الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

CyberEco
معًا لدعم السلامة الرقمية
Together to support digital safety

Parents' Guide

Tailored to the training content

CyberEco

Intellectual Property rights

December, 2023

Doha, Qata

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

Index

Introduction

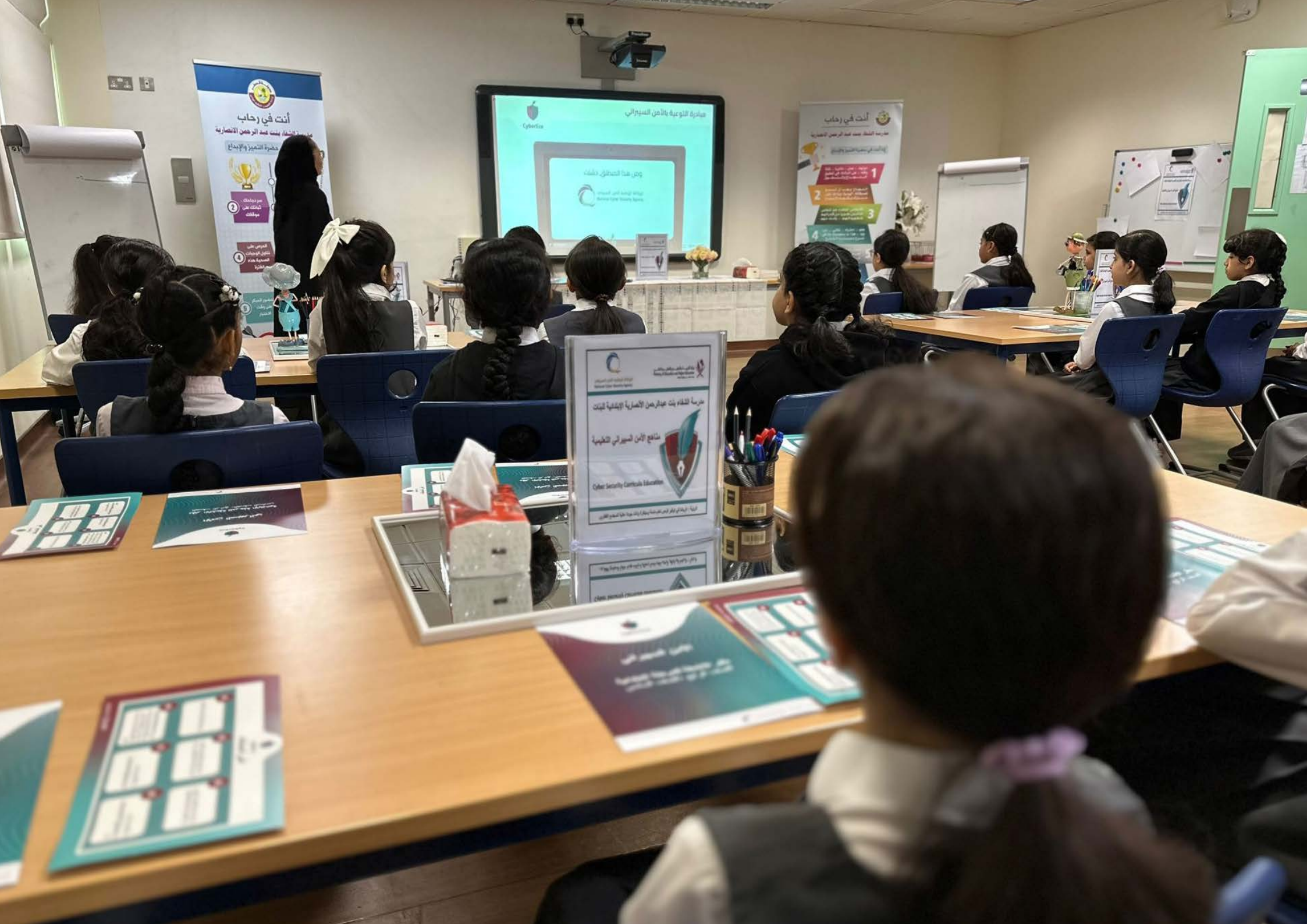
The Internet has witnessed rapid and widespread development, becoming an integral part of the lives of nations, communities, and individuals. According to international reports and studies, digital threats pose the greatest risk to children and adolescents. This holds true in Qatar, especially considering that these groups have limited experience in dealing with Internet risks.

As part of the National Cyber Security Agency's efforts to enhance digital security, at all social levels particularly for children and adolescents.

The project of field visits to schools has emerged as a tangible tool and operational starting point. The aim is to enhance student's awareness of cybersecurity and digital safety concepts by delivering targeted awareness training content to students from the first grade of primary school to the twelfth year of high school, as well as educational and teaching staff and parents. The project focuses on organizing field visits to both public and private schools in the state, contributing to the enhancement of the cyber curricula through innovative training and awareness content delivered during various workshops as part of the visitation program.

First axis

CyberEco Project


أنت في رحاب
مبادرة التوعية بالأمن السيبراني
Cyberfox
مدرسة الشفاء بنت عبدالرحمن الأنصارية الابتدائية للبنات
منافع الأمن السيبراني التعليمية
Cyber Security Curricula Education

Overview of the project

The fundamental concept of the CyberEco project is to elevate students' awareness of cybersecurity and digital safety concepts by delivering awareness-raising training content to all students in schools across various educational levels. This is achieved through interactive activities that ensure students' engagement and alignment. The project's approach completely departs from rote learning or traditional content; instead, it relies on new and innovative methods. These include interactive training, adopting training methods based on educational games, utilizing educational videos, and organizing competitions.

Meaning of the Project Name

"CyberEco" The name of the project is divided into two parts: the first is Cyber, which expresses the digital world and electronic space, which has become the most important feature of the era, and the second part is "Eco", which is an abbreviation of the word Ecosystem, which means environmental system, and thus the full name CyberEco refers to building a cyber environment surrounding students.

Target Audiences

- Students in public and private schools and at all educational levels.
- Teachers and educational staff.
- Parents.

Project vision

Transforming digital safety into a sustainable practice for children and adolescents in the State of Qatar.

Project message

Enhancing the awareness of school students in the State of Qatar about the concepts of cybersecurity and digital safety.

Project Goals

- Increase awareness among the target audience about cybersecurity concepts and digital safety.
- Offer interactive training and awareness content for students.
- Develop digital talents among students.
- Strengthen communication between staff and parents.
- Enhance cybersecurity and digital safety indicators in Qatar.

Significance of the Project

- Increase global interest in the idea of educating children and adolescents in this vital, strategic field.
- The necessity of expanding awareness of this field and introducing students to the meaning of responsible use and security of information and communications technology.
- Training and educating Qatari youth to deal efficiently and professionally with all forms of digital technology so that they become the core of specialized experts in this field in the future.
- The need to keep pace with the continuous and rapid development in training and qualification tools, especially in the field of cybersecurity.

Expected outcomes of the project

- Enhancing the scientific content of cybersecurity curricula for school students with diverse and distinct interactive training content.
- Providing a state of constant competition among students for innovation in the cyber field, and motivating them to submit innovative project ideas.
- Reducing the rates of negative issues associated with the use of the Internet among students.
- Supporting the state's national plans to build and support cyber talent among school students.
- Consolidating the reality of the State of Qatar as a distinguished country in the field of digital safety and child safety on the Internet.
- Establishing a culture of digital safety among various social segments in the State of Qatar, especially among children and youth.

Second axis

Parents' Guide

Parents are crucial stakeholders in the CyberEco project, given their continuous interaction with their children, which allows them to directly contribute to the project's success and goals. This guide serves as a general reference for parents, providing insights into how to interact and collaborate with the project. It also emphasizes the importance of their engagement with their children and highlights the significance of communication with educators to achieve the best possible results from the project.

The concept of the guide and its significance

The guide revolves around the significant role of parents in fostering digital literacy for students. As the closest familial figures, parents play a pivotal role in motivating student collaboration and interaction with the training content provided within the project. The collaboration and interaction of students with the trainers are crucial factors contributing to the project's success and goal achievement.

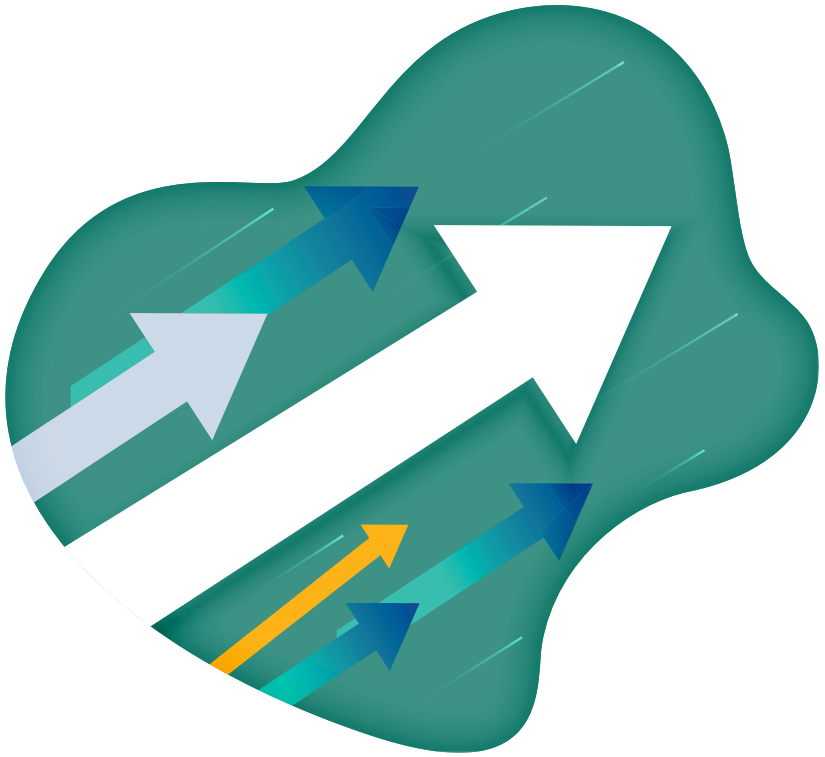
The scope of the guide extends to encompass the importance of furnishing parents with comprehensive information about the project. The anticipated guidance and support from parents hinge on their thorough understanding of the project's nature, significance, goals, and the overall content of its training. Consequently, the guide aims to acquaint parents with various pertinent details about the project in both its general and specific contexts. It seeks to clarify the expected roles of parents and students and offers general guidance on how to interact and collaborate with the project and its staff.

The following points highlight the guide's significance:

- It serves as a primary tool for equiping parents with detailed information about the project, its goals, its significance, and the nature of its training and awareness content.
- It addresses the need to provide parents with detailed information about the role expected of them in the context of project implementation.
- The comprehensive success of the project necessitates full cooperation between the parents and the class teachers, and the guide serves as a major tool in directing and organizing this cooperation.
- It is necessary to involve parents in the project, given their proximity to their children and better understanding of their educational needs. The guide explains how to manage and organize their role in the project.
- It is crucial for parents to continue guiding and directing students in digital literacy even after the project concludes. The guide serves as an introduction to clarify their ongoing role in monitoring students' digital guidance.

Goals of the guide

- Offer parents accurate and detailed information about the project, including its objectives and tools.
- Clarify parents' expected role within the project and demonstrate how they can effectively fulfill it to enhance success and goal achievement.
- Highlight the foundations of collaboration between parents and the project implementation team to ensure the best possible outcomes.
- Ensure high levels of collaboration and interaction between students and the project implementation team by providing parents with general information and guidance on this matter.



Foundations and principles of interaction with the guide

- Understanding the details of the CyberEco project, including its goals, importance, mission, and vision, requires accurately comprehending the information provided in the first section of this guide.
- Complete awareness of the tasks expected of parents, a thorough understanding of these tasks, and readiness to undertake them, as detailed in the context of the fifth axis of this guide.
- A broad overview of the key topics covered in each training workshop, enabling the parents to gain a general understanding of the context of the training content presented in each workshop. This information is detailed in the fourth section of this guide.

Third axis

Educational characteristics of participants


معرض أبحاث الطلبة الداخلي ٢٠٢٢ - ٢٠٢٣
لمدارس منطقة الجنوب و شقيصة
مدرسة
عبد الله بن على المسند الثانوية لبنين
مدرسة عبد الله بن علي المسند الثانوية لمستقلة البنين
ABDULLAH BIN ALI AL MISNAD SEC. SCHOOL FOR BOYS
مركز مصادر التعلم
سياسة استعارة مصادر المعلومات بمركز مصادر التعلم
PUSH BAR TO

By educational characteristics, we refer to the unique differences that distinguish each educational stage. These differences are linked to experiences and behaviors specific to each stage, necessitating the use of methods tailored to the targeted educational stages of the project. Given that education and training in this initiative rely on interaction and various interactive tools, specific instruments suitable for each stage are required. This section of the guide will elaborate on the educational and cognitive characteristics of each stage of education.

Primary school

Nature of the stage:

This stage spans from the age of six to twelve and is considered the most crucial in a child's life. It is during this period that children are instilled with good behavior and acquire knowledge about various aspects of their surroundings, whether at home with the family, at school, or even on the Internet.

During this stage, the child commences formal education, and his perspectives undergo transformation as he learns and interacts with various individuals. At this age, children are highly impressionable, quickly absorbing and internalizing everything they encounter. Although education during this phase is generally considered more straightforward than in earlier years, it necessitates a considerable amount of calm and patience. This is because children at this age are not yet familiar with many skills and, therefore, need to learn and practice them without undue pressure.

Middle school

Nature of the stage:

The stage of adolescence is also known as the transitional phase between children in the primary stage and young people in the secondary stage. It is a period during which students undergo numerous changes in terms of appearance, personality, mental and emotional aspects, as well as social status. Naturally, this stage is accompanied by hormonal changes **and is characterized by the following features:**

- The student started to perceive the world around him with a greater sense of realism.
- He starts to realize that his actions have long-term consequences.
- Numerous subjects have become unclear to him, and he requires assistance in comprehending them through unconventional means.
- Develops concrete thinking, enabling the grasp of concise concepts and symbols.
- He exhibits a selfish tendency and may overlook the feelings of others.

High school

Nature of the stage:

At this stage, the student undergoes full development and enters the stage of youth, leading to certain behavioral changes, the most notable of which include:

- The inclination to rebel and disengage from studies.
- Resorting to defensive tactics to avoid tasks, particularly academic ones.
- Displaying a state of inattention and neglect.
- Intense emotions, heightened tension, and occasional irritability.

At this stage, students' enthusiasm for computers and the Internet grows, leading to a profound understanding of their activities. Therefore, it is essential to be well-prepared for cognitive interaction with them.

Fourth axis

Training Topics

In this section of the guide, a summary of the training topics directed at the target audience of the "CyberEco" field visits project will be provided. The training topics will be categorized according to educational stages. Recognizing the significance of parents' awareness of the training content for the project's target audience, this section will offer concise information about the training topics and the key information imparted by the project team.

Primary school

At this stage, digital training will be offered with two axes: cybersecurity risks and cyberbullying and how to face it. **Here is a summary of the key information that will be provided on this two axes:**

The first training kit

Cybersecurity Risks

- Chapter One: The Concept of Cyber security and Digital Safety
- Chapter Two: The risks associated with cybersecurity
- Chapter Three: How do I protect myself from digital threats?


مدرسة عبدالله بن علي المسند الإعدادية
ترحب بالسادة الضيوف من
الوكالة الوطنية للأمن السيبراني
مجلس القراء
مركز مصادر التعلم
CyberEco
PII
الاسم
أرقام التعريف الشخصية
معلومات العنوان الشخصي
القراءة هي متعة التجول في عقول الآخرين

There are always many risks that lurk for Internet users. These risks can cause major problems in the assets or data of users, and they are often intentional and targeted for the purpose of stealing money or information and data.

Chapter One: The Concept of Cyber security and Digital Safety

Cyber security:

Cyber security is all the practices that are used to protect computer devices, networks, software applications, critical systems, and data from potential digital threats. The responsibility for this protection lies with institutions, especially those that have customer data, which must rely on measures and tools that help them ensure cyber security and protect sensitive data from all unauthorized access attempts.

As for digital safety, it is:

All activities and measures aimed at protecting your personal data and digital assets online, as well as digital safety, are part of cybersecurity. Cybersecurity is a broader and more comprehensive concept, occupying a wider space in digital protection, encompassing the safeguarding of networks, operating systems, and the data stored within them from unauthorized access, tampering, or breaches.

Chapter Two: The risks associated with cybersecurity

The internet has become an integral part of the daily lives of most of the world's population. The internet can be used for many things on a daily basis, but with the increasing reliance on the internet, many cybercrimes have emerged, which occur in the digital space, and despite that, their risks extend to the real world.

Internet risks

- **Cyberbullying,** which is being subjected to ridicule on the internet, whether in the conversations exchanged on social media platforms or in the comments on posts and photos, or through games.
- **Share private information,** many children fall into this problem due to their lack of awareness of the limits that must be aware during posting on the internet. There is a lot of private information and data that should not be shared with others, such as home address, school name, area of residence, and especially public ones.
- **Phishing,** which is a type of hacking that relies on deceiving users to open a link or attachments in an email, and then the hack occurs, which can be used to monitor users, or to access a lot of data and information that may cause a real danger to the life of the user and all those around him.
- **Scams,** which include deceptive messages that can reach through a computer, smartphone, or tablet for a free game, or a new phone gift for a small fee, and so the user sends credit card numbers, and instead of receiving a gift, the balance is withdrawn from him without a return.
- **Malwares,** This software can be downloaded without the user's consent or permission. This software causes major damage to computer devices, phones, tablets or any device connected to the internet, because it may cause data theft, or threatening in order to obtain a ransom, or other problems that may be caused by this programs.

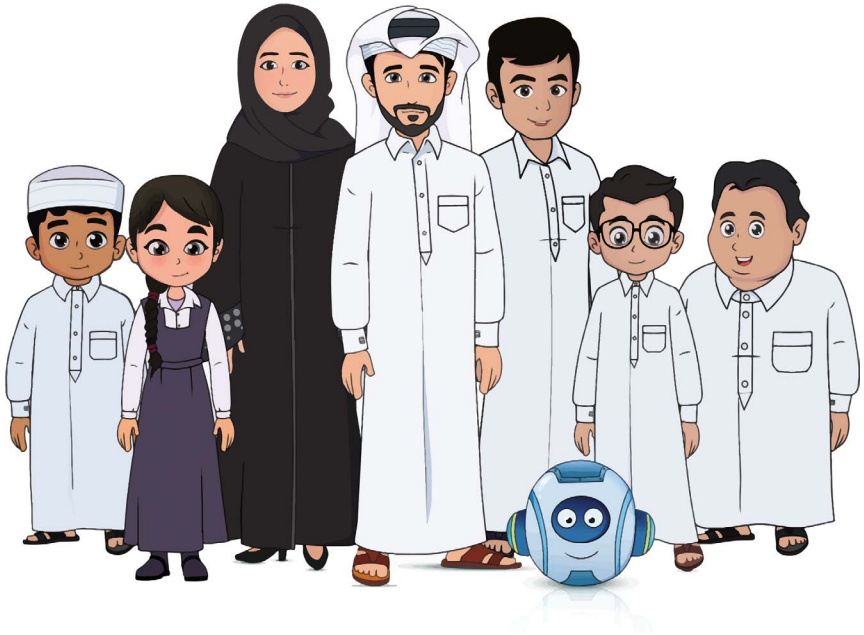
Risks of personal data theft

Data or information theft involves the illegal transfer of personal, confidential, or financial information.

The most important data that are targeted for theft by hackers:

- Bank account information.
- Passwords.
- Passport numbers.
- Driver's license numbers.
- Social security numbers.
- Medical reports.
- Subscription Information.

The information that has been stolen is often sold, or can be exploited to obtain financial profits from this theft, especially bank accounts.



As for the way data is stolen, it often occurs in one of the following ways:

- **Social engineering,** with its most common form being phishing, involves disguising as a trusted entity or organization to deceive the victim into opening a particular message.
- **Weak passwords** that are easy to guess or expect.
- **Security loopholes,** which may be caused by unsafe or poorly designed applications or programs, which data thieves exploit in order to enter and steal user's data.
- **Human errors,** the theft may have occurred due to a leak from the data owner himself, who shared his data without realizing that there was a risk in the matter, and that data may have accidentally reached the wrong hands, which led to its leak.
- **Information that is publicly available,** which is often found in posts on various social media platforms in which people freely share many personal data and information that can reveal a lot about them, without even realizing it.

Risks of data theft

- Data theft can lead to the leakage of client's data in companies and institutions.
- Attackers can demand a large ransom.
- Damage to reputation and loss of trust.
- Costs related to retrieving data or re-securing servers and databases.
- Wasting time due to systems crashing during and after hacking process.
- Financial costs due to theft of banking data.
- Psychological damage that may result from the theft of data and information.

Risks of Cyberbullying

Cyberbullying is the exploitation of the Internet and all modern technological techniques in order to harm another person or persons in a deliberate and repeated manner. Bullying is unwanted and passive aggressive behavior, but this time it takes place on cyberspace through messages, comments, on social media platforms or websites, its primary goal is to harm and abuse the victim, whether in a material, moral, social or psychological way

Cyberbullying has many forms; the most important of them are:

- **Harassment and annoying,** by sending offensive or inappropriate messages, whether socially or morally, or perhaps writing negative, insulting comments on everything the victim shares on social media platforms.
- **Defaming reputation,** which is simply posting incorrect information or fake rumors about other people with the aim of ridicule or distorting reputation.
- **Identity Theft,** which occurs when a person hacks into another person's account and begins using their account and writing and sharing embarrassing and offensive things and materials.
- **Electronic stalking,** which means sending electronic messages repeatedly with the aim of threatening, harassing or intimidating, and causing the victim to feel fear and anxiety.
- **Electronic ostracism and exclusion,** this occurs when someone is deliberately left out of the group or excluded from a game, and this is considered a form of social bullying.
- **Electronic hacking,** which relying on malware programs or stealing passwords in order to control the victim's accounts or devices.
- **Bullying through photos,** is publishing inappropriate photos of the victim, or photographing the victim without his awareness and publishing the photos on social media platforms.
- **Spaying,** through the use of specific applications that attempt to hack the privacy of others by deceiving them, after which the bully publishes that private information and sends it to others to harm the victim.

As for the risks of bullying:

- Making the victim feel lonely, isolated, and wanting to completely stay away from gatherings and stay with others.
- Feeling ashamed, and thus feeling anxious, distressed and embarrassed.
- Loss of self-confidence as well as trust in others.
- Low self-esteem and feelings of inadequacy and lack of value and importance.
- Some health problems of the victims; especially those related to food and sleep.
- Delay in academic achievement or commitment to work.
- Feeling of constant fear and insecurity.

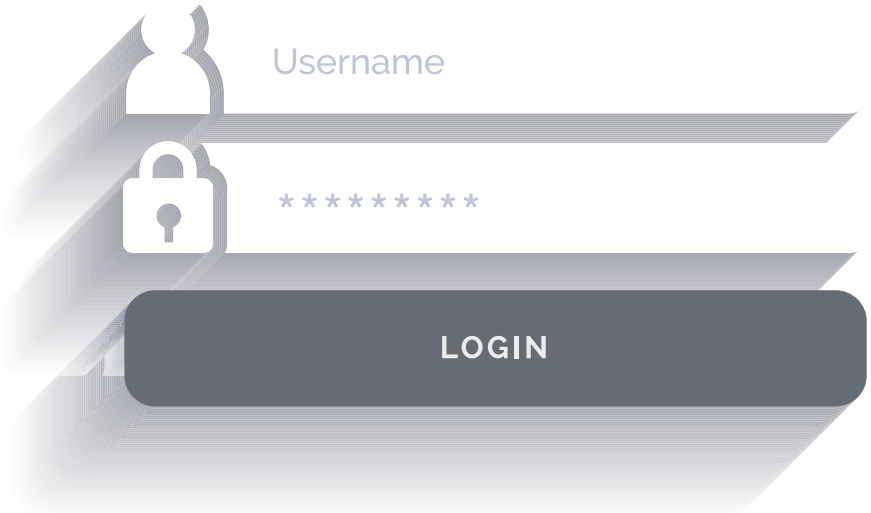
Chapter Three: How do I protect myself from digital threats?

Use strong passwords to protect data

Using a strong password helps keep personal information and emails secure, as well as protect files and other data.

How to write a strong password

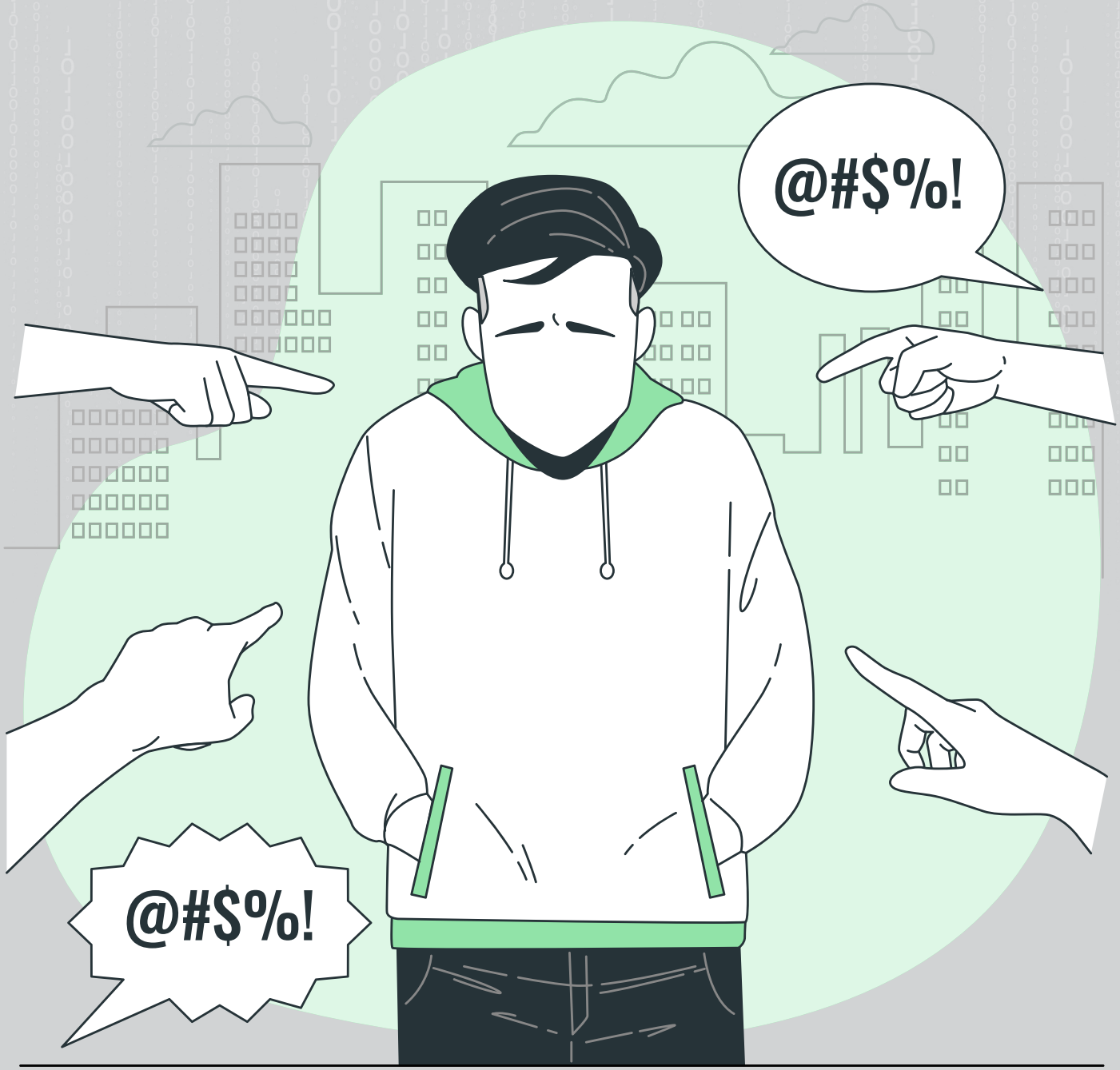
- It must consist of more than 1012- letters and numbers.
- It is preferable to use symbols, letters and numbers.
- It is important to use uppercase and lowercase.
- Avoid using date of birth, or distinct dates.
- Avoid using the word Password.
- Avoid linking all accounts with one password.
- Do not use personal data or common words.
- Use a password that is memorable and cannot be guessed by others.
- Use two-step verification, or add a personalized password recovery email.



The second training kit

Cyberbullying and How to face it

- **Chapter One:** The concept of cyberbullying
- **Chapter Two:** How to face the risks of cyberbullying



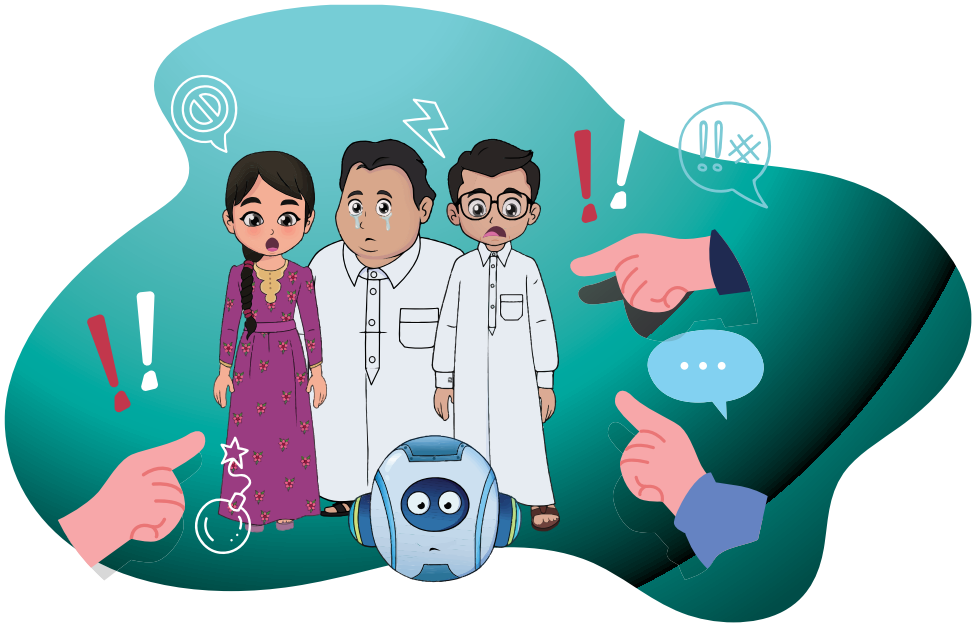
Cyberbullying has become one of the most prominent dangers on the Internet, especially towards children. Therefore, it is necessary to educate children about cyberbullying and teach them to completely reject this behavior from a young age.

Chapter One: The concept of cyberbullying

Most Internet users are exposed to cyberbullying, which often appears in conversations exchanged over the Internet, or in comments on posts on social networking sites, but children are often the most vulnerable to this type of behavior, and unfortunately they are greatly affected by this content, and some of them may even go so far as to suffer from depression.

What is cyberbullying?

Cyberbullying is the use of the Internet or modern technologies in order to harm or harm specific people in a deliberate, repetitive, and hostile manner. Bullying in general is unwanted, passive aggressive behavior, but this time it takes place through cyberspace and modern technological tools, through messages or comments on platforms Social media or Internet sites, the goal of which is to harm and abuse victims.



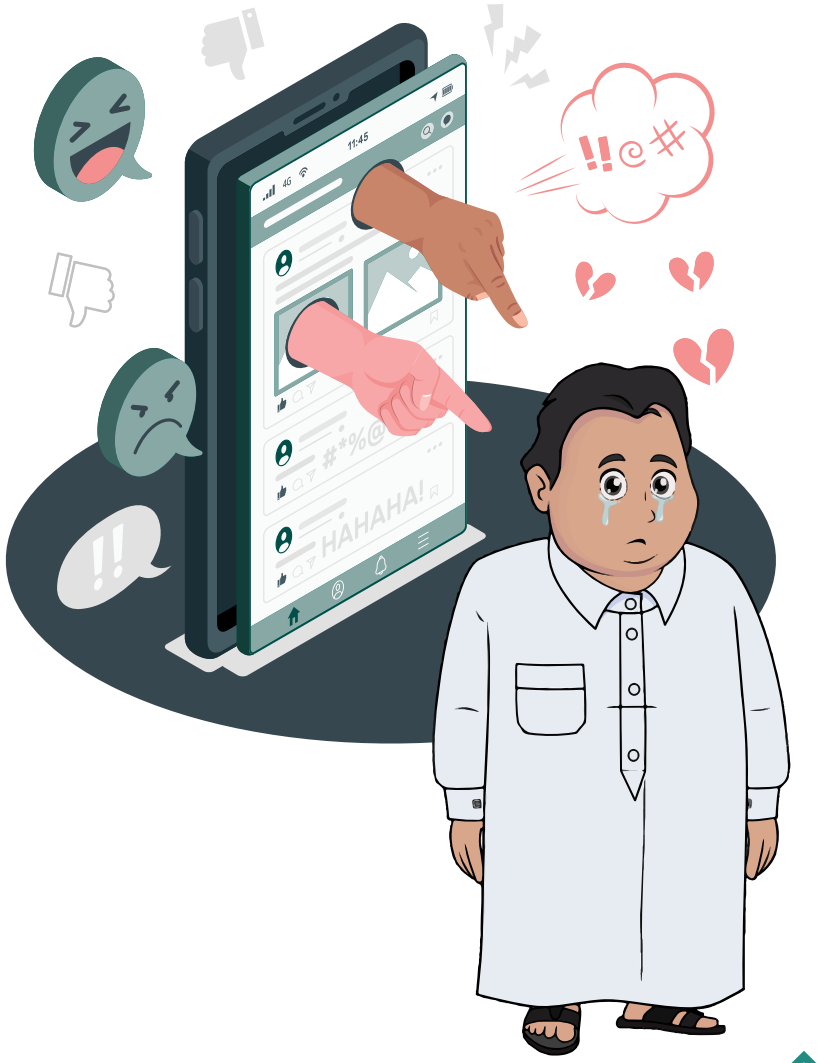
What are the manifestations and forms of cyberbullying?

- **Annoying:** This is by annoying the victim by sending annoying or offensive messages, or commenting offensively on the victim's posts on social media.
- **Bullying through photos:** This form of bullying occurs by publishing photos of the victim without his consent on social media platforms, or publishing inappropriate photos.
- **Spaying:** through special spaying programs, the aim of which is to know details about the victim's private life, and use them to blackmail or disturb him.
- **Damage to reputation:** by spreading rumors or incorrect information; with the aim of bullying and abusing the victim.
- **Stalking:** It is called electronic stalking, and this type of bullying occurs by sending threatening or annoying messages to the victim on a continuous basis, and through several platforms, such as e-mail or social media platforms.
- **Identity theft:** This type of bullying occurs through either hacking into one of the victim's personal accounts and publishing in his name, or through creating new pages and websites and claiming that they belong to the victim, with the aim of insulting him.
- **Hacking:** This is by using of malware programs to steal personal information and passwords.
- **Digital ostracism:** by excluding a person from a group or electronic game; this is with the aim of annoying him.

Effects resulting from cyberbullying

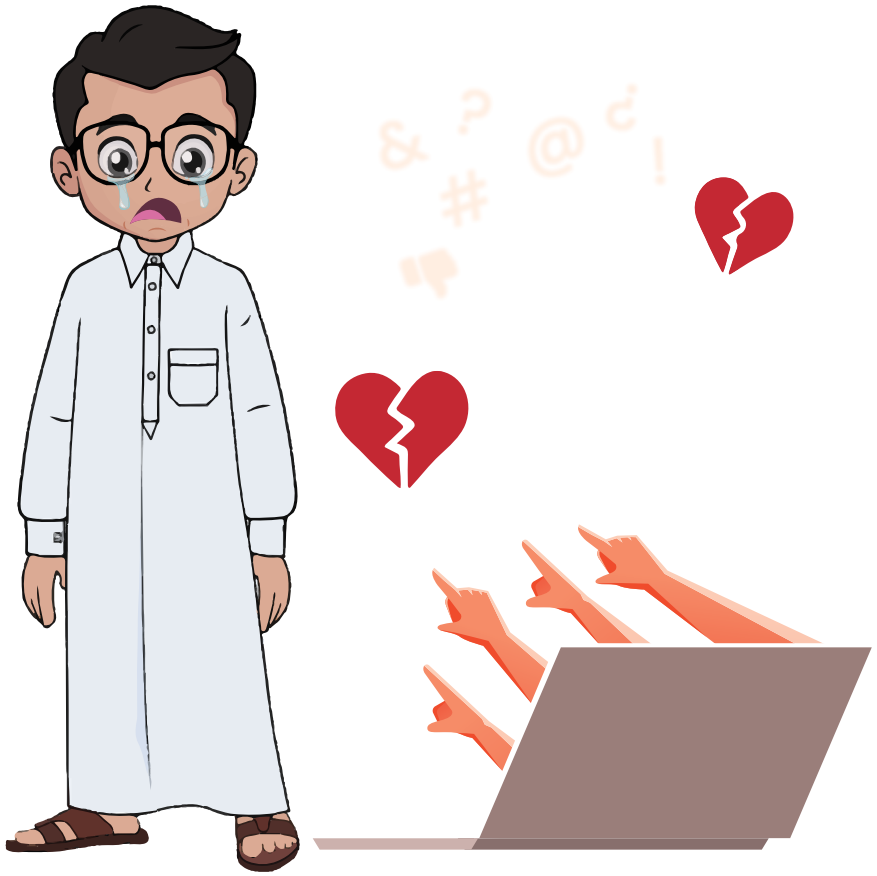
When cyberbullying occurs, the victim feels that he is vulnerable to bullying at any time and in any place. He was exposed to bullying while inside his home, which affects him on several levels:

- **Mentally:** He begins to feel upset, embarrassed, and even angry.
- **Emotionally:** He feels ashamed and loses interest in the things he loves.
- **Physically:** Because psychological problems affect him, especially sleeping and eating, and thus he may suffer from insomnia, stomach pain, bulimia, or loss of appetite, and of course headaches.



Risks of cyberbullying

- Feeling lonely, isolated, and wanting to spend long periods away from others or social events.
- Feeling exhausted, anxious and distressed, feeling extremely embarrassed and ashamed, especially in the case of distorting reputations and spreading rumors.
- Lack of confidence in oneself and in others, and a feeling of inadequacy and lack of value and importance.
- Many health problems that clearly appear in the appearance of the victims; because it is related to food and sleep.
- Feeling very angry and depressed.
- Delay in academic achievement and loss of work.
- Feeling afraid and insecure.



Chapter Two: How to face the risks of cyberbullying

How do I protect myself from cyberbullying?

- Teaching and training children to deal with bullies, and encouraging them to disclose what happens to them to parents or teachers; to take the necessary measures.
- Learn internet etiquette before using it.
- Learn about the laws, rules and policies of websites, especially social media platforms, especially with regard to cyberbullying and pursuing bullies.
- Reserving photos and personal information, especially those circulated on social media platforms.
- Insist on taking legal action against bullies and not give in, show weakness, or be afraid of them.
- Ignore offensive comments and messages and do not respond to them.
- Block bullies immediately and avoid confronting or threatening them.
- Use passwords that are difficult to guess or hacking.
- Maintain the confidentiality of login data and avoid using public Internet networks or logging in to anyone.
- Make sure you're signed out if you're using a device other than your own, or if you're sharing your device with other people.
- Do not trust strangers and do not give others any private information about you, even if you feel that they are trustworthy and safe.

Middle school

In this stage, digital training will be provided through three axes: forgery and online fraud, phishing, and copyrights. **The following is an explanation of the most important information that will be presented on these axes.**

The third training kit

Forgery and Online Fraud

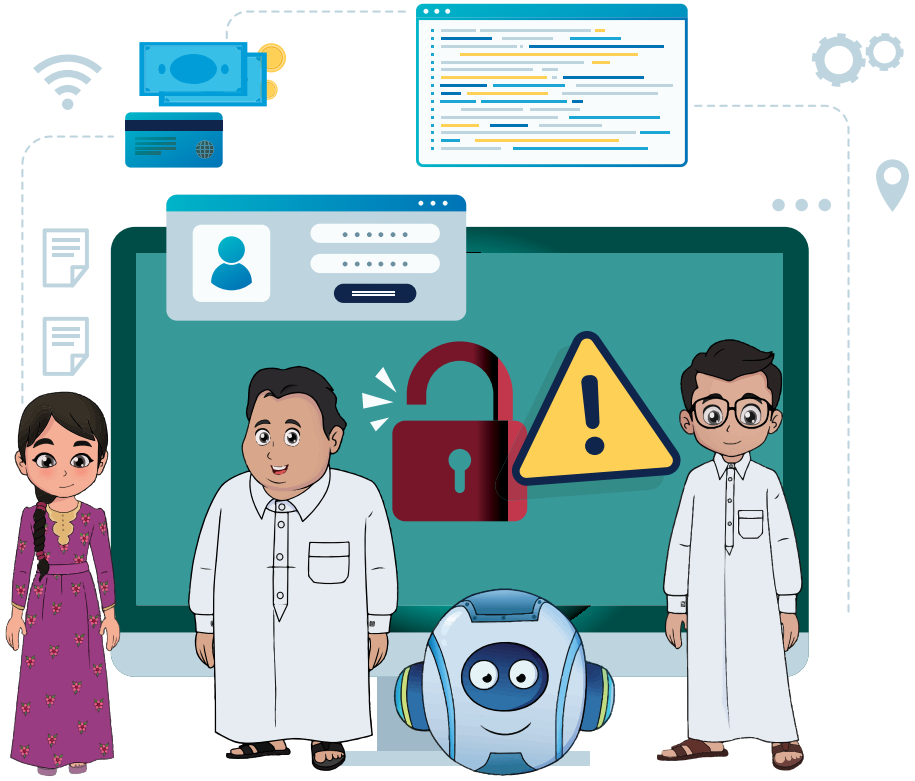
- **Chapter One:** The concept of Forgery and Online Fraud and its types
- **Chapter Two:** How online fraud are executed
- **Chapter Three:** How to act if exposed to online fraud

Chapter One: The concept of Forgery and Online Fraud and its types

The Internet revolution and the great technological boom have facilitated many things, including financial and commercial transactions through technological media. Naturally, with this, the means of online fraud have evolved to become a real threat to most Internet users. This is what makes us learn about new ways, methods, and means of fraud that are used on victims every day.

Online fraud:

Online fraud is a form of fraud whose aim is to seize money or property illegally. It is carried out using the Internet and the programs that operate through it and often leads to large losses, which may reach millions of dollars annually, in addition to moral losses, of course.



Types and forms of online fraud

Online fraud can be executed using the following tools:

- **E-mail:** this is when you receive an attractive email message stating that you have won a competition, have a gift phone, or have a free vacation. All you have to do is click on the link. As soon as you enter, you will be asked for some personal and financial information, or you will be asked to transfer a small amount to obtain the prize, of course. Once you do this, your information and financial data will be with the fraudster.
- **Applications that are hacked or that you download from unknown sources** or links for login that, once you click on them, your data and files are hacked, and your passwords or bank card numbers that you own can easily be stolen, and you may become a victim of blackmail in exchange for paying money.
- **Computers,** especially in companies and institutions, are a target for hackers, and fraudsters always resort to hacking with malware programs and links in order to stop them from working or steal data in exchange for blackmailing you.
- **E-commerce sites,** which have become widespread, are just a front for fraud, as they ask you to make a purchase, and after paying, the product does not reach you, or you receive a fake product, and perhaps also on the payment page, your financial and banking data are stolen.
- **Fraud in the name of charity,** in which the fraudster claims to organize donation campaigns for victims or to provide assistance to someone, and of course either the money is sent directly or your bank data is stolen.

Chapter Two: How online fraud is executed

Loopholes that help with online fraud

- Neglecting to update registration systems, programs and applications, especially those that perform protection operations.
- Neglecting to use specialized antivirus programs and making sure to constantly update them.
- Using passwords that are easy and predictable.
- Opening attachments that come with email, especially those that are unknown or appear strange.
- Advertising links or links that come to you from unknown contacts or via email.
- Sharing personal information with others, whether through social media platforms or individuals impersonating an official entity to obtain information from you, poses a risk.
- URLs with strange or untrusted extensions.
- Recording banking data on electronic websites - e-commerce sites- especially obscure ones.

Personal Data Security and Online Fraud

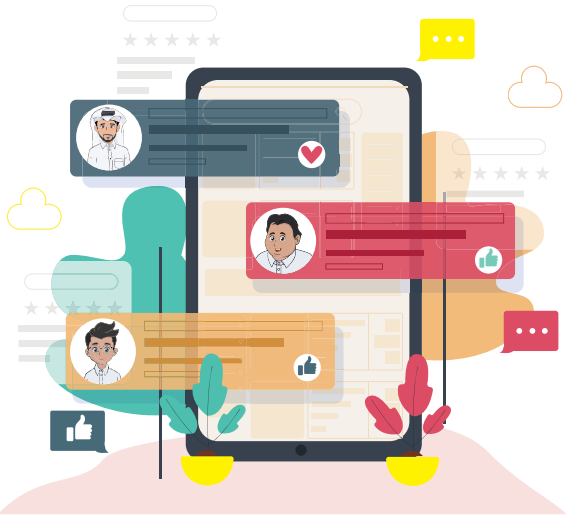
Data security refers to all the measures that are used to secure data and prevent any unauthorized access because the confidentiality and integrity of databases must be maintained and protected from any suspicious practices that may lead to destroying the reputation of people or institutions and harming them financially and morally.

To protect yourself from data theft, you must:

- Avoid sharing any personal information, whether in emails or on social media platforms.
- Strong passwords.
- Protect your bank accounts and cards by monitoring your balances, verifying every transaction on your account, and promptly reporting any discrepancies in withdrawal activities.
- Enhance the security of the devices you use by ensuring continuous automatic updates of systems and applications. Additionally, install anti-virus and anti-spyware programs, activate firewalls, and use passwords for important files.

Digital footprints and Online Fraud

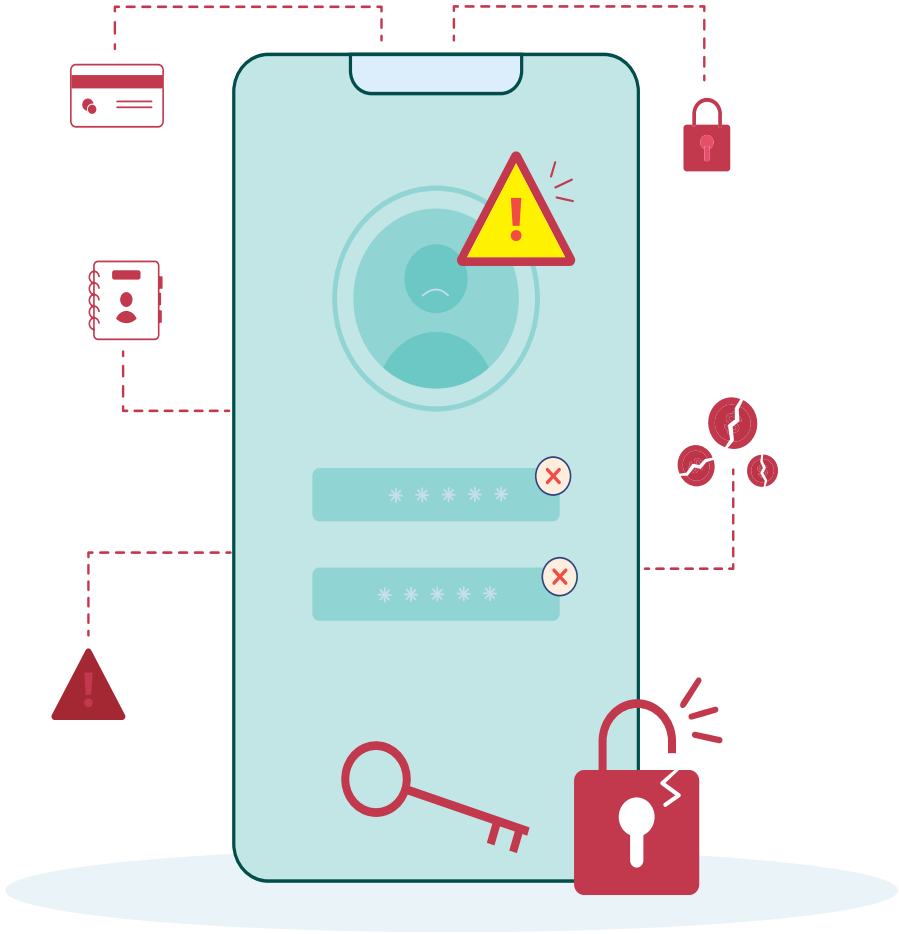
A digital footprint is the digital shadow or trace of all the data you leave behind when you use the Internet. It includes the websites you visit, the email messages you send, and the information you post about yourself on social media platforms. You leave a trace with every use, and regardless of how simple your actions may be, they are considered part of your digital footprint. Unfortunately, there is a significant relationship between the digital footprint and fraud attempts. This is because everything related to you can become available to the public on social media platforms, allowing others to influence and control your digital reputation, which is no less important than your reputation in reality.



Chapter Three: How to act if exposed to online fraud

Guidelines for protection against online fraud

- Use the official legal copies of applications.
- Download your applications from well-known official stores, not from anonymous websites.
- Ensure that you regularly update the operating system on your phone or computer.
- Do not click on any links from unknown sources, regardless of the sender.
- Do not engage in third-party transactions, especially involving funds; as you may unknowingly become involved in fraud or a money-laundering attempt.
- Use antivirus programs and applications.
- Use strong and complex passwords.
- Do not shop from new or unknown stores without first verifying their reputation and credibility, both in the products they sell and in terms of payment.



What should I do if I am exposed to online fraud?

You should promptly inform your parents or one of your teachers if you are exposed to online fraud. Subsequently, contact the cybercrime police to address the issue, resolve the problem swiftly, and safeguard your data from theft. Reporting promptly aids legal authorities in apprehending the fraudsters and protects potential victims.

You should also contact your bank as soon as possible and request a complete suspension of your account. Given that you've been exposed to fraud, it's crucial to halt all banking operations that fraudsters may attempt. The importance of sharing your experience in detail on social media platforms is crucial. This helps educate others about the mistakes you've encountered. There are specialized groups dedicated to exposing perpetrators in such cases, providing an opportunity to engage in dialogue with participants for advice and solutions, which can be highly valuable.

Fourth kit

Phishing attack

- **Chapter One:** The concept of phishing and its types
- **Chapter Two:** How to Carry Out Phishing Attacks
- **Chapter Three:** How to Act if Exposed to Phishing

Chapter One: The concept of phishing and its types

The concept of phishing

Phishing is a dangerous and effective method of hacking devices, wherein individuals or institutions are targeted through malicious links or attachments sent to users. These are often mistakenly downloaded or clicked, leading to the theft of their data and personal information.

According to studies, 32% of hacking operations worldwide are phishing attacks, and approximately 64% of institutions and organizations have been exposed to phishing at least once in their history.

Types and Forms of Phishing

- **Social Engineering:** It is an attack based on deceiving victims into taking quick action using false and deceptive information, often impersonating official institutions and trusted entities. The goal is to deceive the user and prompt them to act swiftly, without careful consideration.
- **Simulating links:** This method involves creating fake copies of official sites. These counterfeit sites closely resemble the originals and may appear entirely legitimate at first glance. Once you enter the site and provide your information, it requests, the thief gains access to your data. Consequently, they can exploit it for various purposes, even for malicious personal intent.
- **Phishing through email,** Which is the most common method, involves sending an email with attachments or links to a user. Once clicked, the device can be controlled and hacked.
- **Ransomware:** These programs are very common and utilize hidden software, often disguised as a trusted attachment. Once clicked, they are downloaded to the device. They may disable systems and steal data, demanding a ransom instead of outright destruction.
- **Spear phishing (Whaling):** In this method, specific individuals are targeted through information collected by searching for them and monitoring their digital footprints.
- **Whaling, Especially politicians, economists,** or celebrities, data is often hacked and stolen to be exploited for blackmail and financial gain.
- **Phishing via text messages,** Which is done through short messages that come in the form of texts and are usually personalized to persuade the recipient to click on the link or take a specific action, leading to the hacking of the device.
- **Vishing, I**t is a form of phishing that relies on artificial intelligence, where the voices of specific people are generated to send messages to victims, persuading them to transfer money or disclose certain information.

Chapter Two: How to Carry Out Phishing Attacks

Vulnerabilities Exploited by Phishing Attackers

There are several methods used to carry out phishing attacks, including:

- **Phishing based on need,** exploits the victim's desires or creates a false sense of urgency to persuade them to take immediate action without much thought. For example, sending a link promising a gift or a paid vacation. In such cases, recipients may click without realizing that they are unwittingly providing their data to the phishers.
- **Overconfidence often arises** when phishers impersonate credible identities, not necessarily limited to individuals but extending to entities such as Google or the Facebook application. Through this impersonation, the phisher can easily acquire information.
- **Emotional manipulation involves** using psychological pressure methods to persuade victims to act immediately without thoughtful consideration. This often includes impersonating an institution or a source familiar to the user, with a focus on evoking feelings of fear and anxiety. People, in such situations, tend to make quick decisions to protect themselves.

Mistakes made by internet users

- Acting quickly and without thinking.
- Not being sure of the validity of the matter, whether it's a link sent to them, a website that requires login, or even a voice call requesting specific data.
- Clicking on attachments or links from unknown or unreliable sources.
- Sharing personal and confidential information on social media accounts.
- Ignoring the securing of accounts with strong and complex passwords.

Digital footprint and Phishing

The peril of the digital footprint lies in its permanence and the accessibility of data, particularly on social media, where everything you share about yourself and those around you becomes readily available. Employers can easily verify your Digital footprint, and it can be exploited to harm, blackmail, threaten, and tarnish your reputation. In the worst circumstances, it may even be used for impersonation or creating a fake identity with the same name and data.

Chapter Three: How to Act if Exposed to Phishing

Phishing Protection Guidelines

- Never trust emails that ask for your information, request you to click on a link, or download attachments. Simply delete them immediately.
- Ensure the installation of antivirus and anti-malware software, and keep them regularly updated.
- Create strong passwords, change them periodically, and avoid using the same password for different accounts.
- Avoid sharing personal information on social media platforms, as doing so may make you susceptible to phishing scams.

Protecting data from hacking

In order to protect your data from hacking, you must do the following:

- Install protective programs and ensure prompt updates, including operating systems.
- Secure devices connected to the Internet and use strong, complex passwords.
- Ensure that the firewall is activated on your devices.
- Implement hard disk encryption to transform your data into unreadable codes.
- Avoid accessing public internet networks.
- Do not neglect to erase your data from old devices.
- Use strong and complex passwords for your various electronic accounts.
- Enable two-factor authentication.
- You can use the guest network at your home to protect yourself from hackers.

What should I do if I encounter a phishing attempt?

In the event that you are exposed to phishing, you must immediately reach out to your parents or a teacher at school to help facilitate direct communication with the cybercrime police for specialized assistance. Provide all the information you know so that they can intervene to stop and apprehend the hacker.

The fifth kit

Copyrights

- **Chapter One:** The Concept of Electronic Copyrights and Publishing
- **Chapter Two:** Forms of Electronic Copyright Infringement


القوانين الصفية
الرسالة
Mission
"Regulate and support high quality learning opportunities across all educational levels to provide individuals in Qatar's society with the knowledge, skills, and attitudes according to their abilities and in line with the national values and needs".
الرؤية
Vision
"Leading innovative, high-quality, life-long learning opportunities serving Qatar's society".
8:32
رؤية السوارة
الريادة في توفير فرص تعلم دائمة ومبتكرة وذات جودة عالية للمجتمع القطري
رسالة السوارة
الهوية والانتماء
CyberEco
الإسم
PII
مدرسة سعيد بن زيد الإعدادية للمبين
Saeed Bin Zeid Preparatory School For Boys
LIBRARY

Chapter One: The Concept of Electronic Copyrights and Publishing

Copyrights are the rights that individuals or institutions possess when they create any type of content, provided that the content is original, not copied or stolen, and is stored in a physical medium. The owner of the copyright has the exclusive right to use the work or content and can sell or grant others permission to use the work or content.

Types of Electronic Copyrights and the International Institutions that Sponsor Them

- Audiovisual works such as television programs, movies, and videos.
- Sound recordings and musical compositions.
- Written works such as lectures, articles, and books.
- Visual works such as paintings, posters, and advertisements.
- Video games and computer software.
- Drama and theatrical works.

The World Intellectual Property Organization (WIPO) is the primary global body specializing in serving the public, including individuals and companies, to protect intellectual property rights and copyrights. It serves as the global forum for intellectual property policy. Many countries have established similar institutions locally with the goal of protecting the intellectual property, content, and artistic production of individuals and companies.

Chapter Two: Forms of Electronic Copyright Infringement

- Imitating and selling original works while presenting them to the public as imitations.
- Imitation, selling, or trading with other producers, even if they are outside the country.
- Publishing contents and works on the internet without written permission from the author or the rights' holder.
- Using the content or parts of it without obtaining the permission of the content owner, even if the name of the rights holder is mentioned.
- Removing, distorting, or disabling original content to publish fake content.
- Removing the name of the producer, rights holder, or author from the artwork.

How to Address Electronic Copyright Infringements

- **Photocopying,** scanning digital forms, copying, or pasting any parts of the original work without obtaining permission from the author or producer.
- **Email,** which is the least used type, occurs when someone has the exclusive rights to use a product or content, so he sells or distributes it through email and forwards it to other people.
- **Networks,** when copyright infringement occurs on a public or private network, so that everyone can see the content without the consent of the author or the original rights' holder.
- **File sharing by uploading** or downloading files to websites and allowing others to re-download and copy them.
- **Hacking** and fraud involve creating counterfeit versions of original content and selling them to others, even when they are aware that the content is not authentic.

Strategies for safeguarding against electronic copyright infringement

- **First:** Acquiring a license, whether the content is an image, passage, audio, or of any nature.
- **Second:** Include a security badge that offers cost-free protection for the content. It can be placed on websites and may safeguard the content from copying and hacking attempts.
- **Third:** Verify plagiarism through websites designed to detect content copying.
- **Fourth:** As for users, it is essential to refrain from participating in such theft, as it causes harm to producers and artists both financially and morally and contributes to making the cyberspace environment unsafe.

High school

In this stage, digital training will be provided in three axes: the IMAP4 protocol, web bots, and content security policy (CSP). **The following outlines the key information that will be covered in these axes.**

Sixth training kit

What is the IMAP4 protocol?

- **Chapter One:** The concept of the IMAP4 protocol
- **Chapter Two:** How the IMAP4 protocol operates?


ACT
SAT
Pre-Algebra
OBJECTIVE PHYSICS
MODERN PHYSICS

The IMAP4 (or POP) protocol is one of the fundamental methods for accessing email. The IMAP4 protocol is particularly recommended, especially if you use multiple devices, such as a smartphone, laptop, or tablet, to check your email messages. .

Chapter One: The concept of the IMAP4 protocol:

The IMAP4 protocol is responsible for accessing your email messages from anywhere and on any device. Simply log in, and you'll find your messages without the need to download, upload, or store them on the device you're using. This allows you to read emails at any time and from any internet-connected device.

This protocol distinguishes itself by not automatically downloading attachments. Instead, you have to click on them to download or open the offering the user greater speed and the ability to receive a larger volume of emails without the need for storage space on the device being used.

The significance of the IMAP4 protocol

The significance of this protocol lies in its capability to open emails from any location and on any device, be it your own or that of a friend or colleague. It also enhances speed in terms of response, access, and opening, as attachments are not downloaded automatically but upon your click. Furthermore, it does not necessitate storage space on the device since it is entirely accessible on the internet. This allows emails to retain messages as long as you do not delete them manually, as it does not consume space like other protocols.

Additionally, this protocol enables users to access their email on multiple devices simultaneously. This means you can download the email application or open it from the browser on your mobile phone and, simultaneously, on your computer.

The distinction between IMAP4 and other email protocols

The IMAP4 protocol is not the sole method for managing email. Another protocol is the POP3 protocol. Originating as an older protocol, it was initially designed for opening mail on a single device. As a result, it lacks two-way synchronization, a feature found in modern protocols. The POP3 protocol operates with one-way mail synchronization, enabling users to download emails from the server to the client. Consequently, it lacks many of the basic functions found in contemporary services.

POP3 cannot retrieve messages from more than one device, limiting users to reading messages from a single device and saving messages from only one device. Furthermore, it restricts the saving of messages to just one device through which it operates. An advantage and disadvantage of this protocol simultaneously are that it downloads your messages, enabling you to read them even when your device is offline. However, it comes with the drawback of consuming significant storage space, especially concerning attachments.

Chapter Two: How the IMAP4 protocol operates

When an email message is sent, the Simple Mail Transfer Protocol (SMTP) determines how email messages are sent, and then:

1. A Transmission Control Protocol (TCP) connection is set up between the client and the email server. This protocol is responsible for recognizing and predicting an email message.
2. The client then sends a series of commands to the server, including the mail itself.
3. The email server uses its own software called a Mail Transfer Agent (MTA) to check the record of the Domain Name System (DNS) for email and then find the received IP address.
4. The MTA translates the DNS record into the IP address to know where emails are sent.
5. Finally, SMTP searches for the MX (mail exchange) record associated with the recipient's domain name. If there is an MX record, the email will be sent to the corresponding email server.

IMAP4 protocol and email organization and protection

One of the most important features of the IMAP4 protocol is that it stores mail by default on the virtual server. Therefore, if any problem occurs, for example, server hacking, there is no problem, and there is no need to worry. Because quite simply, this protocol is stored on the virtual server, and therefore email messages will not disappear, unlike POP3, on which messages disappear if the device on which they were downloaded is damaged or lost for any reason.

This protocol also provides an extra layer of security by logging in with passwords and usernames, and the two-factor authentication feature can be activated easily. The protocol relies on encrypting passwords using mathematical equations that make passwords complex, and attackers cannot understand them once they read them.

Seventh Training Kit

Web bots

- **Chapter One:** The concept of web bots and their types
- **Chapter Two:** The Mechanism and Benefit of Web bots

Global network bots, Internet bots, or web bots are all names that express those programs that perform automatic tasks on the Internet. These tasks vary between simple and complex, but are repetitive. Therefore, these robots are important because they work at a higher rate than a human works alone. The biggest task for bots is indexing Internet pages by fetching and analyzing information from servers automatically and at high speed. The data on the pages is reviewed and indexed if it conforms to the rules that govern the bot's behavior on the server.

Chapter One: The concept of web bots and their types

Web bots are programs that work very quickly and perform simple and complex tasks at high speed. The biggest task they perform is indexing web pages. Usually, bots mimic the behavior of humans, but they are much faster than humans because they are automated, and therefore, it can perform many useful tasks. They are also used in customer service.

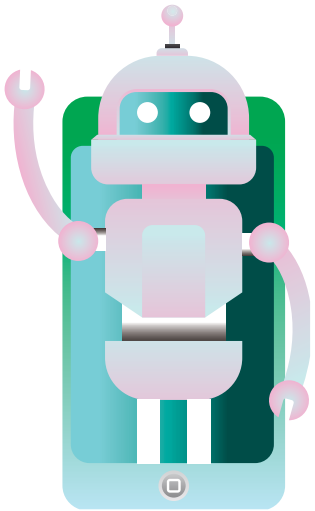
Global network bots are digital tools that can be used for good or bad things, including harmful bots. They are essentially software and therefore can be exploited and hacked.

The concept of web bots

Bots are programs that perform a number of tasks automatically, repetitively, and predetermined. Of course, they are distinguished from humans by their speed and the ability to exploit them in many tasks, most notably indexing search engines and web pages, as well as customer service.

bots help companies in many ways, including:

- Extending working hours and cost savings.
- Improving resources and increasing access to larger segments of the public.
- Doing boring and repetitive tasks.
- Data collection and analysis.



Types of web bots

There are several types of bots, and they are divided between good and malicious. Here are the types of beneficial and harmful web bots:

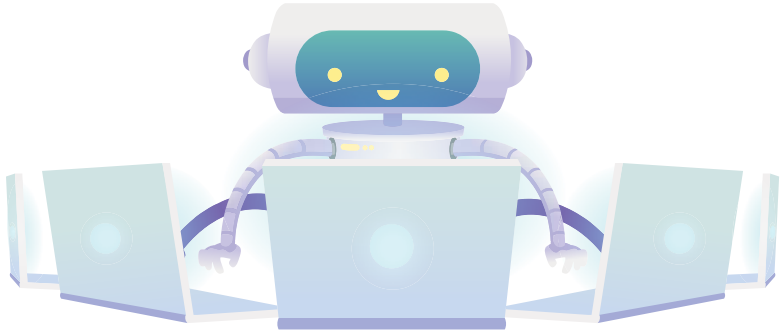
Beneficial types

- **Chatbots:** These are bots that simulate human conversations, rely on artificial intelligence, and are used by most companies to respond to customer inquiries.
- **Web trackers,** This type is called spiders, which are search engine bots that scan and index web pages. They help search engines provide a better search experience by extracting data and understanding the structure of the content and how relevant it is.
- **Web data scraping tools:** They are called trackers, and they are tools that help scan and download specific content on the Internet. Companies use them, especially in e-commerce, to monitor the prices of direct products on retail platforms.
- **Shopping bots,** These are bots that specialize in monitoring product prices on a number of websites to help customers find the best deals.
- **Surveillance bots,** They specialize in reducing exposure to security incidents by scanning systems to find errors or malware and then alerting you to unusual activities by collecting and analyzing user interaction and web traffic data.
- **Transaction bots,** This type confirms the validity of things, such as the validity of recording payment details before transaction termination, especially on e-commerce websites, and verifying the accuracy of bank and credit card details and personal information in payment processes. This type of bot is considered very secure to protect financial and sensitive data.

As for Harmful Web bots, they include:

- **Download bots:** These are bots programmed to automatically download programs and applications, giving false classification to the applications they use to gain more visibility and attract subscribers illegally.
- **Spam bots,** These are bots that extract addresses from the Internet and then create large lists of addresses to send messages to large numbers of users. This type can also create an email account to publish on forums and social media platforms. These bots are often used to encourage people to click on links to hacked websites or download malicious files.
- **Ticket bots,** This type is found exclusively on sites that sell tickets. They buy tickets at low prices and then resell them at higher prices. In some countries, these bots are considered unethical .
- **Distributed Denial-of-Service (DDoS) Bots,** These are malware bots used to conduct a distributed denial-of-service attack. A distributed denial-of-service attack is an attempt aimed at harming a targeted system, such as a website or a specific application.
- **Fraud bots:** These are bots that are sometimes called click fraud bots, which use artificial intelligence to mimic human behavior to carry out advertising fraud. It is used to click on ads on websites to generate advertising revenue for the publisher.
- **File-sharing bots:** These bots operate by logging repeated search terms on applications, messaging programs, or search engines. They subsequently offer suggestions containing illegal or undesirable links to malicious files or websites.
- **Social media bots:** These are bots that create fake activity on social media platforms, such as fake accounts, follows, likes, or comments. These robots mimic the behavior and activity of humans on social media platforms, but they most likely send unwanted content, publish wrong information, or support and enhance the popularity of something or someone.

- **Botnets:** This type is a group of hidden bots that work together in a coordinated manner on tasks that require large amounts of computing power and memory. They are often used to reduce costs because botnets are installed on devices connected to the network that belong to others. Then that network can be controlled remotely and planned to benefit from its computing power without paying for it.



Chapter Two: The Mechanism and Benefit of Web bots

How do web bots operate?

Bots can communicate with each other using the Internet, and they can also use instant messaging or tweet through the IRC Internet chat protocol. Bots consist of sets of algorithms that help them carry out the tasks they will perform. The types of bots are designed according to the tasks they will perform and the different methods they will use to perform tasks, for example, chatbots.

- These bots interact according to rules set by people through pre-defined commands that a person can choose between.
- Chatbots can reach a level of intellectual independence, especially since they have the advantage of learning from human input as well as searching for keywords.
- Artificial intelligence is used in chatbots, so they are built on intellectually independent commands. Artificial intelligence also enables them to process language to make it more similar to the natural language of humans.

What are the benefits of web bots?

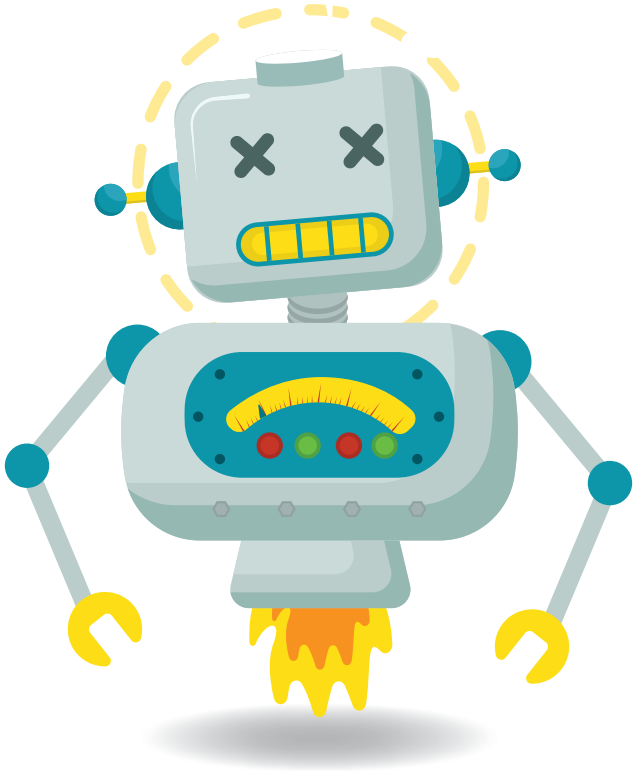
- High speed; they are faster than humans, especially at repetitive and routine tasks.
- It saves time and money and offers many options for companies and customers.
- Available throughout the day.
- It can help large companies communicate with larger audiences without a problem.
- Can be customized.
- It is used for various purposes.
- It can enhance the user experience.

How do you protect your device from harmful bots?

- Installing programs specialized in combating malware is important because it blocks viruses, hackers, and any malware that could infect your devices.
- Continuously updating the programs and systems you use.
- Use strong passwords that are difficult to guess.
- Avoid clicking on unknown links, whether you find them by chance, receive them in a message, or even via email.
- Avoid websites, especially those that use pop-up ads or ones that appear to block most content and claim they can detect viruses or protect your devices.
- Activate the firewall that helps block malicious attacks.
- Using a bot manager can help protect against malicious bots.

When your device is infected with bots, you must do the following:

1. Disconnect your device from the Internet immediately to stop the theft of data and information and prevent bots from entering the network.
2. Transfer all significant data to another device or external hard drive after ensuring that it is free of malware.
3. Reset the device to factory mode. This step will get rid of the bots, but unfortunately, everything else on the device will be lost with it, but you still can retrieve it from the back up in the previous step.
4. Finally, clean the computer and use the necessary security tools.



Eighth Training kit

Content Security Policy

- **Chapter One:** The Concept of Content Security Policy and its working mechanism
- **Chapter Two:** Activating Content Security Policy and Digital Risk Reduction Strategies

Chapter One: The Concept of Content Security Policy and its working mechanism

The Concept of Content Security Policy

A content security policy (CSP) is the key element responsible for providing a computer security standard by preventing cross-site malware (XSS), hacking attacks, or other code entry attacks resulting from the execution of malicious content in the trusted web page context. It is also a way to reduce the risk of various types of attacks and remove them completely by identifying reliable sources of web page content. .

How a Content Security Policy Works

The Source standard allows web administrators to send an HTTP file or response address specifying the sources from which the browser is allowed to download its content. Of course, content is not downloaded from any sources not explicitly mentioned in the Source and is not run on the browser. This includes all types of content, whether text, patterns, images, media, frames, or lines.

A content security policy is important because it acts as an extra layer of protection that can mitigate the impact of other security loopholes in web applications. However, it does not replace good coding practices or other security measures; it is just an additional layer of defense.

Chapter Two: Activating Content Security Policy (Source) and Digital Risk Reduction Strategies

Enabling Content Security Policy (Source)

To activate the Content Security Policy, navigate to the site's settings. Proceed to the privacy section, select security, and adjust the permission settings for the Content Security Policy. Additionally, enable the feature to send security reports generated by this valuable capability.

Limiting Digital Risks through Content Security Policy (CSP)

- **Default Source**
  it is the primary factor for other fetch directives when they are not explicitly identified.
- **Child-Source**
  Lists reliable sources of web users and documents the overlapping browsing contexts that occurred.
- **Script-Source**
  Identifying trustworthy sources of JavaScript.
- **Object-Source**
  Specifies trustworthy sources for <object>, <embed>, and <applet> elements.
- **Style-Source**
  Identifying trustworthy sources for style sheets (CSS).
- **Img-Source**
  Identify trustworthy sources for your favorite images and shapes.
- **Frame-Source**
  Specifies trustworthy sources for overlapping browsing contexts loaded using elements such as <frame> and <iframe>.
- **Connect-Source**
  Restricts the loading of URLs through script interfaces.
- **Upgrade-Insecure-Requests**
  Instructs the web browser to treat all unsafe URLs on the site, released through HTTP, as if they were replaced by secure URLs.
- **Require-sri-for**
  Requires the use of Sub resource Integrity (SRI) for external text or styles on the page.

Students' Parents Training Kit

Securing electronic devices and countering security breaches

- **Chapter One:** The significance of the security of electronic devices and networks
- **Chapter Two:** Types of digital threats in devices
- **Chapter Three:** How to Secure Devices from Digital Threats

Chapter One: The significance of the security of electronic devices and networks

Maintaining the security and confidentiality of information is crucial for individuals and companies. Breaches can lead to significant problems, particularly for businesses dealing with confidential customer data. Risks include data leakage, potential reputation loss, and customer attrition.

The Significance of digital stability for networks and connected devices

Digital stability is one of the most important things that companies and even individuals must be keen to protect because threatening this stability means a great deal of risk related to:

- **Information:** Especially since digital security means protecting your data and personal information for accessing the work system, or that you use to accomplish important tasks, or the data for the final files for those tasks.
- **Work Stability:** Because after being exposed to any cyber attack, institutions and companies need a large amount of time to recover and return to stability - before being attacked - and thus maintaining digital security and stabilization ensures the continuity and stability of work.
- **Avoid Legal Problems:** Because leaking data about individuals or companies will expose you to legal accountability and you may be punished for this reason.

Digital Risks Facing Digital Devices (phones, computers and tablets)

- Exploiting Security vulnerabilities: Targeting system vulnerabilities - such as outdated, old, or unsupported operating systems - which become the most vulnerable to attacks because they contain gaps that can be easily exploited.
- Hacking Weak or Easy-to-Guess Passwords.
- Malware attacks
- Social Engineering: Which helps hackers catch victims out and hack their devices easily, just by monitoring and analyzing the behavior of the potential victim and working to trap him.

Chapter Two: Types of digital threats in devices

Ransomware attack

This attack depends on sending file attachments or clicking on a link to automatically download a program on the device. Then this program disappears easily, and at a specific time that was set in advance, the device crashes completely, and you receive a message asking you to pay a ransom for recovering the data and controlling the device.

Device data theft

Data theft occurs in a number of ways, including malware, worms, viruses, and Trojan programs, all of which target devices to obtain data and information recorded on them, control them, or perhaps disable, damage, or destroy them.

Illegal Access

Hackers use more than one form to access data and information that they are not allowed to access, and online fraud and phishing are the most prominent and common forms that they use to access data and control devices and networks.

Malware

It is one of the most prominent forms of malware that is used to hack devices and networks

- Viruses.
- Worms
- Trojan horses
- Spyware

Chapter Three: How to Secure Devices from Digital Threats

How do you protect yourself from security breaches?

- Use strong passwords and enable two-factor or multi-factor authentication whenever possible.
- Use a different password for each of your accounts.
- Close accounts that you have stopped using.
- Make sure to change passwords regularly (The suggested duration is from two to three months).
- Before disposing of electronic devices, erase all data and accounts on them.
- Make a backup copy of your important files.
- Secure your phone with a screen lock.
- Use security programs and firewalls.
- Exercise caution before clicking on any link.
- Check the form of links you enter and the use of the HTTP protocol.
- Regularly review your bank accounts and credit reports to ensure there are no suspicious transactions.
- Understand the value of your data and avoid disclosing it to anyone or through social media platforms.

The fifth axis

Interactive training games.

As part of the field visits project to schools, several training games will be provided for students, serving multiple objectives. These include providing information relevant to the concepts of cybersecurity and digital safety to students within a framework of entertainment, and competition. These games are designed to serve as supplements and supports for the scientific material that will be presented to students as part of the training packages.

In general, training games are considered an effective tool in teaching children and adults the fundamentals of digital security and principles of digital safety.

These games derive their effectiveness from their ability to capture the attention and focus of students, relying on the elements of excitement and entertainment. Students acquire information within an entertaining framework, preventing feelings of boredom or monotony.

The total count of training games is five, covering various educational stages. Some are tailored for primary level students, while others target Middle and High school students. Overall, these are interactive games, meaning that they require the participation of more than one student in the game. The following is a brief overview of these games.

The first game

Cyber Block

Recommended age for the Game

+10 years

Game Idea:

The main idea behind «Cyber Block» is to present fundamental concepts and knowledge of cybersecurity and related topics in a simplified and fun way that helps players learn in an innovative and non-traditional manner.

At its core, the game aims to provide students with information on concepts related to cybersecurity and digital safety, such as network security, information security, applications security, and other relevant subjects. These concepts are divided into positive concepts like confidentiality and safety, and negative concepts like cybercrime and data theft, among others. All these concepts, both positive and negative, are printed on the game board. Positive concepts are referred to as safe zones, while negative ones are termed dangerous zones' each student has their own tokens to navigate the board, and when their tokens lands on a safe zone, they are awarded a prize card containing points. However, if their tokens lands on dangerous zone on the board, they receive a penalty card that may either restrict them from playing further or result in the loss of some points.

The winning team is the one who accumulates the highest possible number of points.

The second game

Cyber Quiz

Recommended age for the Game

+7 years

Game Idea

The game takes young students on an exciting competitive journey by directing questions related to cybersecurity in simplified and relevant topics. This occurs within a specified time frame, all in an attractive competitive format ensuring entertainment and learning in an innovative and unprecedented way.

At its core, the game comprises 25 cards, with each card dedicated to a concept from the realms of cybersecurity and digital safety, such as data integrity and cybercrime, among other concepts. Each card is associated with four questions, resulting in a total of 100 questions.

The game also includes 25 numbered figurines ranging from 1 to 25. At the beginning of the game, each student selects one figurine, receiving a corresponding playing card with a number matching the chosen figurine. The student is then required to answer one of the four questions associated with the card.

If the student provides a correct answer, they will earn a point in the form of Coins. Each coin is equivalent to one point. The winning student is the one with the highest number of points at the end of the game.

The third game

Cyberno

Recommended age for the Game

+17 years

Game Idea

The fundamental idea behind the «Cyberno» game is to educate high school students about cybersecurity terminologies, concepts, as well as the risks and threats associated with cybersecurity in a more stimulating manner that encourages critical thinking and linking cyber information. This approach contributes to acquiring information through an innovative competitive process. The game is designed to be a collaborative experience, fostering an enthusiastic competitive atmosphere.

The game consists of 116 cards, distributed among prize cards, penalty cards, and cards related to concepts of cybersecurity and digital safety. At the beginning of the game, each student is given 7 cards. Subsequently, each student reads the content of one of their cards to another student, who must then guess the title of the card and its information. If successful in guessing, the student can discard one of their cards. The winning student is the first one to successfully discard all of their cards.

To add some excitement, there are special cards that grant their holders additional advantages, allowing them to evade answering or change the question.

The fourth game

Cyberway

Recommended age for the Game

+15 years

Game Idea

The game idea revolves around conducting knowledge competitions on cybersecurity among students. The game combines challenge, competition, knowledge, and entertainment. It provides information and tests the students' cognitive inventory within a competitive framework based on competition and amusement.

The game involves dividing students into three teams, with at least one student in each team. Each team is assigned a different color, such as red, blue, and purple, and these colors have their own significance in the context of cybersecurity.

The game also includes a game board divided into squares numbered from 1 to 100. The squares are colored according to the team colors, with each team having its own figurine to move across the game board. Students use a dice to determine the number of squares their figurine will move on the game board.

The game consists of a set of cards, each team having its own set. Each team poses a question to one of the other teams, and if the opposing team successfully answers, they move their tokens one square forward.

To enhance the excitement in the game, the game board features symbols, some with negative implications and others with positive ones. When a team's tokens lands on these symbols, it either gains an advantage to move forward or incurs a penalty, forcing it to move backward.

The winning team is the one that reaches the starting square number 100 first.

The fifth game

Educational Ideas Game

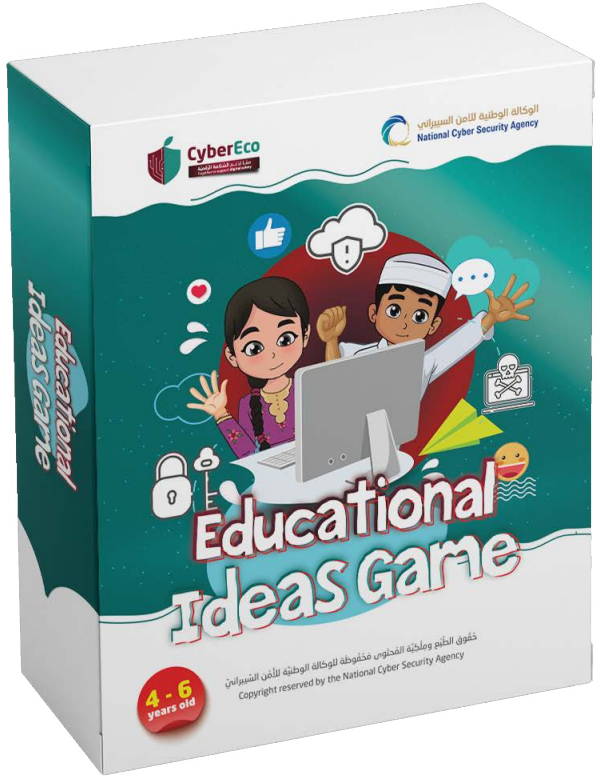
Recommended age for the Game

4-6 years

Game Idea

An educational awareness game for young students, using colors, drawings, and coloring.

The game aims to introduce young students to symbols of general concepts related to cybersecurity and digital safety through simple steps that are easy to understand at this young age in an enjoyable way. The game also aims to have a long-term positive awareness impact in instilling the principles of digital safety through a fun social activity between teachers and students in the classroom and during breaks, or with their parents at home.



The sixth axis

The Expected Role of Parents in the CyberEco Project:

The cooperation of parents with the field visit implementation team is a key input to the success of the project and the achievement of its objectives. Therefore, it is necessary to define the roles expected of parents in the context of the project and to clarify the mechanisms and pillars of this cooperation.

The difference between in-classroom and non-classroom Exercises

The tools used in the context of the field visit project include implementing two types of training activities: in-classroom and non-classroom Exercises. Parents must be fully aware of these concepts.

- **In-classroom exercises:** These are activities that students practice in-classroom with the participation and supervision of the trainer or teacher to achieve the training objectives of the project.
- **Non-classroom Exercises** these are activities that students' practices outside the classroom, aiming to continue awareness-raising work at home under the indirect supervision of parents. And there is no harm in parents participating with them in these activities.

Providing cultural media

The CyberEco project provides various types of cultural media to students and trainees to help them understand and assimilate the training content. Cultural media are developed appropriately for each stage of participating students and the topics they are studying to help them master the content and understand it deeply and closely to reality.

Continuous communication with teachers

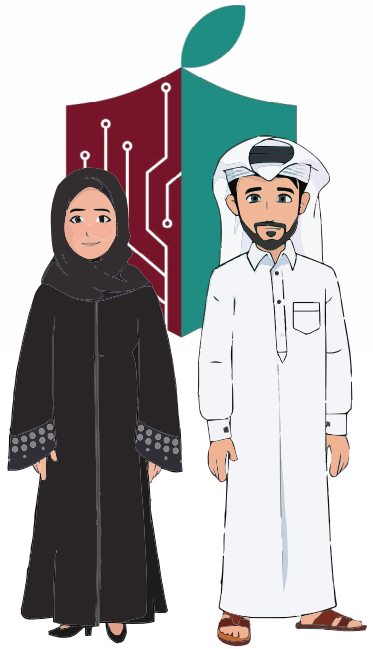
One essential factor that ensures the success of this project is effective communication between teachers and students' parents. This is necessary to establish integration between the roles of the trainer or teacher in the classroom and the parent at home, as both are concerned with the child's interests. Their primary and most important goal is to make the project successful, enhance the digital literacy of students, and increase their ability to safely navigate technology.

Addressing problems

The CyberEco project encompasses all the capabilities necessary to ensure success and the achievement of project objectives. However, the occurrence of problems is always a possibility. Therefore, various means of direct communication have been established with the program administration, those in charge, as well as with teachers and students' parents. This is to facilitate immediate and prompt action in response to any issue that may arise, affecting students and their progress in mastering the project's content.

The Expected Role of Parents

- Parents need to provide sufficient support to their children in understanding and comprehending the workshop content. They should ensure that their children receive information by asking questions about the topic, evaluating their answers, assisting them in research and external exploration, and expanding their cognitive exploration framework.
- Parents should allocate sufficient time for their children to engage in various interactive activities during their free time. Additionally, they should thoroughly read the game guide to ensure maximum enjoyment and benefit for both parties simultaneously.
- Parents should maintain continuous communication with the teacher regarding the workshop content. They should ensure their understanding of the related topics and inquire about any information that may be difficult for them to comprehend. This will help them support their children and ensure their complete understanding of the content.



The integration of the role of teachers with the students' parents

The relationship between the parent and the teacher is one of the basic pillars of any complete and successful training and educational system. Therefore, there must be continuous communication and a satisfactory formula of interaction between the parent and the teacher. Below are the most important pillars that regulate the forms of cooperation between teachers and students' parents within the framework of the CyberEco project:

- **Collaboration Framework in the Field of Extracurricular Exercises:** Students may have inquiries about the extracurricular exercises assigned in the context of the field visits project. Some of these inquiries may not be answerable by the students' parents, so the parents may convey these inquiries to the class teachers, who will provide answers or, in turn, convey them to the executive team on the project.
- **Evaluation:** The process of evaluating students' benefit from the training content will take place in cooperation between teachers and students' parents through exchanging information about the development of the student's behavior in dealing with the Internet and technological tools.

CyberEco

مَعًـا لِدَعْـمِ السَّلامَة الرَّقميَّة

Together to support digital safety

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency