

Cybersecurity Risks

Training kit

Trainer's booklet



CyberEco

قيمة قبلنا مدعا لقه
yates Isatigib hoqquz of rathogot



Primary School



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Cybersecurity Risks

Primary School

Training kit

Trainer's booklet

Intellectual Property rights

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

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

Anyone who breaks this could face legal consequences.

December, 2023

Doha, Qatar

This content is produced by the team of

National Cybersecurity Excellence Management, National Cyber Security Agency.

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



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

🌐 <https://www.ncsa.gov.qa/>

✉ cyberexcellence@ncsa.gov.qa

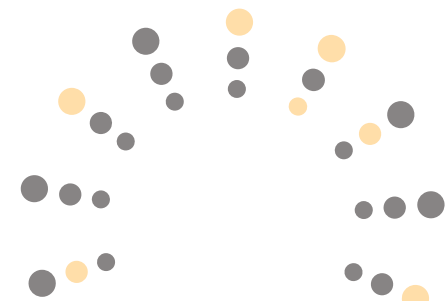
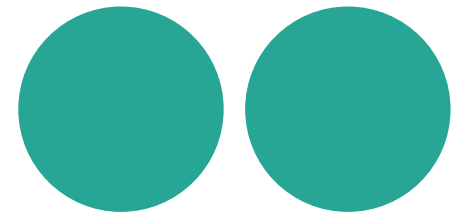
☎ 00974 404 663 78

☎ 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.

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

- Providing the trainer with training tools that help him deliver the training content to the students.
- To present information and training content in an easy and simple manner.
- To offer training content on cybersecurity risks along with multiple training tools and method

Contents of the Training Kit

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

1. **Presentation files.**
2. **Training games**, such as shape coloring, drawings and crossword puzzles, 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: The Concept of Cybersecurity and Digital Safety

First: What is Cybersecurity?..... 21

What is cybersecurity? 21

The importance of cybersecurity? 21

Types of cyber security? 22

Second: Characteristics and tasks of cybersecurity 23

Data protection 23

Protection of Intellectual Property 23

Protection against Money Theft 23

Protection against Espionage 23

Enhanced Customer Trust 23

Business protection 24

Protection of personal data 24

Security Provision and Productivity Maintenance 24

Website protection 24

Recover leaked data 24

Third: The Difference between Information Security and Cybersecurity.

Information Security..... 25

The risks that information security deals with 25

What are the Fundamental principles of information security?.. 26

Key Measures Employed by Information Security Specialists..... 27

Similarities between cybersecurity and information security....28

What is the difference between cybersecurity and information security..28

Chapter two: Risks associated with cybersecurity

First: Cybercrimes, (Internet risks).....33

What is Cybercrime? 33

Types of Cybercrime? 34

How hackers operate35

Common mistakes made by internet users 36

Dealing with a Personal Account Breach on Social Media..... 37

How do you know that your account has been breached?..... 37

How do I protect myself from cybercrime? 39

Second: Dealing with abuse via social media sites

(Dangers of cyberbullying)

What is cyberbullying?	41
How can we differentiate between joking and cyberbullying?..	41
How can digital bullying affect my mental health?.....	41
How to deal with cyberbullies.....	42

Chapter three: How do I protect myself from digital threats?

First: Use password to protect data.

How to create a strong password?.....	48
---------------------------------------	----

Second: Email protection.....51

Choosing a strong password.....	51
Activating "Two-Factor Authentication"	51
Regularly changing passwords.....	51
Using different passwords.....	51

Updating installed software.....	52
Tracking anonymous emails.....	52
Blocking spam emails with unknown content.....	52

Third: What should I do when I am exposed to digital threats?

Dealing with electronic blackmail cases	55
Protecting personal data from theft.....	56
Examples.....	57

Exercises and training61

References

WorkShop Timetable

Content	Content
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 primary school students.
2. The trainer presents slides for each point discussed. For example, when talking about the concept of Cybersecurity, the first slide is displayed: What is Cybersecurity?
3. After explaining 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 mentioned competition questions are presented.
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 educational videos mentioned in the file. Separately - to students at the end of each chapter, or when he sees the time is appropriate.
9. Examples of Cyber incidents are mentioned during the presentation of the scientific material.
10. When posing the question of how we can differentiate between joking and Cyberbullying, It is encouraged to open a discussion with the students to hear their opinions.
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.
- 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 digital threat or attack, such as having his data hacked, and how he dealt with this situation.
 - The student takes on the role of a trainer and write general instructions for his colleagues and family explaining the procedures required to prevent digital risks.

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.



Second: scientific Content





Chapter One

The Concept of Cybersecurity and Digital Safety

- What is cybersecurity?
- The importance of cybersecurity?
- Types of cyber security?



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 concept of cybersecurity includes: information security, electronic security, digital security, and similar aspects. Cybersecurity is a set of technical, administrative and organizational measures relied upon and used to prevent the theft of electronic information from individuals and entities, aiding in the recovery of all stolen information.⁽¹⁾

The importance of cybersecurity

Given the digital transformation in many sectors across numerous countries and the emergence of the so-called digital economy and investment in technical sectors, this has created a need to safeguard the interests of users of communications and information technology services.

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.

Therefore, after the significant advancements in the world of technology, and the evolution of various digital transactions, relying on cybersecurity has become one of the most important things of our time, which means that it helps protect individuals and institutions from Cyber-attacks launched by online hackers against all devices used daily, such as (computers, digital devices, smartphones, and tablets).

Especially with the emergence of new forms and tools of cyber-attacks amid technological advancements - that significantly target the theft of all data and information, and the subsequent fraud and theft of money.⁽²⁾

1. Youssef, Amir. (2015AD). Information technology crimes in the Arab Gulf States, and international and local efforts to combat them, Internet and electronic computer crimes in the Arab Gulf States. Egypt: Dar Al-Kutub Al-Arabiyya. pp. 68-74.
2. Previous reference.

Types of cybersecurity

There are several different types of cybersecurity, which are:

The first type: Network Security

Most Cyber-attacks occur through computer networks, and one of the best solutions is to rely on cybersecurity to protect all computer networks from these attacks, cybersecurity helps provide the best immediate solutions to control data elements and access networks completely, preventing theft of stored data, among other things.

The second type: Cloud Security

Recently, artificial intelligence has been utilized by individuals and institutions to enhance work quality and accomplish tasks more efficiently in less time. Handling the vast amount of data stored has become challenging. Hence, various companies are working on providing better services to address this issue rapidly, such as Google Cloud and Microsoft Azure.

The third type: application security

Web applications are known to be connected to the Internet, making them susceptible to hacking and data theft. Cybersecurity here works to protect data from any attack such as viruses, information encryption, and more..

The fourth type: operational security

In case of data breaches, cybersecurity aids in accessing several alternative plans, and this type appears in most large companies and institutions.⁽¹⁾

1. yagibca, prateekt (2023) Cyber Security, types and importance, GeeksforGeeks. On site: <https://www.geeksforgeeks.org/cyber-security-types-and-importance/>

Cybersecurity possesses numerous distinct features and benefits which we outline below in the following points:

Data Protection

Cyber-attacks often cause significant concern for many companies and institutions, as they can lead to their inability to safeguard their customers' data. To maintain the confidentiality of all customer data, it's essential to rely on cybersecurity tools to ensure data protection.

Protection of Intellectual Property

The safeguarding of Intellectual property is one of the most important aspects of cybersecurity, and there are various types of protection, such as trademarks, trade secrets, copyright, and others, fall under the umbrella of safeguarding intellectual property.

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 are some cybersecurity tools to mitigate these threats.

Protection against Espionage

Cybersecurity helps prevent hackers from spying on individuals and institutions. 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.

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.

Business protection

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

Protection of personal data

Cybersecurity helps protect all customer data from theft or manipulation, as any virus penetrating electronic devices means hackers can access to all sensitive data.

Security Provision and Productivity Maintenance

Viruses breaching company-operated devices hinder employees from performing their tasks, sometimes leading to complete work stoppage, and here the importance of cybersecurity emerges. To prevent this from occurring, or to intervene immediately in such incidents; To prevent the issues from escalating and to restore normal operations.

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 due to virus entry.

Recover leaked data

Cybersecurity not only focuses on data maintenance but also aids in swiftly recovering stolen and leaked data.⁽¹⁾



1. Sarker, I.H. and Kayes, A.S.M. (2020) Cybersecurity Data Science: An overview from machine learning perspective - journal of big data, SpringerLink. On site: <https://link.springer.com/article/10.1186/s40537-020-00318-5>

Third:

The Difference between Information Security and Cybersecurity

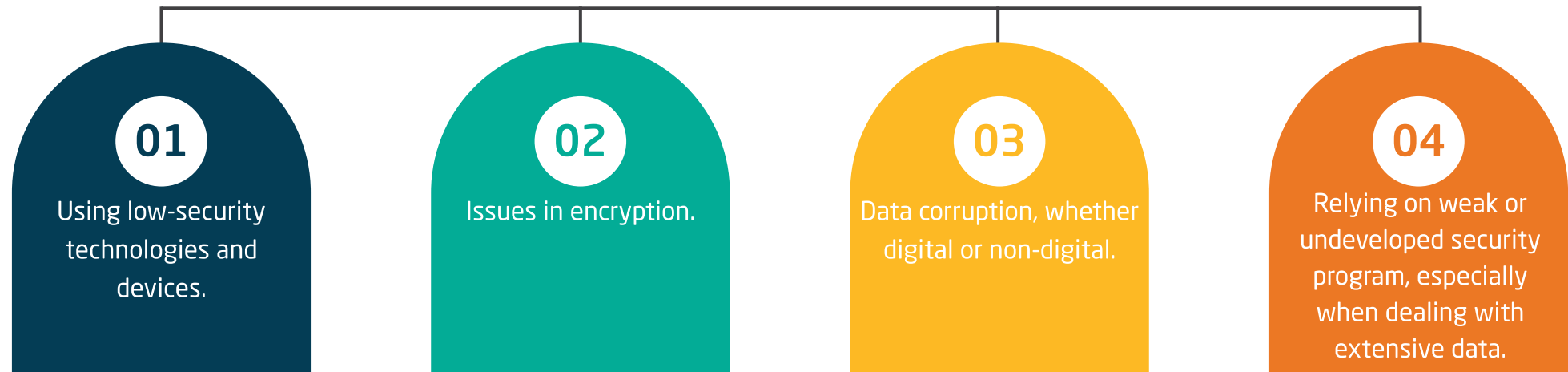
Information Security

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. Information security is increasingly utilized with the development of websites and the expansion of their methodologies⁽¹⁾.

The Risks Addressed by Information Security

Among the most important risks that information security deals with are the following:



1. Al- Otaybi, Mead (2017), Basics in Cybersecurity, available at the link:<https://www.docdroid.net/1BTYYas/asasyat-fy-alamn-alsybrany-pdf>

What are the Fundamental principles of information security?

Confidentiality:

This principle aims to make information exclusive to those with permission to access it, and to withhold it from any unauthorized individual, through encryption or other methods.

Non-repudiation and denial:

The principle states that no one can deny receiving information or that it was not sent to them; encryption ensures that the sender sent the information to the intended recipient.

Originality:

The principle ensures that the recipients are the actual people intended to receive the information, not impersonators. The same applies when sending digital currencies like Bitcoin through digital wallets.

Accountability:

This principle involves tracking the actions of those who accessed this information, ensuring we know who changed or modified any part of the information, maintaining a record of these actions for reference.

Safety or Non-alteration:

It is concerned with protecting information from modification by unauthorized individuals. This principle maintains the accuracy and reliability of data.

Information Accessibility:

This principle involves providing information to authorized individuals whenever they need it.



Key Measures Employed by Information Security Specialists

01

Strengthening passwords.

02

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

03

The ability to control access to data.

04

Encryption.

05

Legal responsibility.

06

Cultural awareness.

Similarities between cybersecurity and information security

There are points of similarity between the two fields, which are:

- 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?

- Despite their shared concern for protecting and preserving information, there are significant differences in concept and function:
- Information Security preserves all your data upon agreeing to the terms of using an electronic application. While cybersecurity prevents the application itself from spying, blackmailing, or tracking you based on your interests and followers on the application platforms.
- Information security can be vulnerable to hacking when using spyware, piracy, and viruses, while cybersecurity is an electronic system that shields devices from receiving any kind of viruses, and alerts the user to take appropriate steps to safeguard their data from theft.
- Information security can notify you of an attempt to hack one of your platforms or the data you own. However cybersecurity can track the hacker, know his personal identity, and collect information about him, while ensuring that the hacker is fully charged legally.
- The role of information security ends if the user stops authorizing the use of his information that he provides at the beginning of using the application, such as geographical location identification, while cybersecurity can determine the user's location, activity, and interaction with the external environment, by connecting through multiple digital platform, and utilizing various program tools used by the same individual.

- The role of information security ends if the user stops authorizing the use of his information that he provides at the beginning of using the application, such as geographical location identification, while cybersecurity can determine the user's location, activity, and interaction with the external environment, by connecting through multiple digital platform, and utilizing various program tools used by the same individual.
- Information security can protect the images and data of individuals publicly classified on social media platforms, while cybersecurity helps you access all data and all hobbies that connect to your data either legally or illegally⁽¹⁾.



1. Al- Otaybi, Mead (2017) Fundamentals of Cybersecurity, Previous reference..



Chapter Two

Risks associated with Cybersecurity

- Cybercrime (Internet risks)
- Common mistakes made by internet users (risks of personal data theft)
- Dealing with personal account breach
- How do I protect myself from cybercrime?
- Dealing with online abuse through social media platforms (cyberbullying)



First:

Cybercrimes (Internet risks)

What is cybercrime?

Cybercrime (or electronic crime) is an advanced form of cross-border crime that occurs in the realm of cyberspace, which has no boundaries. Perpetrators and victims of cybercrimes can be spread across different regions, and the effects of the crime can extend across communities around the world. It is a criminal activity that targets a computer, computer network, or a device connected to a network, aiming to use them in unauthorized ways.

Most cybercrimes are committed by thieves or hackers seeking financial gains. In other rare cases, the goal behind cybercrimes might be to cause damage to computers for reasons other than profit, which could be political or personal. Cybercrimes can be committed by individuals or organizations. Some of these cybercriminals are organized, use advanced techniques, and are possessing high technical skills, and some are just novice hackers.⁽¹⁾

1. Smith, A.D. and Rupp, W.T. (2002), "Issues in cybersecurity; understanding the potential risks associated with hackers/crackers", Information Management & Computer Security, Vol. 10 No. 4, pp. 178-183.

Types of cybercrimes include:

- 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.

Thus, we find that cybercrimes include two main activities:

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

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.

Hackers can also use malicious software to prevent users from accessing a website or the network, or to block a company providing a service from reaching its customers. This method is known as a Denial-of-Service (DoS) attack. It also includes cybercrime installing malicious software on computers and smart devices, and disseminating this software on networks⁽¹⁾.

1. Person, Tim, P. and Jordan, T. (2017) A sociology of hackers: 10: Cyberspace crime: Tim Jordan, Paul Tayl, Taylor & Francis. On site: <https://cutt.us/NwnyZ>

Common mistakes made by internet users (risks of personal data theft)

Internet users often make several mistakes, which digital hackers can exploit to carry out their attacks. Here are the most significant of these errors:

- 1. Similar passwords:** It is necessary to avoid using the same password for all your personal accounts and e-mail. If one account is compromised, it could lead to the theft of all your accounts, complete compromise, and exposure of your data to risk.
- 2. Privacy settings:** One of the most dangerous mistakes on social media platforms is ignoring privacy settings and failing to follow latest changes made by different websites to protect users.
- 3. Lack of secure system:** Many users neglect to update their smart device systems .Whether laptops or phones, which exposes them to dozens of vulnerabilities that hackers may exploit for data theft and device breaches.
- 4. Clicking on links:** Despite experts' warnings against clicking on unknown link, many users still commit this mistake, resulting in the compromise of their accounts.
- 5. Accepting friend requests:** 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:** Users often make the mistake of sharing too many details about their personal lives, work, and home without realizing the potential risks.

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:

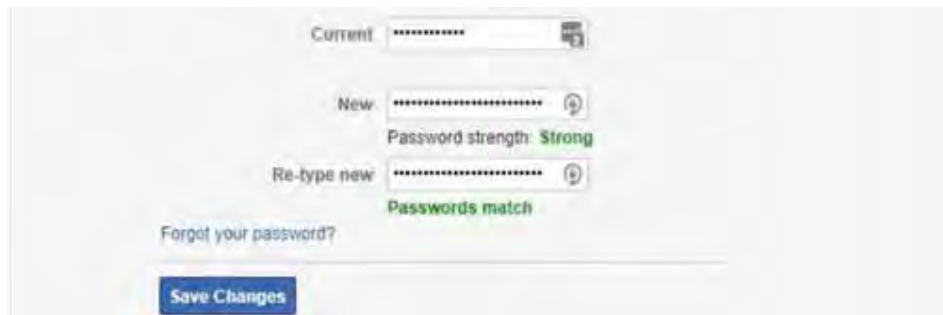
- Click on the arrow in the top right corner.
- Selecting “Settings” from the menu.
- Go to (Security and Login).
- At the top, you will see a list of devices through which you were most recently logged in to your account, and when they were active.
- Click See More to open the list and review past sessions.



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

change password:

- If the hacker hasn't changed your password, you're lucky. This is a good time to update your password before logging out of unknown sessions.
- Click on the (Settings) menu
- Click on the (Security and Login) option.
- Scroll down to access the Login option
- Click on Change password.
- Enter your current password, and choose a new, strong password, or you can use a password manager application (such as: Last Pass), then click on "Save Changes" option



Reporting the breach:

If you find that your account has not been hacked, but has started sending unwanted messages to your friends, you must report this to the social media platform administration, such as Facebook, by using the link: [Facebook.com/hacked/](https://www.facebook.com/hacked/).

Removing suspicious apps:

Sometimes, your account is hacked through applications that you have granted access to and given some permissions to. To remove such applications, follow these steps:

- Go to (Settings) in your account.
- Click on the (Applications and Websites) option.
- From the menu, click on the (Show All) to see Active Apps and Websites.
- Select the suspicious application or website, and then click on the (Remove) button in the top left.
- Confirm whether you also want to (delete all Facebook posts, photos and videos) from these sources.

Damage control:

After doing everything you can to regain control of your Facebook account and prevent further damage, tell your friends and family what happened; This step is a precaution in case the hacker misuses your account.

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?

Below are some simple tips to protect your computer and personal data from cybercrimes:

Keep software and operating system updated

Keeping the software and operating system on your device, such as your computer or phone, updated ensures that you benefit from the latest security patches to protect your electronic devices.

Use anti-virus software and keep it updated

Using an anti-virus program is a smart way to protect your system from malicious attacks. It allows you to scan, detect and remove threats before they become a problem, thus protecting your computer and data from cybercrimes.

Use strong passwords

Make sure you to use strong passwords that are difficult for others to guess, and avoid storing them anywhere. You can also use a reputable password manager to generate strong random passwords; to make it easier for you.

Ignore attachments in spam emails

Attachments in spam emails are a common way to infect a computer with malware and other forms of cybercrime. So never open an attachment from an unknown sender.

Avoid clicking on links in spam emails or on untrusted websites

Another way people fall victim to cybercrime is by clicking on links in spam emails, or unfamiliar websites. Avoid doing this to ensure your online security.

Refrain from providing personal information unless you feel safe

Never provide personal data over the phone or via email to anyone; unless you are absolutely sure the security of line or email. Ensure you are speaking to the person you think you are talking to

Contact companies directly regarding suspicious requests

If a company contacts you and requests personal information or data from you; end the call without giving them anything, then call them again using the number on their official website, to make sure you are speaking to them and not cybercriminals. It is also better to use a different phone number; because cybercriminals can keep the line open.

Pay attention to the URLs of websites you visit

Monitor the URLs of websites you open. . Do they appear legitimate? Avoid clicking on links that contain unfamiliar URLs, or that look like a spam message. If your Internet security product includes features for secure online transactions, make sure to enable them before conducting financial transactions online.

Second:

Dealing with online abuse through social media platforms (Cyberbullying)

What is cyberbullying?

Cyberbullying is bullying using digital technologies. It can occur on social media platforms, messaging platforms, online gaming platforms, smartphones, and involves repeated behavior aimed at intimidating, angering, or defaming the targeted individuals.

Examples of such cyberbullying include:

01

Spreading rumors or posting embarrassing pictures of someone on social media.



02

Sending harmful or abusive messages, images, videos, or making threats through messaging platforms.



03

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 sometimes it's hard to determine whether someone is joking or attempting to cause harm, especially online. It might end with statements like, "I was just kidding," or "Don't take things too seriously." 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. If it continues after you've asked the person to stop, or you feel uncomfortable about it, it might constitute cyberbullying.

How can digital bullying affect my mental health?

The effects of cyberbullying on mental health vary based on the medium used. Cyberbullying via text messages or through images or videos on social media platforms can be very harmful for teens, causing feelings of shame, tension, anxiety or lack of self-confidence about what people say or think about them.

This might lead to isolation from friends and family, negative thoughts and feelings of loneliness, feeling overwhelmed, frequent headaches, nausea, or pain.

Other common effects include school absenteeism, and may influence the adolescents health.

How to deal with cyberbullies

- The first step is to talk to someone you trust, like a friend, family member, school counselor, or another trusted adult.
- If you're uncomfortable talking to someone you know, seek assistance from a helpline available in your country to speak to a professional social worker.
- 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, as social media companies are obligated to maintain the user safety.
- Gathering evidence like text messages or screenshots containing offensive content posted on social media against you, and reporting it can be helpful.
- Think twice before posting or sharing anything online; it might remain on the internet forever, and could be used against you later.
- Do not give any personal details such as your address, phone number, or school name.
- Learn about the privacy settings on your favorite social media apps

Preventive measures against cyberbullying:



Decide who can see your posts or send direct messages about the content you post by adjusting the privacy settings in your account.



You can report hurtful comments, messages and images, and request their removal.



Apart from unfriending, you can also block specific individuals from seeing your account or contacting you



You can also choose to direct comments to specific people; just to show them without completely blocking them out.



You can remove or hide materials from your information that you don't want specific people to see.





Chapter Three

How do I protect myself from digital threats?

- Use passwords to protect data.
- How do you create a strong password?
- Email protection
- Who do I turn to when I am exposed to digital threats?

0 3



First: Using a password to protect data

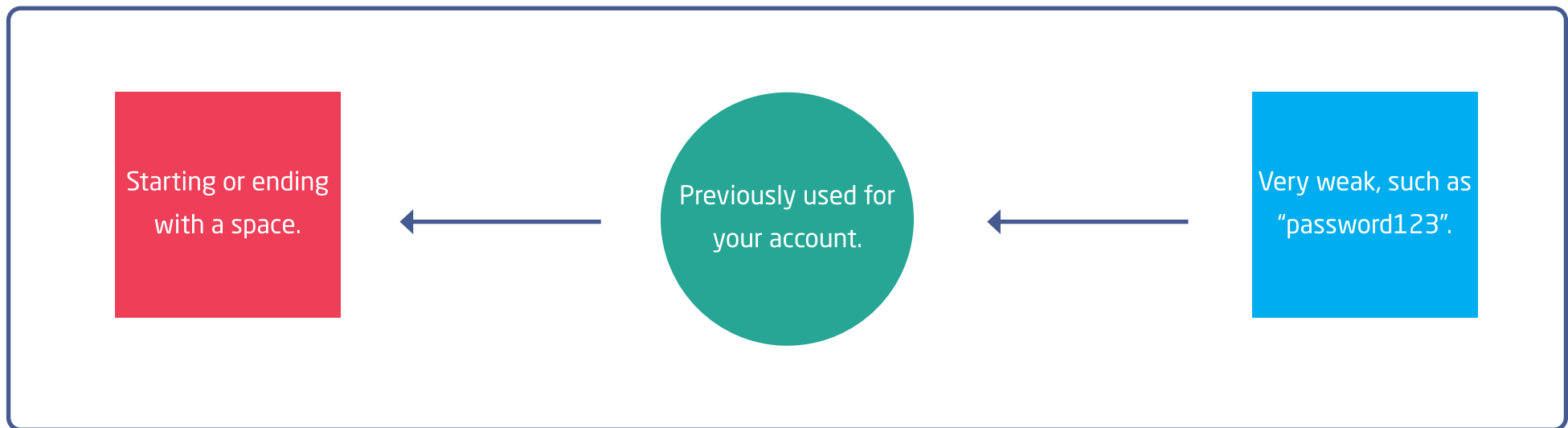
By creating a strong password, internet user can benefit from the following ways:



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.

A password should not be:



To create a strong password, it's preferable to follow these guidelines:

01

A strong password should be easy for you to remember but nearly impossible for anyone else to guess.

02

Use a different password for each important account, such as your email and online pages.

03

It's risky to reuse the same passwords across important accounts; if someone gets the password to one of your accounts; he has access to your email and the rest of your accounts.

04

Use a long password that is easy to remember. Longer passwords are stronger, so the password should be at least 12 characters long

- **Here are some tips to help create long passwords that are easy to remember, such as:**
 - 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 easy passwords that can be predicted or guessed, such as:

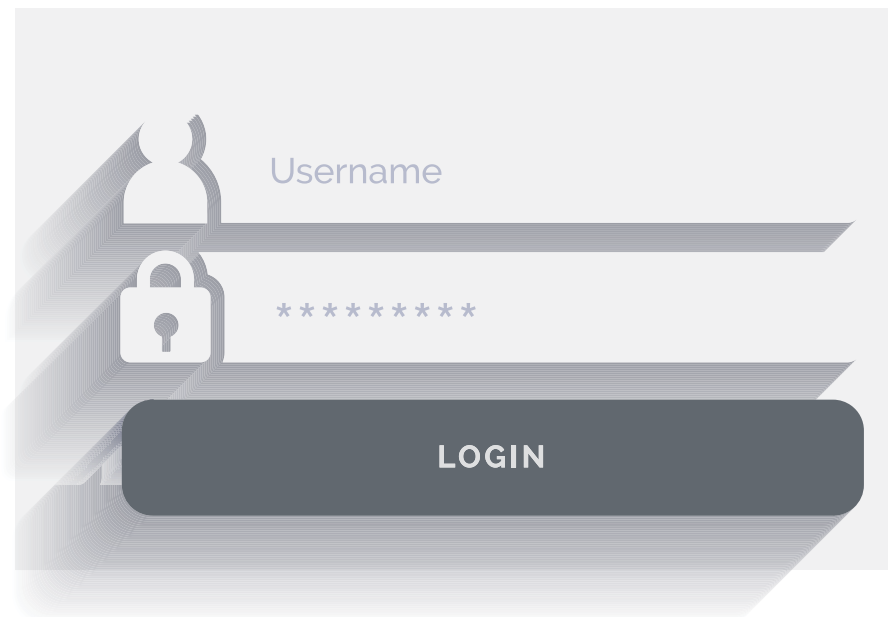
- People who know you.
- Information available through your social media profile.

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.
- **Avoid using simple words, phrases and patterns that are easy to guess. like:**
 - Obvious words and phrases, like "password"
 - Sequential letters or numbers such as "abcd" or "1234"
 - Keyboard patterns, like "qwerty" or "qazwsx"

If you need to write down your password, do not place it on your computer or desk. Ensure any written passwords are stored in a secure or locked place.



Second:

Email Protection

Securing your email from hacking and cybercrime means safeguarding yourself against fraud, scams, and malware, which often executed through tracking emails and links sent to you from someone, thereby gaining access to your information through those details and links sent to you.

Among the crucial steps you should take to protect your email account from hackers and cybercriminals are:

Choosing a strong password

Email accounts with weak passwords are the most vulnerable to hacking, and are often easy to access, Hence, selecting non-guessable, lengthy passwords with a mix of uppercase and lowercase letters, numbers, and symbols is essential.

Activating “Two-Factor Authentication”

It is one of the crucial measures to secure your email account, requiring users to input more than one verification method to gain access. This feature demands both the password and a second

security method, such as sending a text message with a security code to the user’s phone number. Most email service providers offer this feature to all users.

Regularly changing passwords

Regularly changing passwords is one of the most important reasons that can prevent others from accessing or using your account. If someone obtains your previous password, it won’t be your current password.

Using different passwords

Using one password across all sites related to the same email poses a risk to all your accounts, and therefore if the password for one website is hacked, it can be used to access all your accounts on other sites.

Updating installed software

Regularly updating the software on your device is crucial to maintain the security of your account and protect it from being hacked. Where you should continuously updating your email application, internet browser, and any other applications on your device is essential. Additionally, always ensure that your operating system, whether it's Windows or macOS on your computer or Android or iOS on your smartphones, is up to date. These updates usually include security patches and bug fixes for systems and applications.

Blocking spam emails with unknown content

Many hackers exploit emails, text messages, and web pages to hack accounts, and impersonate individuals or organizations, using fake messages containing links or files embedded with viruses and malware, and once they are opened or clicked, your accounts are accessed and your data is stolen.

To avoid this type of hacking; You should avoid opening spam messages, messages with unknown content, and do not open links, suspicious files, and suspicious web pages.

Tracking anonymous emails

You can track emails; if you are not sure of the source of the message and its main purpose; most e-mail service providers allow you to track e-mail messages, identifying their source, which is an important step in dealing with e-mail messages.



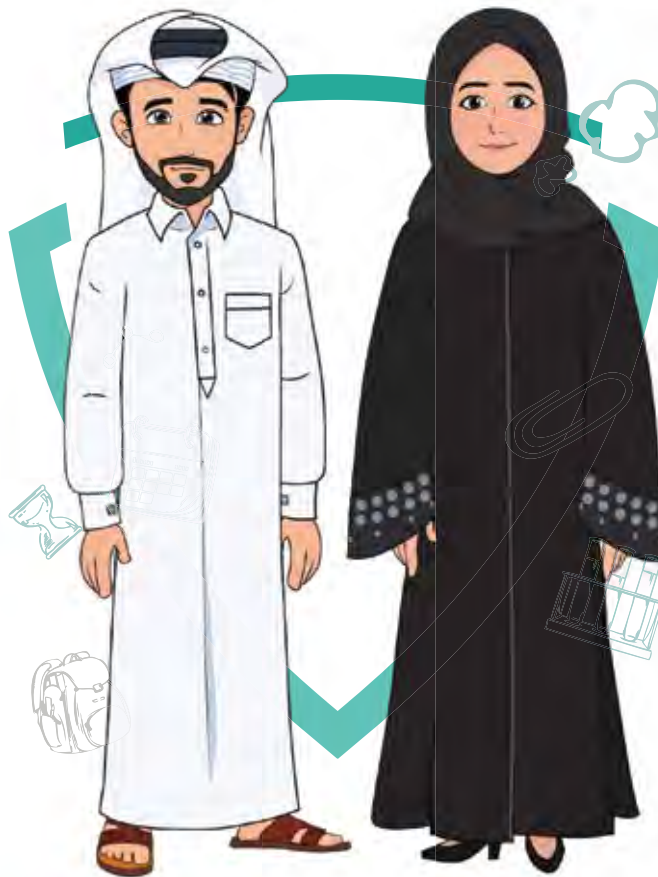
To track emails in Gmail, follow these steps:

- 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.

Knowing that all the previous steps will lead to the addresses being showed, either in a new window or in the Internet address box; where you can see the source of emails before opening them, and if you have any doubts about these messages, you can either unsubscribe from receiving messages from the source, or block the anonymous email source.



Third:

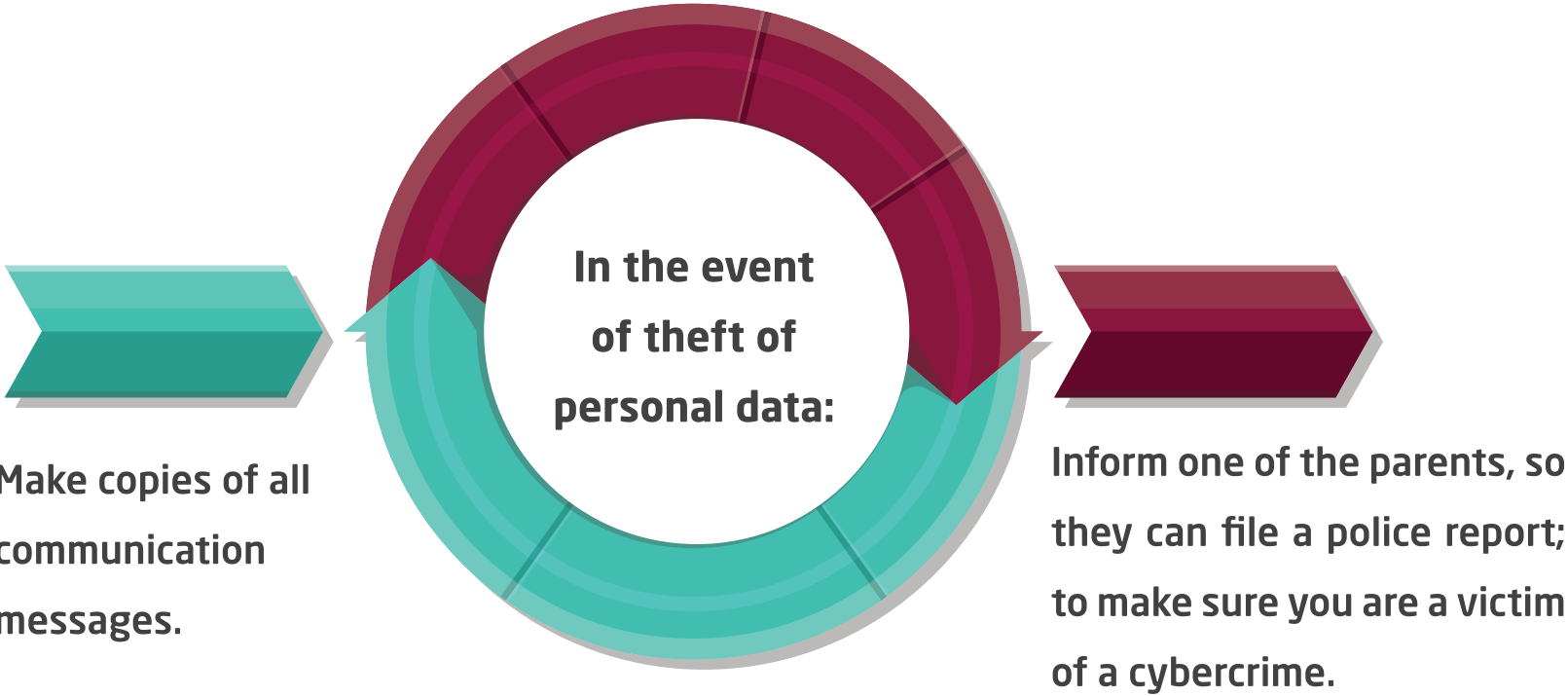
The authorities I turn to when I am exposed to cyber threats

Dealing with cases of cyber blackmail

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.

Protecting personal data from theft



Examples

The examples mentioned below may include information that exceeds the students' ability to understand, so the trainer is requested to present them in a simplified manner. Their aim is to provide facts to the students about the effects caused by cyber-crimes. The examples were expanded and some references were added, so that the trainer could expand the idea and understand it, so that he could provide accurate and simple information at the same time.

First example: "Melissa" virus ⁽¹⁾

In 1999, a virus called "Melissa" appeared, and it was considered the most famous of the viruses that infected electronic devices at that time, after it caused the shutdown of e-mail systems, which were crowded with infected e-mail messages emanating from the virus, causing huge losses.

This virus was sent inside a file called "List.DOC" that contained passwords for 80 malware, and the original form of the virus was sent via email to many people.

The virus infected many devices immediately after it was opened by copying itself via email; It collects the first 50 names from the address list, sends emails to these email addresses, and also hides important files.

The American police arrested the creator of the virus, who called himself "Quigbo," and was sentenced to 40 years in prison and paid a fine of half a million US dollars.

1. Melissa Virus, FBI, on site: <https://cutt.us/m1J9f>

Second example: Morse worm⁽¹⁾

In 1988, (23-year-old) Robert Morris was able to launch the Morse worm virus on the Internet, the first massive cyber attack on the network and caused the infection of six thousands of computers, to which more than 60,000 electronic systems of institutions and government services are linked.

The losses resulting from the “Morse worm” were estimated at approximately 100 million US dollars, until the US government was able to restart the systems again.

Morris was sentenced to 3 years in prison, paid a fine of ten thousand US dollars, and was placed under supervision after his release from prison.

Third example: “Reveton” ransomware⁽²⁾

In 2012, a ransomware called “Reveton” began spreading, which displayed a warning attributed to a law enforcement agency, claiming that the targeted computer had been used for illegal activities. Including downloading unlicensed programs, which is why it is called the “Trojan horse police.”

After informing the user of this, the warning sends a barter message to pay a fine using a prepaid voucher from an anonymous payment service such as Ucash or PacificCard in order for the system to work, and for better targeting, the malware appears on the target device’s screen showing the computer’s IP address, as well as some copies of Footage from the camera. To give the user the illusion that he is being followed.

“Reveton” spread to several European countries in early 2012, and versions of the program varied according to the logos of the law enforcement organizations in each country.

In August 2012, a new version of Reveton began to be published in the United States, claiming to require a \$200 fine for the F.B.I. through the Minipak card.

In February 2013, the Spanish authorities arrested a Russian citizen in Dubai. For his association with a crime network that uses the malware “Reveton”, 10 others were arrested in August 2014.

1. From the Morris worm to targeting facilities... Learn about the five generations of cyber threats, Al Jazeera, December 15, 2019, available at the link: <https://cutt.us/1B445>
2. Lessing, Marlese. (2020). Case Study: Reveton Ransomware, SDXCENTRAL, on site: <https://cutt.us/2IICN>

Fourth example: Regin⁽¹⁾

Regin is a sophisticated malware that was revealed in November 2014, targeting those who use computers based on the Microsoft Windows system.

It has infected many devices in the world:

- 28% in Russia
- 24% in Saudi Arabia.
- 9% in both Mexico and Ireland.
- 5% in India, Afghanistan, Iran, Belgium, Austria and Pakistan.

The main victims of this malware are ordinary individuals, small businesses, and telecommunications companies.

1. Het Regin-platform, Kaspersky, on site: <https://cutt.us/nYOFi>

Fifth example: A list of passwords that can be hacked

A team of researchers from Nord Pass has published a warning to users: To verify their settings, the reason is to use known passwords such as "123456", "qwerty", "password".

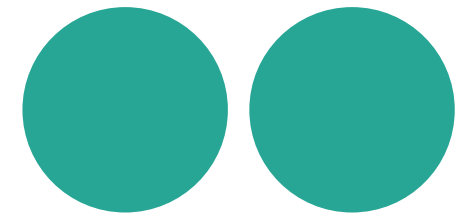
Here are the top 10 most common passwords around the world:

- dolphin
- 123456
- 123456789
- 111111
- 12345
- 12345678
- password
- Qwerty
- 1234567
- 123123

The more your password resembles regular word patterns; The repetition tool takes too long to guess.

There are password formulas that are difficult to guess based on the previous example, such as:

- Cat.lov3r
- CAt.lov3r
- i7ovemyCat !!
- C0tsaremybestfr13nds
- sn00pdoggycat



Trainings and Exercises



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 primary 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 primary 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.

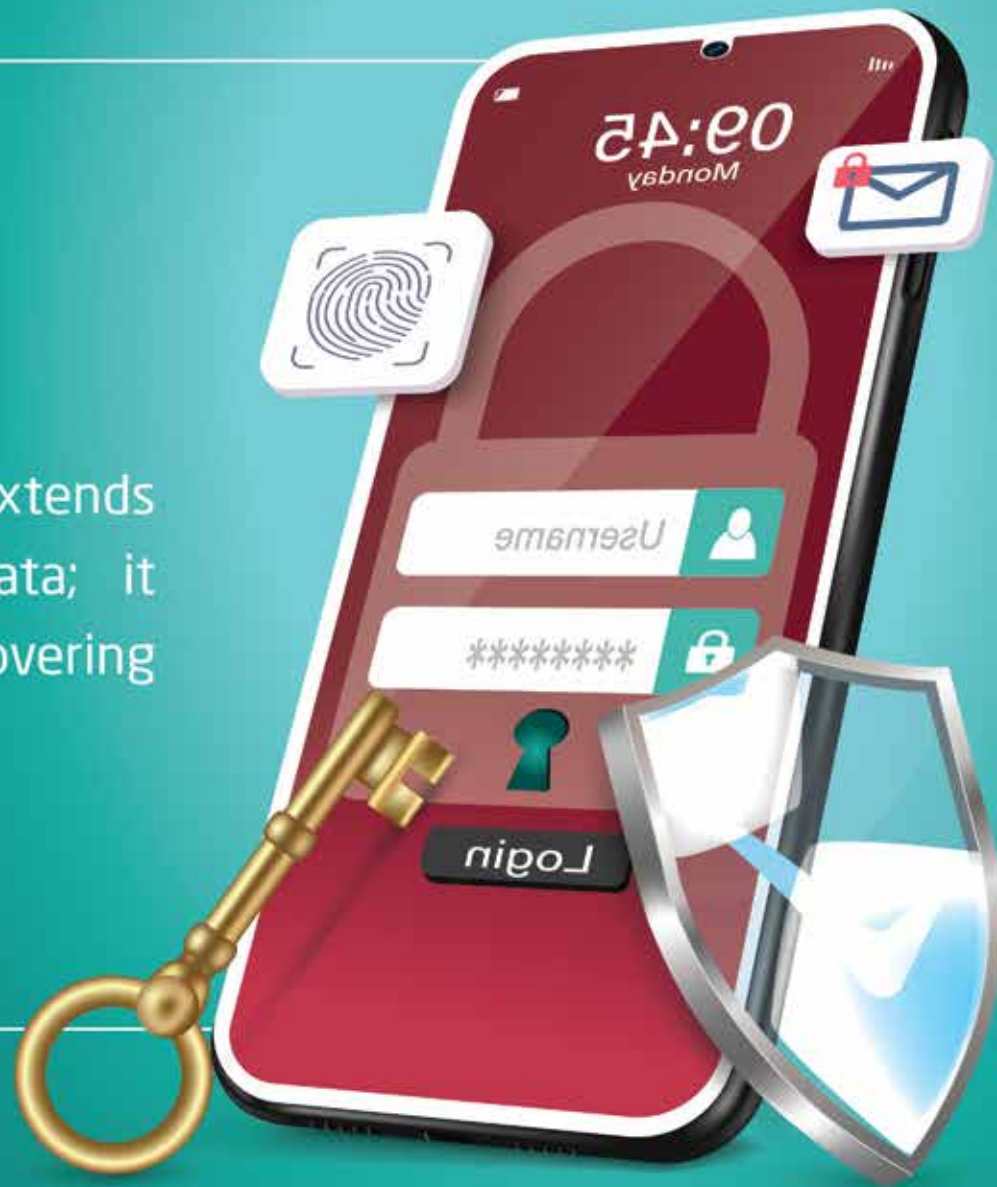


First: in-classroom Exercises

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.

Do you know ?

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





Exercise 1

Identify the true and false 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.



PASSWORD PROTECTED



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.

Exercise 2

Match the terms from column (A) with their corresponding meanings in 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



Leads to social isolation.

Depression and anxiety and stress.

Hacking attempts and data theft on websites.

Is a punishable crime by law.

Leads to ethical, psychological, and physiological issues.

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

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

Because openness to other cultures without controls can lead to the acquisition of what is not appropriate for our culture, and is incompatible with our religious and cultural beliefs.

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.



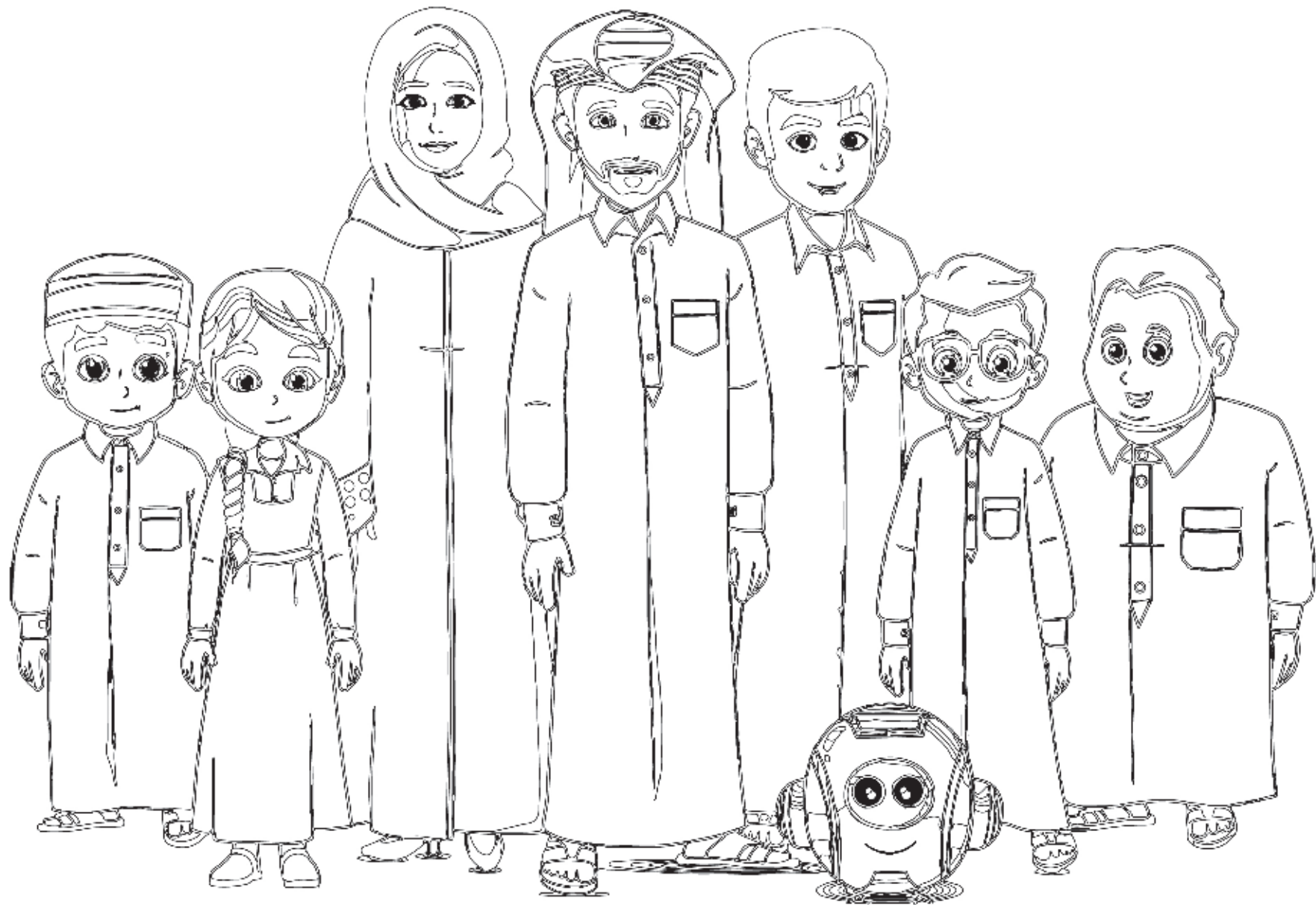


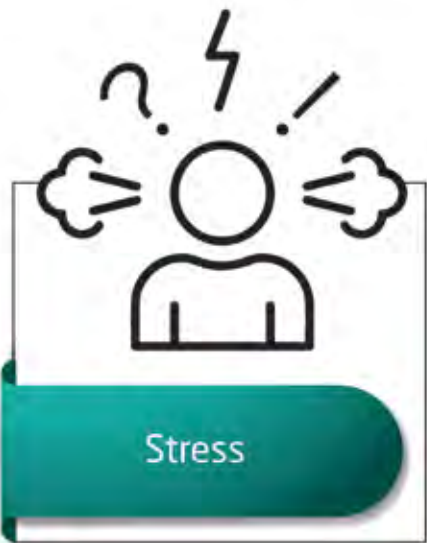


Pay Attention!

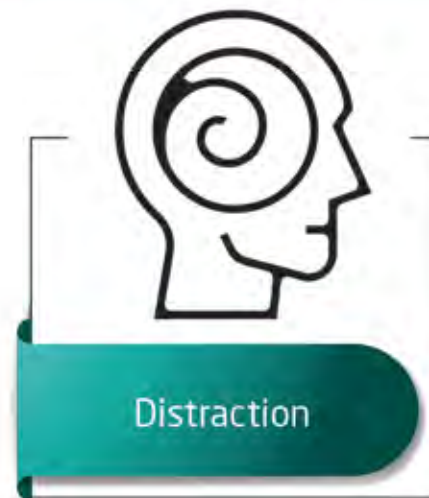
Failing to update the systems of smart devices, whether they be personal computers, phones, or tablets, exposes them to numerous vulnerabilities exploited by device hackers for data theft and device compromise.







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.





Wanting to leave school



Avoiding friends



Ability to face



Low grades



Loss of self-esteem



Sleep problems



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

Read the passwords below carefully, and think whether these words considered a strong password or not.



Medo123

Password

123456

654321

Penten

Me@12do

2020MMeeDDoo\$%

123medo

Pass123

Klmetser

Pay Attention!

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



Exercise 6

Choose the correct answer below:



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.



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 - Problem - Protection - Thieves - 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.

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?

Correct

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?

Correct

There is no problem with data theft.

Incorrect

The hacker cannot benefit from the data he stole.

Incorrect

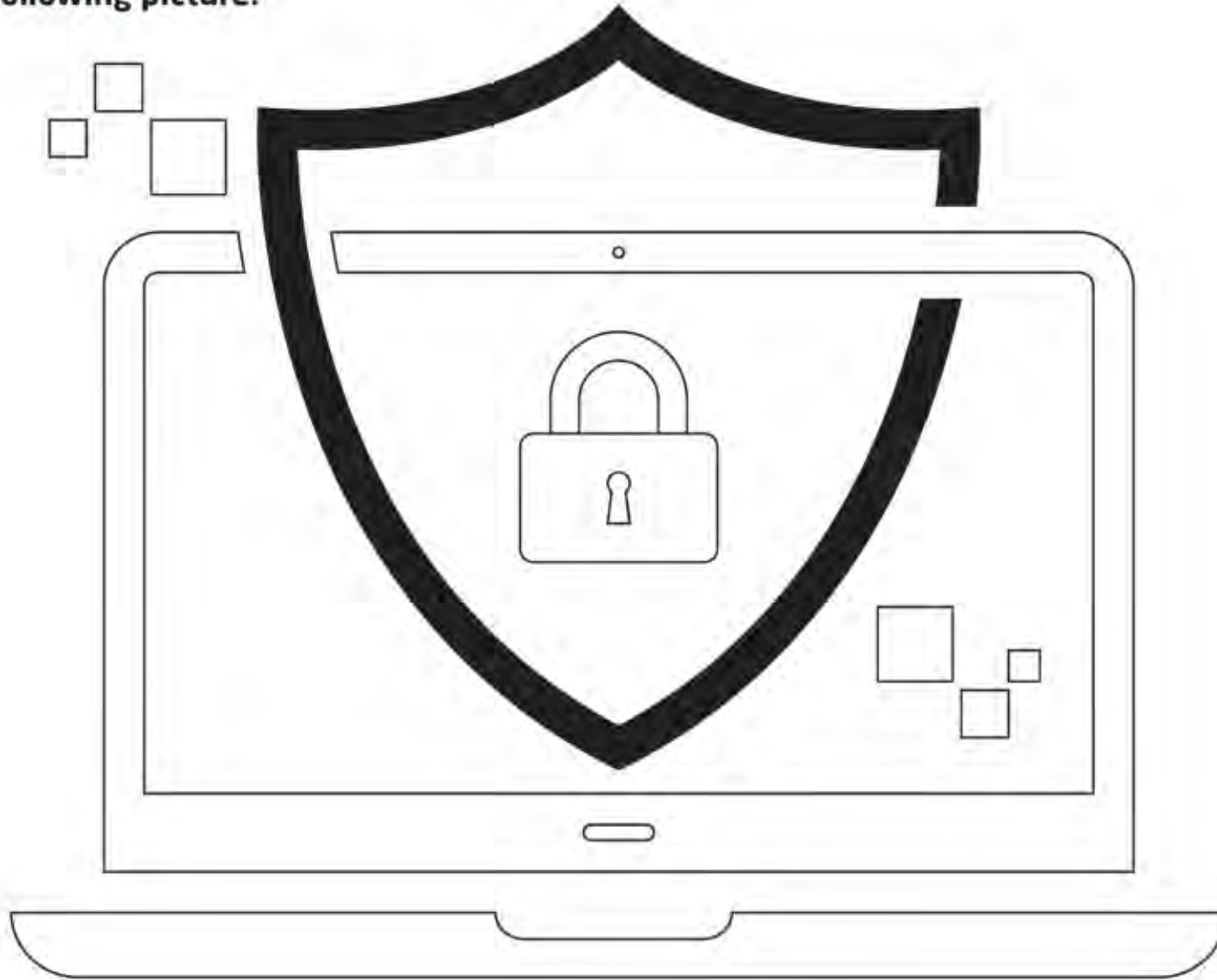
You should choose simple passwords that can be easily guessed.

Incorrect

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.	Correct
No human error can lead to data theft.	Incorrect
Downloads are always safe, and devices cannot be hacked or have data stolen through them.	Incorrect
Problems in databases or servers can result in data theft and make it easy for hackers to access networks or devices.	Correct
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.	Correct
Sometimes theft of phones or computers causes data leakage.	Correct
Using public Wi-Fi networks or computers in public places such as libraries or Internet cafés may expose data to the risk of theft.	Correct
Companies or organizations do not need to secure databases or servers in order to protect customer data.	Incorrect

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:

I use the same letters as the username.	
I use a diverse set of letters and numbers.	Correct
I use my birthday.	
I use a combination of uppercase and lowercase letters and some symbols.	Correct
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.





Discuss the following questions with your colleagues

01

Cybersecurity is also called

(Number of letters 16) (**Computer security**)

02

Length of strong password

(Number of letters: 9 letters) (**12 letters**)

03

People who cause serious harm to our electronic devices

(Number of letters 7 letters) (**hackers**)

04

One of the types of cybersecurity

(Number of letters: 13 letters) (**Cloud security**)

05

One of the examples of intellectual property rights

(Number of letters: 12 letters) (**The trademark**)

Puzzles

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

Phishing Emails

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

Friend requests on social media platforms

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

Cybersecurity

An advanced form of transnational crime that occurs in cyberspace.

Cybercrime

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

Cyberbullying

The password consists of

A combination of letters, numbers and symbols





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:



Graduation project



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.

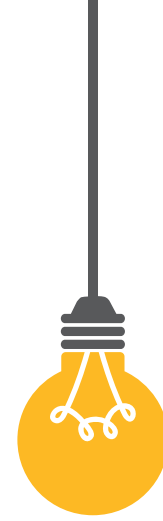
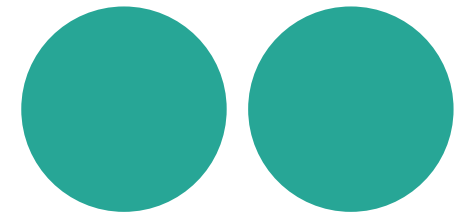


The student takes on the role of the trainer and writes general guidelines for his colleagues or parents, explaining the procedures required to prevent the digital risks.





References



Arabic References:

1. Al- Otaybi, Mead (2017), Basics in Cybersecurity, available at the link:<https://www.docdroid.net/1BTYYas/asasyat-fy-alamn-alsybra-ny-pdf>
2. From the Morris worm to targeting facilities... Learn about the five generations of cyber threats, Al Jazeera, December 15, 2019, available at the link: <https://cutt.us/1B445>
3. Youssef, Amir. (2015AD). Information technology crimes in the Arab Gulf States, and international and local efforts to combat them, Internet and electronic computer crimes in the Arab Gulf States. Egypt: Dar Al-Kutub Al-Arabiyya. pp. 68-74
6. Melissa Virus, FBI, on site: <https://cutt.us/m1J9f>
7. Person, Tim, P. and Jordan, T. (2017) A sociology of hackers: 10: Cyberspace crime: Tim Jordan, Paul Tayl, Taylor & Francis. On site: <https://cutt.us/NwnyZ>
8. Sarker, I.H. and Kayes, A.S.M. (2020) Cybersecurity Data Science: An overview from machine learning perspective - journal of big data, SpringerLink. On site: <https://link.springer.com/article/10.1186/s40537-020-00318-5>
9. Smith, A.D. and Rupp, W.T. (2002), «Issues in cybersecurity; understanding the potential risks associated with hackers/crackers», Information Management & Computer Security, Vol. 10 No. 4, pp. 178-183.

English References:

4. Het Regin-platform, Kaspersky, on site: <https://cutt.us/nYOFi>
5. Lessing, Marlese. (2020). Case Study: Reveton Ransomware, SDXCENTRAL, on site: <https://cutt.us/2IICN>
10. yagibca, prateekt (2023) Cyber Security, types and importance, GeeksforGeeks. On site: <https://www.geeksforgeeks.org/cyber-security-types-and-importance/>





CyberEco



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency