of letters: 12 letters) (________________________________)

Puzzles

Contains links or files with viruses or malware, and once opened or clicked, your data is stolen... What is it ? ....

Once you accept it, your privacy and personal information become threatened... What is it ? ....

Its mission is to protect information technology systems and their components, including devices, services, and data... What is this thing ? ....

An advanced form of transnational crime that occurs in cyberspace. ....

Spreading lies or embarrassing images of someone, sending hurtful messages, or threatening someone on social media are all forms of ....

The password consists of ....

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:

Writing a short story about a student who was exposed to a digital threat or attack; Such as data hacking, and how he responds to this situation.

The student takes on the role of the trainer and writes general guidelines for his colleagues or parents, explaining the procedures required to prevent the digital risks.

CyberEco

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency