



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



CyberEco

معا لدعم السلامة الرقمية
Together to support digital safety

Trainer's Guide for Training Games

Tailored to the training content





Intellectual Property rights

The National Cyber Security 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 Cyber Security 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

Index

Who are we?	7
Introduction	7
Guide Idea	9
Importance of the Guide	11
Guide Goals	12
The Role of the Trainer towards Students in Training Games	12
General Overview of Training Games	12
Game 1: Cyber Block	12
• Game Goals	13
• Recommended age for the Game	13
• Game Components	14
• Gameplay mechanics	15
The Second Game: Cyber Quiz	17
• Game Idea	18
• Game Goals	19
• Recommended age for the Game	21
• Game Components	24
• Gameplay mechanics	24
• Cyber Card Topics and Questions	24

The Third Game: Cyberno	49
• Game Idea	51
• Game Goals	51
• Recommended age for the Game	52
• Game Components	64
• Gameplay mechanics	65
• Game Rules	67
Fourth game: Cyber Way	69
• Game Idea	69
• Recommended age for the Game	69
• Game Title	70
• Game features	70
• Game Components	71
• Types of squares	72
• Gameplay rules	33

The Fifth Game: Educational Ideas Game	75
• Game Idea	77
• Recommended age for the Game	77
• Game Goals	77
• Game Components	77
• Gameplay mechanics	78
Assessment Criteria for Student Performance in Training Games	80



Who are we?

The National Cyber Security Agency is a national institution dedicated to the development and protection of the cyber space in the State of Qatar, enhancing the efficiency and effectiveness of the digital environment to support the progress of the state and society and contribute to the achievement of Qatar's 2030 vision.





Introduction

Training games are an effective tool in education, especially for children and adolescents, as they combine training with entertainment. This motivates students to engage in the game and acquire knowledge. Training games are one of the most effective interactive training tools, especially when they are played in a group setting. Group games have a high ability to stimulate cognitive and competitive interaction among students, which supports the main objective of the game, namely providing information to students within a framework of competition and entertainment.

In the context of the tools used in the field visits project to government and private schools in Qatar, training games have been adopted as a primary tool. These games will be supervised indirectly by trainers to support their ability to guide students on how to interact with these games and how to evaluate their performance. To achieve this, trainers must be provided with a procedural guide that provides them with the

necessary information about the approved games, as well as detailed information about each game and the proposed evaluation mechanisms.





Guide Idea

The concept of the guide is based on the need to provide trainers with the necessary cognitive support to interact with training games. It provides a detailed explanation of each game so that trainers can explain it to students. The concept also includes providing trainers with a methodology for evaluating students' performance in the games. When students play training games, the trainer must evaluate their performance, especially their cognitive performance, and observe their ability to use the information they have been trained on in the games. Overall, games rely on the student's ability to use the information and knowledge provided to them in the games, and winning in the games depends primarily on the students' cognitive abilities. The more extensive their cognitive knowledge, the higher their chances of winning in the games.

Importance of the Guide

The importance of the guide is derived from the importance of training games and their role in supporting and enhancing students' cognitive knowledge. It also plays a role in evaluating students' performance and assessing their ability to utilize the information and concepts they have been trained on. The following are the main points that illustrate the importance of the guide:

- The need to provide trainers with detailed information about each training game to enable them to guide students on how to play.
- The need to provide trainers with a methodology for evaluating students' performance in the training games.
- The importance of observing and evaluating students' ability to utilize their cognitive knowledge in the games.

Guide Goals

The guide for training games aims to achieve the following objectives:

- Enhancing trainers' ability to interact with training games and guide students on how to play.
- Providing trainers with detailed information about each game, including its objectives and gameplay.
- Equipping trainers with a clear methodology for evaluating students' performance in the training games and assessing their ability to utilize their cognitive knowledge to win in the games.



The Role of the Trainer towards Students in Training Games

To achieve the goals of training games, the trainer must undertake several tasks and responsibilities. **The following highlights the most important ones:**

- Supervising the distribution of students among the training games and indirectly supervising team formation in case the game is played in groups.
- Explaining the game mechanics to students and clarifying the objectives and gameplay.
- Addressing students' inquiries regarding the games and their rules.
- Directly supervising the game and taking notes on students' performance to use in the evaluation process.



General Overview of Training Games

There are five different training games, each with its own overall shape and gameplay. However, they share a common aspect, which is that winning in these games primarily depends on the students' digital cognitive knowledge. The games also vary in terms of the number of players and the age group they are designed for. Generally, the games cover different age groups in the three educational stages: Primary, Middle, and High school. The following table provides details about the age group and number of players for each game:



Game	Cyber Block	Cyber Quiz	Cyberno	Cyber Way	Educational Ideas Game
Age Group	+10 years	+7 years	+17 years	+15 years	4-6 years
Number of Players	Two teams and a referee, each team has 1-2 players	Two teams and a referee, each team has 1-5 players	2-6 players with a referee	Three teams, each team has 1-3 players	Two or more players
Winning Criterion	The team with the highest number of points (Coins) wins	The player with the highest number of points (Coins) wins	The player who finishes all their cards first is the winner	The team that reaches square number 100 first wins	The student who answers the most questions correctly is the winner

The following provides details about each game, how to play it, its goals, and its rules.





Game 1: Cyber Block

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.

Game Goals

- Develop students’ digital skills.
- Introduce students to new cyber-related concepts and terms.
- Simplify and deliver information to students in an entertaining manner.
- Convey cybersecurity information in a fun way that facilitates full comprehension of the material.
- Write terminologies in both Arabic and English to enhance students’ ability to effectively interact with the cyber environment.
- Motivate students and enhance their sense of excitement, enjoyment, and achievement by collecting as many rewards as possible and defeating competitors.

Recommended age for the Game

+10 years



Game Components

1. A large board divided into 24 stations, with two colors:

A. **12 Stations in Green (Safe Cyber Stations) Include positive terms related to cybersecurity, they are:**

1. **Confidentiality:** Controlling access to data and allowing or restricting certain categories of users from accessing it.
2. **Integrity:** Ensuring the integrity of data and information, as well as protecting them from sabotage attacks or theft.
3. **Availability:** Ensuring the Availability of all systems, services, and information, making them available to companies or clients as needed.
4. **Network Security:** Practices aimed at Securing computer networks from intruders through software and various technologies, including firewalls, email security, antivirus software, and malware protection.
5. **Information Security:** The process of designing and implementing tools to protect important information from damage, loss, modification, or disruption, especially during transmission or storage. It includes encryption and vulnerability management.
6. **Application Security:** Focuses on keeping software and hardware free from any threats. This stage is typically performed during the design phase. Long before software or hardware deployment.
7. **Operational Security:** The management of risks for all internal cybersecurity operations, including decisions related to data assets and protection, access permissions and data sharing procedures.

-
8. **Cloud Security:** Involves protecting the core cloud storage systems at all times, given the vast amounts of data they contain, including business services stored in data centers.
 9. **Infrastructure Security:** A security measures that protect vital infrastructure such as communication systems, networks, data centers, servers, or IT facilities from terrorism, sabotage, and corruption attempts.
 10. **Cyber Deterrence:** Refers to all efforts aimed at preventing harmful actions and attacks that may occur in cyberspace.
 11. **Ethical Hacker, White Hat:** An individual or group attempting a legitimate penetration of the enterprise/ company system, aiming to identify vulnerabilities that an attacker (unethical hacker) could exploit for unauthorized access to the system or data.

12. **User Authentication:** It is a technology that prevents unauthorized users from accessing a specific level of information and identifies the users who are allowed access that level.



B. 12 Stations in Red (Dangerous Cyber Stations) Include negative terms that pose a specific cyber threat, which are:

1. **Cyber Attacks:** Any attack that attempts to control, modify, change, sabotage, disable, destroy, or steal information in the electronic space, they often target organizations to destroy or harm them and compromise the safety of the data and information they contain.
2. **Cybercrime:** It is an evolved form of crime that occurs globally and targets computers, networks, or infrastructures.
3. **Phishing Attacks:** A type of attack that aims to steal or damage sensitive data by deceiving individuals into revealing their personal information and taking control of it, often targeting banking data or passwords.
4. **Spear Phishing Attacks:** An fraudulent operation carried out through email or electronic communications, targeting individuals, organizations, or companies. The primary goal is data theft and often relies on installing malware on the victim's device.
5. **Encryption Attacks:** These attacks involve malicious scripts that automatically download and install itself on the victim's device without permission; it is then used to compromise all the data on the device, either by stealing, manipulating, or damaging it.
6. **Ransomware:** It is the most well-known and widely used program because they target confidential and sensitive information. These attacks force victims into deleting all their data. In case they do not pay a ransom within a specified time frame.
7. **Eavesdropping Attacks:** A type of attack that relies on interception and theft of information transmitted through a network via a computer or smart device.

-
8. **Malware Attacks:** Malware is specifically designed to cause harm or damage to a computer, server, client, or network without the user's knowledge.
 9. **Trojan Horses:** A type of malware that is hidden as attachments in emails or bundled with a free downloadable file. Once downloaded, the malicious code begins to work and attacks data, spies on information, and monitors the user's activities.
 10. **CyberBullying:** The use of digital technologies for bullying, often occurring through social media platforms, messaging platforms, and online gaming.
 11. **Online Fraud:** One of the most prevalent forms of crime nowadays, often targeting obtaining banking data for stealing funds or engaging in online shopping using other people's cards.
 12. **Data Theft:** The process of stealing digital information stored on devices, servers, or in the cloud, which often involves sensitive information or privacy violations.



2. 24 figurines corresponding to numbers to start the game, each figurine marked with a unique number from (1-24).
3. 24 cards dedicated to the stations explaining cybersecurity terms, clarifying the reason for the station's positive or negative impact for students.
4. 10 medium-sized plastic tokens distributed among the students at the beginning of the game (divided into two groups, each group having 5 different shapes in one color, allowing each student to choose a unique token to move with).
5. 60 large green cards representing various rewards, as follows:
 - 5 cards (You can play the next round).
 - 5 cards (Congratulations, you've won the Team Leader card).
 - 5 cards (You've won the Cybersecurity card).
 - 5 cards (You've won the Golden card).
 - 5 cards (You've won the Silver card).
 - 5 cards (Congratulations, You've won the Bronze card).
 - 5 cards (You've won the Key Symbol).
 - 5 cards (You obtained the Wi-Fi Symbol).
 - 5 cards (You can discard the Eye Symbol for yourself or your team).
 - 5 cards (You can discard the Trojan Horse Symbol for yourself or your team).
 - 5 cards (You've gained 2 coins from the opposing team).
 - 5 cards (Choose a penalty for the opposing team).



6. 60 large red cards representing various penalties, as follows:

- 5 cards (Skip the next turn).
- 5 cards (Leave the team).
- 5 cards (Give up 2 coins to the opposing team).
- 5 cards (You/your team lost the team Leader card).
- 5 cards ((Received a Spy card).
- 5 cards (You/Your team lost the Golden Card).
- 5 cards (You/your team lost the Silver card).
- 5 cards (You/your team lost the Bronze card).
- 5 cards (You/your team lost the Cybersecurity card).
- 5 cards (You/your team lost the Wi-Fi Symbol).
- 5 cards (Gained the Eye Symbol).
- 5 cards (Gained the Trojan Horse Symbol).



7. 40 large colored side symbols distributed by the referee among the students, as follows:

- 10 pieces of the Key Symbol (Symbol = 5 coins).
 - 10 pieces of the Wi-Fi Symbol (Symbol = 10 coins).
 - 10 pieces of the Eye Symbol - The symbol causes its owner/team to lose 5 coins.
 - 10 pieces of the Trojan Horse Symbol - The symbol causes its owner/team to lose 10 coins.
8. 200 Coins pieces dedicated to rewards, penalties, and final score calculation for each team



Gameplay mechanics:

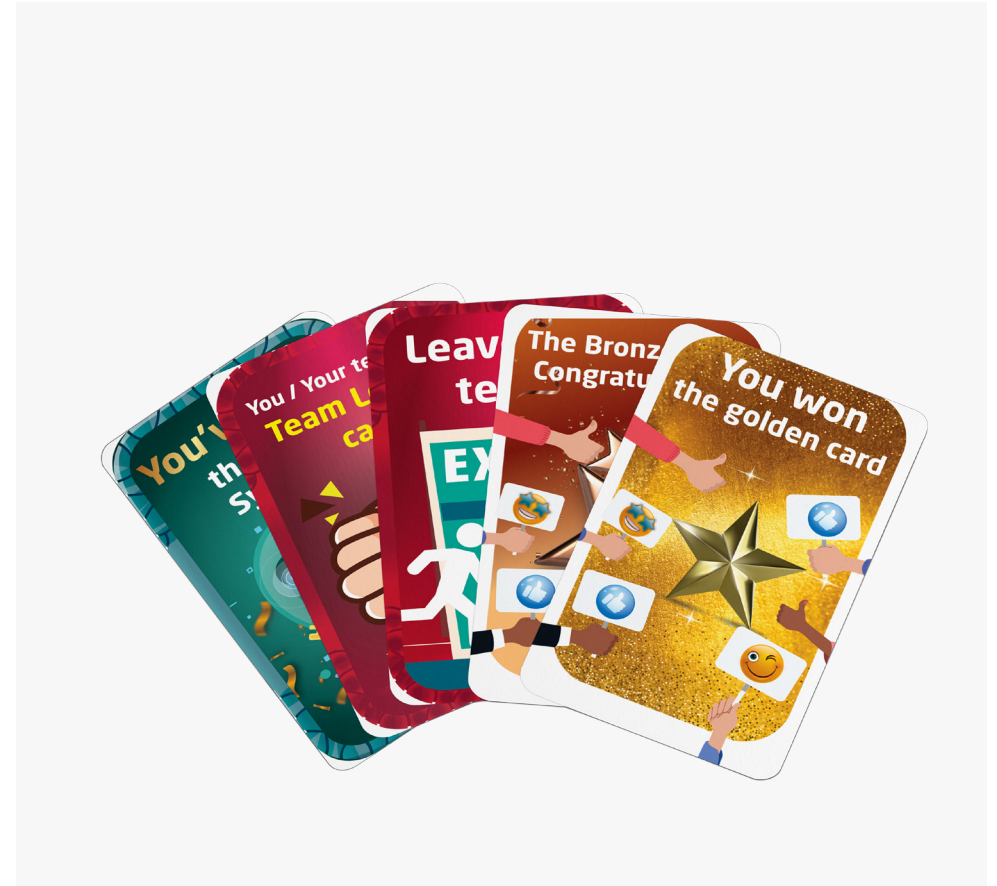
1. The game relies on teamwork, where students are divided into two teams, each team consisting of one or two students. An additional student takes on the role of the referee, distributing rewards and penalties to the members of both teams.
2. Each student receives a small token to move on the board.
3. The player chooses a random number from the figurines with numbers and moves according to the number that appears to them.
4. If a student lands on a safe station, they will receive the corresponding information card and read the information to their teammates for discussion. Then the players choose from a set of green cards, which are various rewards such as:
 - You can play the next turn.
 - Congratulations, you have become the team leader.
 - You won the golden card.
 - You won 2 Coins from the opposing team.
 - o You won the key symbol.
5. If the player lands on a dangerous red station, they will receive the corresponding station's explanatory card. They will read the information on the card to their teammates for discussion. Then the player chooses from another set of red cards, which are various penalties, such as:
 - Skip the next turn.
 - Leave the team.
 - Give up 2 Coins to the opposing team.
 - You won the Eye symbol.
 - You won the Spy card.
 - o Your team lost the golden card.



6. The turns continue between the players, and in the end, the points are counted for each team, as following:

- Key symbol (worth 5 Coins).
- Wi-Fi symbol (worth 10 Coins).
- Eye symbol (makes its owner/the team lose 5 coins).
- Trojan Horse symbol (makes its owner/the team lose 10 coins).
- Team leader card (doubles the player's points, so if the leader has 5 coins, for example, their points count as 10 coins).
- Golden card (worth 15 Coins).
- Spy card (causes the owner/ the team to lose 10 coins).

7. The winning team is the one with the highest number of points.





The Second Game: Cyber Quiz

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.

Game Goals

1. Teach students new and simplified cyber terms.
2. Recognize the benefits or risks of new cyber terms.
3. Enhancing linguistic and cognitive skills in the field of cybersecurity for students.
4. Strengthening students' cybersecurity knowledge through entertainment and competition elements.
5. Writing terms in both Arabic and English directly assists in improving linguistic skills and reading ability.
6. Give children enthusiasm, entertainment, and a sense of accomplishment by competing to gain the most points by correctly answering cybersecurity questions.

Recommended age for the Game

+7 years



Game Components:

1. 25 medium-sized plastic figures/symbols with numbers from 1-25, each with a different number.
2. 100 medium-sized coins distributed to students for correct answers.
3. 25 cards related to cyber topics, each card covering a specific cyber topic, including essential summarized information in a simplified manner (each card numbered from 1-25 with the card's title).
4. 100 question cards; for each topic, there are four cards containing questions about the specific cyber term reviewed in the card, which students must answer to earn points (one card for each question).
5. A flyer containing a model of answers to the cyber topic questions.
6. A small hourglass timer to measure the time to answer each question.
7. Game Manual.



Gameplay mechanics

1. The game relies on individual performance (up to a maximum of 5 students), where each student competes with their peers to win and accumulate the highest number of Coins (points).
2. One of the students takes on the role of the referee to distribute questions and evaluate answers.
3. Initially, the game board is laid out in front of the students, and cards and the sand timer are placed in their designated spots on the board.
4. Each student chooses a random number from numerical figurines, and the one with the highest number starts the game.
5. The first student selects a numbered figurine without seeing the assigned number and, based on the revealed number, determines the cyber topic card for which they will answer one question.
6. The student draws the cybersecurity topic card based on the number, reads the information aloud, and discusses it with their peers and the referee.
7. The referee then asks one question from this card to the student, and the timed countdown for answering begins.
8. If the student answers the question correctly before the time runs out, they receive one piece of Coin (each piece is worth one point).
9. If the student does not answer the question within the specified time, they receive nothing.
10. If the student answers the question incorrectly, they receive nothing.
11. Roles rotate among the students, and each student strives to collect as many Coins (points) as possible during the game.
12. The winning student is the one with the highest accumulation of Coins (points).



Cyber Card Topics and Questions:

1. Data Integrity

Data integrity is a crucial aspect that must be preserved and protected from malicious attacks or theft. **The four cards for this topic are as follows:**

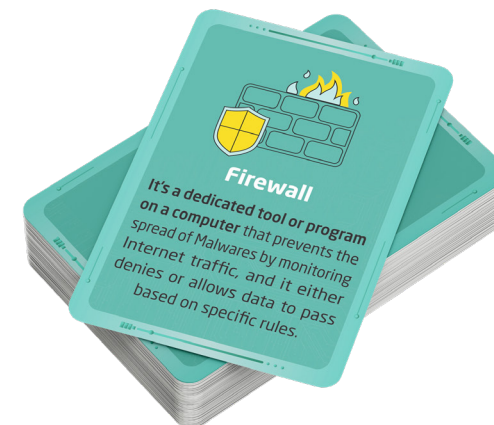
1. Wallet and ID extended for someone to grab (Question: True or false?)
2. Our WhatsApp conversations are visible to others. True or False?
3. We don't share our personal and family photos with strangers. True or False?
4. Customizing our Facebook posts to be visible to friends only. True or False?



2. Firewall

It's a dedicated tool or program on a computer that prevents the spread of Malwares by monitoring Internet traffic, and it either denies or allows data to pass based on specific rules. **The four cards for this topic are:**

1. Firewalls can be programs or tools. True or False?
2. Firewall is a security tool. True or False?
3. The firewall is not related to the Internet. True or False?
4. The firewall prevents the spread of Malwares. True or False?



3. Information Security

The process of designing and using tools to protect important information from damage, loss, modification, or disruption, especially during transmission or storage. **The four cards for this topic are as follows:**

1. Information is organized data processed on a computer. True or False?
2. Information security involves using tools to protect important data. True or False?
3. Information security is the protection of data stored on computers. True or False?
4. Protecting data from damage is one of the goals of information security. True or False?



4. Application Security

Messaging applications provide an easy way to communicate with friends, but they can pose a threat to privacy if data is breached. Therefore, it is necessary to apply security rules when using them. **The four cards for this topic are:**

1. Messaging applications do not pose a threat to individuals' data. True or False?
2. WhatsApp is one of the most popular messaging and communication applications. True or False?
3. Encrypting data in messaging applications does not protect privacy. True or False?
4. Following security rules in messaging applications prevents data breaches. True or False?



5. Hackers

Hackers are digital criminals with high programming and technical capabilities in dealing with software, networks, and computer architecture. They exploit their technical expertise for various purposes, such as theft, defamation, sabotage, or simply to demonstrate their high competence. **The four cards for this topic are:**

1. A hacker is someone who obtains information legally. True or False?
2. Hackers have high programming and technical capabilities. True or False?
3. Hackers primarily use security vulnerabilities in their work. True or False?
4. Data theft is not one of the goals of hackers. True or False?



6. Cyber-Attacks

A cyber-attack is an assault by an individual or organization to control, modify, or destroy data using cyberspace, often targeting institutions to disrupt or harm them and compromise the integrity of the data and information they contain. **The four cards for this topic are as follows:**

1. Cyber-attacks must be conducted through internet networks. True or False?
2. Cybercriminals can be individuals or organizations. True or False?
3. Electronic device sabotage is not a type of cyber-attack. True or False?
4. Logging out of an account on a public computer. True or False?



7. Malware

Malware is specifically designed to cause harm or damage to a computer, server, client, or network without the user's knowledge, often spreading primarily via email. **The four cards for this topic are:**

1. Malware affects computers. True or False?
2. Email is one of the well-known methods for spreading malware. True or False?
3. Malware does not target theft or destruction of data. True or False?
4. Security programs prevent the spread of malware within a computer. True or False?



8. Cybercrime

Cybercrime is an advanced form of crime that occurs globally, targeting computers, networks, or infrastructure. **The four cards for this topic are:**

1. A child calls his father to see a mysterious message received from an unknown sender. True or False?
2. Cybercrimes are committed by Cyber criminals. True or False?
3. Cybercrimes do not negatively impact victims. True or False?
4. A complex, lengthy password with symbols and uppercase and lowercase letters. True or False?



9. Trojan Horses

Also known as “game thieves,” Trojan Horses are malicious software hidden as attachments in emails or free download files. Once downloaded, the malicious codes start working, attacking data and spying on users’ activities and information. **The four cards for this topic are:**

1. Trojan Horses cause data attacks. True or False?
2. Trojan Horses do not carry any harmful codes. True or False?
3. Trojan Horses are also called “game thieves.” True or False?
4. Trojan Horses spy on individuals’ data. True or False?



10. Cyberbullying

Cyberbullying involves using digital technologies for bullying, often occurring through social media platforms, messaging platforms, and games. Cyberbullying leaves a digital footprint that can be traced and attributed to the perpetrator. **The four cards for this topic are:**

1. A child isolates himself, and his peers bully him with offensive language. True or False?
2. Offensive comments on social media. True or False?
3. Cyberbullying can occur through social media platforms. True or False?
4. Cyberbullying does not leave a digital footprint. True or False?



11. Data Theft

The process of stealing digital information stored on smart devices, servers, or the cloud, often involving confidential information or privacy violations. This is typically carried out through deceptive mobile messages or misleading emails. **The four cards for the topic:**

1. Clicking on a fake ad to win a tablet. True or False?
2. Opening unknown source messages can lead to personal data breach. True or False?
3. Providing our banking data to untrusted entities. True or False?
4. Data theft does not result in any financial losses. True or False?



12. Safe Technology Practices

Technology and social media have introduced a new type of individual practices, varying between positive and negative. To fully benefit from the ongoing technological advancements, individuals must distinguish between these practices and avoid the negative ones. **The four cards for the topic:**

1. Sitting in an uneven position in front of the computer. True or False?
2. Obtaining consent before posting a specific person's picture. True or False?
3. Video games that depict violence are not suitable for children. True or False?
4. A child sitting in front of his computer for a long time with food and juice in front of him. True or False?



13. Online Fraud

One of the most widespread forms of crime currently, often targeting obtaining banking data for stealing funds or making unauthorized online purchases using others' cards. The four cards for the topic:

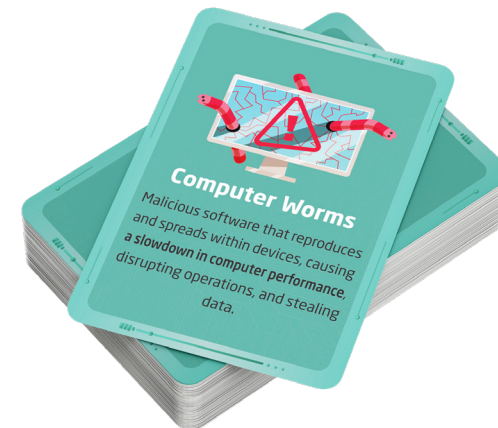
1. Online fraud aims to deceive victims to obtain financial data.. True or False?
2. Deleting a message from an unknown sender on the phone that says "Congratulations! You've won a grand prize!".. True or False?
3. Sharing phone and personal information on social media.. True or False?
4. Online fraud usually targets obtaining banking data.. True or False?



14. Computer Worms

Malicious software that reproduces and spreads within devices, causing a slowdown in computer performance, disrupting operations, and stealing data. **The four cards for the topic:**

1. Slow computer performance is a sign of the presence of worms.. True or False?
2. Opening an unknown source email with an attachment.. True or False?
3. Computer worms reproduce and spread.. True or False?
4. Worms use the device's memory, causing the device to slow down.. True or False?



15. Cloud Computing

A secure online space where a copy of data is stored, retrievable at any time and shareable with others by sending a URL. Synchronization allows accessing data across multiple devices. **The four cards for the topic:**

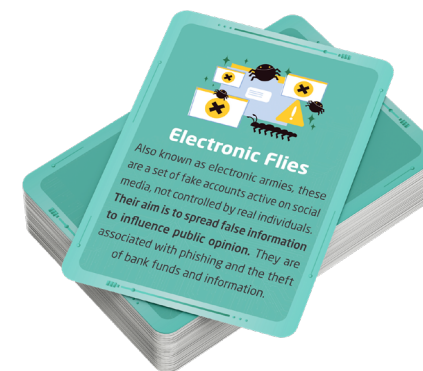
1. Data can be retrieved from the cloud at any time. True or False?
2. Cloud data cannot be shared with others. True or False?
3. Backing up your data on the cloud protects your data. True or False?
4. Cloud computing services cannot be used without internet availability. True or False?



16. Electronic Flies

Also known as electronic armies, these are a set of fake accounts active on social media, not controlled by real individuals. Their aim is to spread false information to influence public opinion. They are associated with phishing and the theft of bank funds and information. **The four cards for the topic:**

1. Electronic Flies are fake accounts active on social media. True or False?
2. The purpose of Electronic Flies is to spread false information. True or False?
3. Bank data breaches are a primary goal of Electronic Flies attacks. True or False?
4. Electronic Flies are also referred to as "electronic armies." True or False?



17. Shoulder Surfing

A social engineering trick where someone observes your computer, aiming to steal confidential information. The main purpose is to steal financial information such as credit card details or account passwords. **The four cards for the topic:**

1. In public places, be careful if someone stands behind you while entering your password. True or False?
2. I Use privacy screens on my devices so that someone standing next to me cannot see what I am doing. True or False?
3. Shoulder surfing is similar to eavesdropping on others' privacy. True or False?
4. Data can be stolen through shoulder surfing. True or False?



18. Smartphone Security

Protecting our smartphones is crucial, involving constant system updates and safeguarding against potential hacking that may lead to overheating or rapid battery depletion, risking data and personal information theft. **The four cards for the topic:**

1. Device overheating and fast battery depletion may indicate a breach. True or False?
2. Avoid using public networks as much as possible. True or False?
3. Installing apps from outside the official store protects my device from breaches. True or False?
4. Regularly updating the phone's system safeguards it against potential threats. True or False?



19. Passwords

Passwords are a protective tool for programs and applications, ensuring that only the user can access them. They protect data from tampering and theft.

The four cards for the topic:

1. Use one password for all applications. True or False?
2. Passwords should include numbers, letters, and symbols. True or False?
3. Sharing passwords with friends is acceptable. True or False?
4. "123456789" is an example of a strong password. True or False?



20. E-Games

Electronic games are enjoyable and beneficial for children, but playing games with friends is more rewarding and fun. . **The four cards for the topic:**

1. Spending a long time on electronic games does more harm than good. True or False?
2. Some slogans appearing in electronic games may not align with our religion and ethics, such as the rainbow flag. True or False?
3. Playing electronic games for extended hours is acceptable. True or False?
4. The electronic games I play should be suitable for my age and free from violence. True or False?



21. Phishing

Phishing is a deceptive method used by Hackers to steal users' personal data by tricking them, with the aim of causing harm. **The four cards for the topic:**

1. Ignoring messages from unknown senders protects against phishing attacks. True or False?
2. Using strong passwords protects against phishing attacks. True or False?
3. Opening attachments from unknown senders via email protects against phishing attacks. True or False?
4. Not sharing personal data with others protects against phishing attacks. True or False?



22. Email Security

Hackers use email to execute various crimes, such as sending attachments containing malicious software or attempting to hack users' emails to access their personal data. **The four cards for the topic:**

1. Changing the email password regularly is necessary. True or False?
2. Opening attachments from unknown senders is not recommended. True or False?
3. It's preferable to choose an easily guessable password for email. True or False?
4. Regularly updating antivirus software protects email from breaches. True or False?



23. E-learning

Amid the COVID-19 pandemic and beyond, E-learning and virtual lessons are becoming increasingly prevalent through various platforms and applications. This means that technology is more in the hands of children, requiring increased awareness and protection of home networks. **The four cards for the topic:**

1. Learning many things remotely via the internet is true. True or False?
2. Limited platforms and applications can be used for e-learning. True or False?
3. Protecting home networks is essential when children use electronic devices. True or False?
4. E-learning can be beneficial for children with certain controls. True or False?



24. Rules for Safe Internet Browsing

Following rules for safe internet browsing protects users from electronic attacks, data theft, and Electronic blackmail. **The four cards for the topic:**

1. Downloading apps from untrustworthy sites is not allowed. True or False?
2. Online ads do not pose a threat to electronic security. True or False?
3. It's advisable to keep the password and username in one place. True or False?
4. Accepting friend requests from unknown individuals is not recommended. True or False?



25. Electronic Blackmail

Electronic blackmail involves demanding money or information from individuals and companies by threatening to disclose private matters and confidential data on social media. Children are among the most vulnerable groups to electronic blackmail. **The four cards for the topic:**

1. Electronic blackmail is demanding money by threatening to disclose private matters. True or False?
2. Various methods are used to execute electronic blackmail. True or False?
3. Children are among the most vulnerable groups to electronic blackmail. True or False?
4. The motives behind electronic blackmail may be financial. True or False?





The Third Game: Cyberno

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.

Game Goals

1. Conveying important information to students about cybersecurity and its key topics, particularly cybercrimes.
2. Instilling a sense of accomplishment in students as they overcome challenges encountered during gameplay.
3. Equipping students with the skill of quick thinking and planning by encouraging them to overcome obstacles.
4. Fostering a spirit of competition among students by motivating each student to strive for victory.
5. Understanding the meanings associated with prominent electronic/ cyber terms, raising awareness about risks and threats.

Recommended age for the Game

+17 years



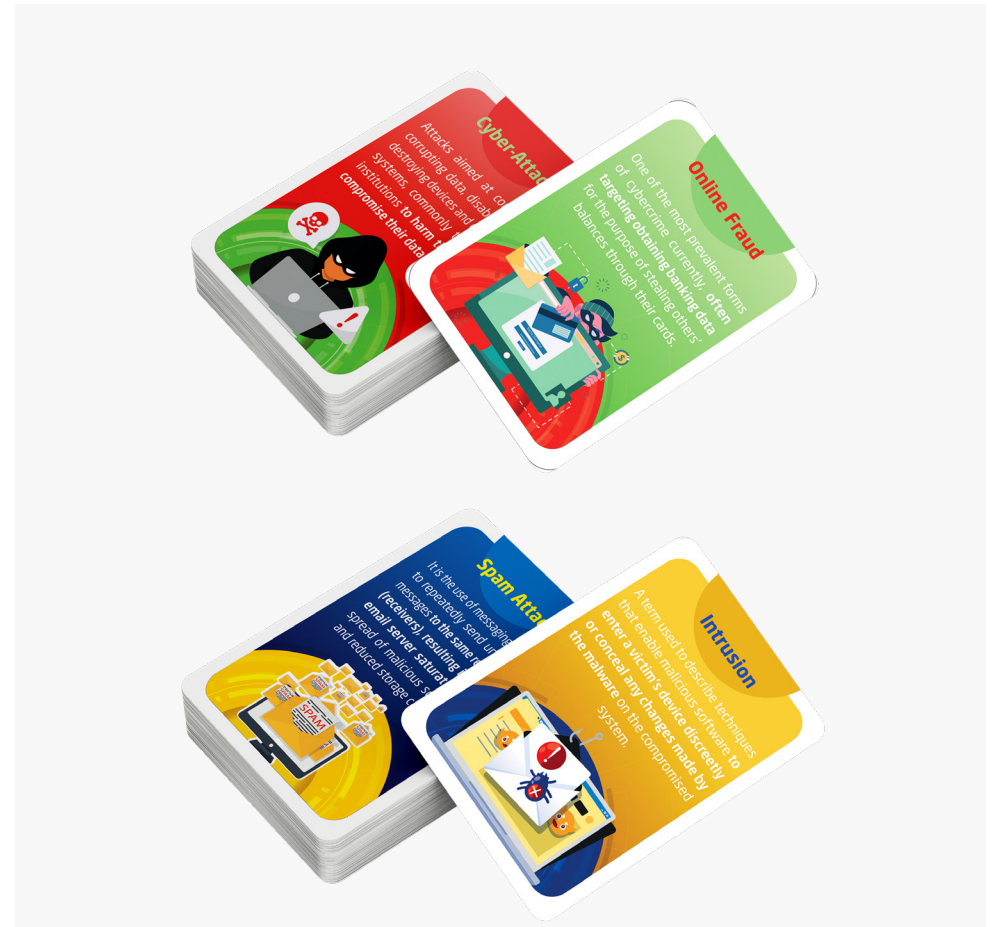
Game Components:

A total of 116 cards divided into four colors: blue, yellow, red, and green.

These cards include:

First: Four cards - one card of each color, covering major cyber topics as follows:

1. **Online Fraud:** One of the most prevalent forms of cybercrime currently, often targeting obtaining banking data for the purpose of stealing others' balances through their cards.
2. **Cyber-Attacks:** Attacks aimed at controlling, corrupting data, disabling, and destroying devices and operating systems, commonly targeting institutions to harm them and compromise their data security.
3. **Intrusion:** A term used to describe techniques that enable malicious software to enter a victim's device discreetly or conceal any changes made by the malware on the compromised system.
4. **Spam Attack:** It is the use of messaging systems to repeatedly send unwanted messages to the same recipients (receivers), resulting in fraud, email server saturation, the spread of malicious software, and reduced storage capacity.

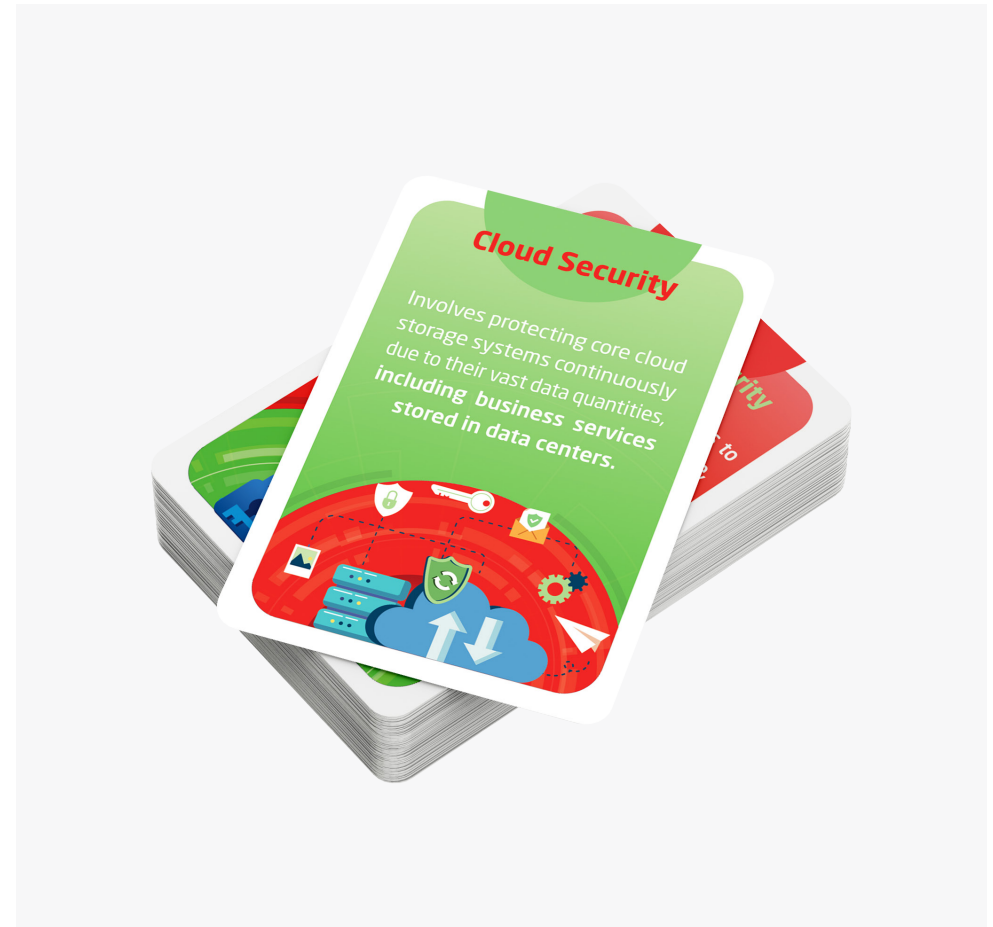


Second: 72 cards encompassing various cyber topics including:

1. **Network Security:** Securing computer networks from intruders through software and different devices, including firewalls and email security.
2. **Information Security:** Designing and deploying tools to protect information from damage, loss, alteration, or unauthorized access, especially during transmission or storage, involving encryption and vulnerability management.
3. **Application Security:** Focuses on keeping software and devices free from threats, often done during the design phase well before the software or device is deployed.
4. **Operational Security:** Risk management process for all internal cybersecurity operations, encompassing decisions related to data asset handling and protection.



-
5. **Cloud Security:** Involves protecting core cloud storage systems continuously due to their vast data quantities, including business services stored in data centers.
 6. **Infrastructure Security:** Security measures protecting critical infrastructure, such as communication systems, data centers, and servers, safeguarding them from terrorist acts, corruption, and sabotage.
 7. **Cyber Deterrence:** Concerned with preventing harmful acts and attacks that might occur in cyberspace.
 8. **Cybercrime:** An advanced form of crime occurring globally, targeting computers, networks, or infrastructures.
 9. **Phishing Attacks:** A type of attack aimed at stealing or damaging sensitive data by deceiving individuals to obtain and manipulate their personal information.
 10. **Spear Phishing Attacks:** A fraudulent operation conducted through email or electronic communications to steal data, often relying on installing Malwares on the victim's device.



- 11. Whale Phishing Attacks:** Target specifically sensitive and confidential information, particularly of the rich and famous, for blackmailing or gaining compensation for that data.
- 12. Encryption Attacks:** Malicious script that automatically downloads and installs itself onto a victim's device without permission, subsequently used to breach and steal or control all of the device owner's data.
- 13. Ransomware:** Software targeting sensitive information, causing device shutdowns or encrypting essential data, which the owner can only access after paying a ransom.
- 14. Eavesdropping Attacks:** Attacks relying on snooping and subsequently stealing information and transmitting it over a network through a computer or smart device.
- 15. Malware Attacks:** Specifically designed malicious software intended to cause harm or damage to a computer, server, client, or network without the user's knowledge.



- 16. Trojan Horses:** Malicious software hidden as attachments in an email or freely downloadable file; once downloaded, malicious codes start operating, attacking data.
- 17. Man-in-the-Middle Attacks:** A type of eavesdropping attack often targeting existing conversations or confidential data shared between two parties.
- 18. Firewall:** A dedicated tool or software on a computer that monitors network processes, allowing or denying the passage of a program based on specific rules.
- 19. Malware:** Malicious software designed to cause harm to a laptop, desktop, or mobile device, potentially slowing down or completely halting its operation.
- 20. Computer Worms:** A type of malicious software capable of self-replication, often spreading across networks by exploiting security vulnerabilities.



- 21.Information security Tools:** Mechanisms employed to safeguard information and data circulated online from tampering and sabotage, using methods to protect them from internal and external risks.
- 22.Data Recovery:** The process of rescuing data that cannot be accessed from the damaged secondary data storage or from the multimedia.
- 23.Data Integrity:** Safeguarding your data and personal information is crucial, protecting them from destructive attacks or theft.
- 24.Information Confidentiality:** It involves managing access to data and facilitating its availability, specifically by defining the authorized categories permitted to access the data.
- 25.Encryption:** It refers to ensuring the security of information by using encrypted algorithms, hashes, and signatures.
- 26.Digital Signature:** Digital signature systems serve as a form of public encryption for data, ensuring data integrity, authentication, and non-repudiation using a private key.



- 27. Message Authentication Code (MAC):** Involves multiple parties sharing a key. One party creates an authentication code attached to the document, and the other can verify the message's integrity through the same key.
- 28. Cryptographic Computing:** Encompasses various technologies including secure multi-party computation, homomorphic encryption, and searchable encryption.
- 29. Hackers:** An individual possessing high software and technical capabilities enabling them to exploit security vulnerabilities in software, systems, and websites for diverse purposes.
- 30. Safe Technology Practices:** The advent of technology and social media has introduced a new set of individual practices, varying between positive and negative practices.
- 31. E-War:** A set of measures used in traditional wars, involving the use of friendly electronic systems to survey the electromagnetic radiation emitted from enemy systems and devices.



- 32. Electronic Reference:** The process of providing the necessary information for Cyber-attacks or electronic protection.
- 33. Cyber Terrorism:** The use of electronic and digital technologies to cause harm, intimidates, coerce others, or attack information systems of individuals and institutions.
- 34. Stalker ware:** A type of technology allowing an individual to monitor and spy on another person by installing an application or software on their phone or computer without their knowledge.
- 35. Digital Risk Management:** The implementation of digital processes aimed at providing necessary support to ensure business continuity and enhance risk assessment.
- 36. Security Vulnerabilities:** Weaknesses, flaws, or errors found within computer systems and networks that attackers can exploit to breach a secure network.



37. Security Vulnerabilities Management: An ongoing, proactive, and often automated process that maintains the security of computer systems, networks, and enterprise applications against online attacks and data breaches.

38. Penetration Testing: A program that helps IT specialists to identify and exploit security vulnerabilities in computer systems.

39. Intelligent Risk Analysis: A risk protection program providing organizations the ability to track, monitor, analyze, and prioritize potential risks for better self-protection.

40. Information Types: Information can be inactive (e.g., a file on a hard drive), mobile (e.g., exchanged electronic communications between two or more parties), or in use (during data computing).

41. Misleading Marketing Messages: Messages sent by hackers via smartphones for marketing products and services, but with the aim of hacking these devices and stealing data.

42. Identity Verification: The process of confirming someone's identity, which may use various methods, including government-issued identification requests.

43. Digital Identity Verification: Confirming someone's digital identity online, such as verifying government databases and social media profiles.

44. Electronic Piracy: Hacking computers over the internet, carried out by individuals or groups experienced in computer software and content recognition.

45. Click jacking: Deceptive attacks manipulating users to click on an invisible or disguised element on a web page, causing unintentional downloading of Malwares.

46. Like Jacking: In this deceptive attack, users are tricked into clicking the 'Like' button on Facebook. The user is required to log in to the website when clicking the link for the attack to succeed.

47. Cursor Jacking: Creating a duplicate cursor attached to the real cursor at a specific offset, making only the duplicate cursor visible, leading to clicking on a malicious link while maneuvering the fake cursor.

48. Content Security Policy (CSP): A detection and prevention mechanism used to reduce cyber-attacks like XSS and click jacking.

49. Zero-Click Attack: A remote attack on a device that doesn't require any additional actions from the user, which can be executed over the air (OTA).

50. Electronic Blackmail: Using online threats to individuals by publishing sensitive information on the internet if they fail to comply with demands from the attackers.

51. Generating Fake Content: Artificial intelligence can create fake content that appears to have been generated by the victim themselves, such as deceptive text messages or emails.

52. Threats of Publish: Using AI to generate threatening messages mimicking the victim's language, where criminals threaten to publish sensitive information on social media if their demands are not met.

53. Espionage and Surveillance: AI monitoring of victims' activities online and on social media, using this information for extortion.

54. Information manipulation: AI can manipulate online information like altering images or modifying messages to appear as if they were from the victim.

55. Exploiting Audio and Animation Techniques: Creating fake audio and animations that seem to involve the victim in inappropriate behavior.

56. Interacting with victims: Designing interactive conversation scenarios with victims and running automated chats to gather information or demand compliance.

57. Personal Data Breach: The theft or leakage of sensitive information by an individual, organization, or group of information hackers seeking it.

58. Multi-Factor Authentication (MFA): An authentication method requiring two or more verification factors—like passwords or fingerprint—to access a source, such as an application or an account on a website.

59. Cloud Computing: A term referring to on-demand computer resources and systems available over the network, capable of providing integrated computer services without relying on local resources.

60. Privilege Escalation: The term refers to an attacker who successfully breaches one or more accounts and takes advantage of those limited privileges to gain access to accounts with higher privileges.

61. Impersonation: The falsification of the sender's email header by an attacker to make the message appear as if it was sent from someone other than the actual source.

62. Email Spoofing: A tactic used in phishing as email users often open messages if they believe it comes from a legitimate and trustworthy source.

63. Social Engineering: This is not a cyber-attack but involves gaining people's trust, persuading them to let their guard down, and encouraging them to take unsafe actions, such as disclosing personal information.

64. Cyberspace is the global environment composed of physical components such as computers, communication networks, digital infrastructures, and internet users, along with non-physical components like software, computer systems, and communication systems.

65. Business Email Compromise (BEC) attacks: A form of email scam where the attacker claims to be a high-level executive, attempting to deceive the recipient to carry out tasks for unlawful purposes.

66. USB Baiting: Cybercriminals install malicious software on USB drives and leave them in strategic locations, making them accessible to someone who uses them, thereby exposing themselves to multiple harmful codes.

67. Privacy: It refers to an individual or entity's ability to isolate themselves and prevent their information from being known by others, particularly organizations and institutions.

-
- 68. Data Packets Sniffing:** These attacks monitor traffic using an application or device, making the victim's web traffic vulnerable to internet criminals.
- 69. SSL BEAST:** Hackers infect the user's computer with malicious JavaScript. Then, the malware intercepts the web cookies and authentication tokens of the website for decryption.
- 70. Browser Cookies:** Useful parts of website information stored by sites visited by users, aiding in remembering web activity and login processes.
- 71. SSL Stripping:** Hackers intercept the Transport Layer Security (TLS) signal from the application or website and modify it to load the site on an insecure connection as HTTP instead of HTTPS.
- 72. Forging Packages:** Hackers create seemingly normal packages and inject them into an existing network to access and monitor data traffic or launch Distributed Denial-of-Service (DDoS) attacks.

Third: 8 Cybersecurity Cards - 2 of each color. These cards allow their owners to have three choices of a subject title, from which they can select only one answer only once.

Fourth: 8 Fraud Crime Cards - 2 of each color. These cards help their owners trick the answer to the card's subject title, and the subsequent student is then required to answer instead.

Fifth: 4 Data Theft Crime Cards. These cards grant the student the right to take over the guessing card from its owner and to choose 3 students to answer the card's subject title. The owner of the incorrect answer will be penalized by losing two cards.

Sixth: 4 Data Breach Cards. With these cards, a student requests another specified student to answer on their behalf or draws 3 cards. In the case of an incorrect answer, 4 cards are drawn.

Seventh: 8 Infrastructure Breach Cards - 2 of each color. These cards immediately terminate the current round of the game and start a new one, but the condition is to start from the last participant in the previous round.

Eighth: 8 Cyberbullying Cards - 2 of each color. These cards allow their owners to select a card from their set and request the first cardholder to guess its subject title. In case of an incorrect answer, 3 cards are drawn.

Gameplay mechanics

- The game must consist of two or more students, with the number of participants reaching up to 6 individuals.
- The minimum age to participate in the game is 17 years old.
- At the start of the game, the game board is placed on the table. Each student receives 7 cards, and the remaining cards are placed in the designated area for drawing cards during the game.
- The game always begins after arranging the cards randomly and distributing 7 cards to each student. The game starts with the student sitting to the right of the card distributor.
- The student chooses one card from their collection and starts explaining the term that represents the subject of the card without mentioning the card's title.
- The next student must guess the title of the card, with only one attempt allowed for guessing.
- If the second student answers correctly, the first student places the card in the designated place for used cards on the game board and takes another card from the draw pile. Meanwhile, the third student draws one card from the second student's collection.
- If the second student gives an incorrect answer, they take two cards from the draw pile, and it becomes the turn of the third student to guess the card's title.
- If the third student answers correctly, the first student places the card in the designated place for used cards, takes two cards from the draw pile, and the fourth student draws a card from the third student's collection.
- If the third student answers incorrectly, they take 3 cards from the draw pile, and it becomes the turn of the fourth student to guess the card's title.
- The game proceeds in this manner until completing a full cycle, then starts again with a new card.

-
- If a student has only one card left, they must say “Last card” before passing their turn; otherwise, they will be penalized by drawing 6 cards from the draw pile.
 - During the game, each student must try to get rid of the cards they possess. When a student plays their last card, they must say «Cyberno,» becoming the first winner.
 - The turns continue among the remaining students until the last student becomes the loser.
 - In the event that the reserve draw cards are exhausted and there are still multiple students left, the game distributor temporarily stops the game, rearranges the cards, designates them again as reserve cards for drawing, allowing students to draw from them.

Game Rules:

- If a student owns a Cybersecurity card, they can request three choices for the card’s title when it’s their turn to guess, from which they can choose only one answer once.
- If a student owns a Fraud card, they can deceive in answering the card’s title, and the next student is obliged to answer instead of them.
- If a student owns a Data Theft card, they can take the card’s place for guessing from its owner, select 3 students to answer the card’s title, and penalize the incorrect answerer among them by drawing two cards.
- If a student owns a Data Breach card, they can request another specific student to answer the card’s title instead of them or draw 3 cards. In case of an incorrect answer, they draw 4 cards.
- If a student owns an Infrastructure Breach card, they can immediately end the current game cycle and start a new cycle, but it must begin from the last person in the previous cycle.
- If a student owns a Cyberbullying card, they choose a card from their collection and request the student who owns the first card to guess its title. If the answer is wrong, they draw 3 cards.



Fourth game: Cyber Way

Game Idea

The game idea is to hold knowledge competitions about cybersecurity among students. The game combines challenge, competition, knowledge, and entertainment. It provides information and tests the students' knowledge base in a competitive framework based on competition and entertainment.

The game consists of a board divided into 100 small squares, with a beginning and an end. The squares are colored in different colors. Each student has a special figure that they place on the board. The game comes with a dice, which is rolled and the student's figure is moved to the squares according to the number of points that appear on the dice.

The game begins with the students rolling the dice. The student with the highest number of points goes first, followed by the student with the second highest number. Landing on any square gives a distinctive difference in the moves.

The first student to reach square number 100 is the winner.

Recommended age for the Game

+15 years

Game Title

The game is named "Cyberway," which consists of two parts: the first part, "cyber," refers to the cybernetic environment, and the second part, "way," signifies the cyber path or route. Consequently, the name of the game becomes "Cyberway," meaning the cyber path. This aligns with the essence of the game, which involves a path that the player follows starting from square number (1) and ending at square number (100).

Game features

The game requires the existence of three teams, each with a different color, corresponding to the known hacker hats.

1. Red Team

An attack team aims to carry out virtual attacks on the digital systems and infrastructure of institutions. It seeks to hack these systems, but not to harm them, but rather with the aim of determining the possibility of penetrating them. If penetration is possible, this means that the organization's security systems are weak and cannot withstand cyber-attacks.

2. Blue Team

A team specialized in cybersecurity, but it is a defensive team whose primary mission is to protect the institution from hacking. It is responsible for dealing with and protecting data, devices, and infrastructure.

3. Purple Team

Derived from the blue and red teams. It relies on the results of the work of both teams. It prepares a list of vulnerabilities and weaknesses that the red team can find, and presents it to the blue team to repair and improve the cyber defense systems for these vulnerabilities.

Game components

1. The main game board: It is divided into squares with numbers from 1 to 100. The squares of the board are colored according to the colors of the hats; and within some squares of the board there are shapes, divided into two sections; shapes that symbolize digital security, and others for danger. The shapes that symbolize security are the shield and key symbols, and the shapes that symbolize danger are the spider and skull symbols.
2. Figures of different shapes, divided into 3 colors according to the colors of the hats, which are distributed to the students when they start playing.
3. A dice to determine the order of the students, and to move the figures on the board.
4. 90 question cards (30 cards for each color).
5. A flyer that includes the answers to the questions contained in the cards.



Types of squares

The squares on the board are colored according to the colors of the hats. When the blue team rolls the dice, it moves normally within its blue squares. But, when it stands on one of the squares of the other hat teams, it will have to answer the questions of the other team, as it got one of its squares. If it fails to answer, it will return to its previous square before rolling the dice.

- **Blue squares:**

Its questions will be on advanced cybersecurity concepts of a defensive nature such as: (digital fingerprint analysis - DNS audits, network activity monitoring, use of least privileged access, enforcement techniques, malware analysis, operating systems, digital forensics, and incident response).

- **Red squares:**

Especially advanced concepts of an attack nature, such as: (penetration testing, communications interception, social engineering, software development, physical security).

- **Purple squares:**

Related to the most serious cybersecurity risks (deploying intrusion detection/prevention activities, monitoring network traffic for suspicious activity, regular vulnerability scanning, developing and implementing a comprehensive security plan, launching malware attacks and cyber bugs against critical systems, executing social engineering attacks, attempt to access sensitive data, Identifying and correcting security vulnerabilities).

Gameplay rules

1. The game is based on teamwork and can be played with a minimum of 3 students.
2. The students are divided into 3 teams, according to the colors of the hats.
3. Each student chooses a figure of their team's color to move on the game board.
4. Each student rolls the dice, and the student with the highest number of points starts the round, followed by the student with the second highest number.
5. When a student's figure is on a square of the same color as their team, the game proceeds as normal. For example, if the blue team's figure is on a blue square, there are no consequences. However, if the figure is on a square of a different color than the team's color, the student will be required to answer a question from the team whose color matches the square. For example, if the blue team's figure is on a red square, the blue team will then need to answer a question from the red team. If the student or any member of their team fails to answer the question, the student will return to their previous square before rolling the dice. However, if the student or any member of their team answers the question correctly, the student will move one square forward, and the rest of the students will follow do the same.
6. If a student's figure is on a square with a shield symbol, the figure will move one square forward. If the figure is on a square with a key symbol, the figure will move two squares forward. The shield and key symbols

help students progress forward. (If a student's figure moves one or two squares forward, the student will not be required to answer any questions if the figure lands on a square of a different color than the team's color. This is because the student is considered to have already answered questions from the other teams in the previous step).

7. If a student's figure is on a square with a spider symbol, the figure will move one square backward. If the figure is on a square with a skull symbol, the figure will move two squares backward. The spider and skull symbols push students backward. (If a student's figure moves one or two squares backward, the student will not be required to answer any questions if the figure lands on a square of a different color than the team's color. This is because the student is considered to have already answered questions from the other teams in the previous step).

8. The game continues in this manner and the team whose student reaches first to square number 100 wins.
9. If all of the questions have been answered and no student has reached square number 100, the game is stopped, and the winner is the student whose figure is in the square closest to 100.



The Fifth Game Educational Ideas Game



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 roles are exchanged between the parties (teacher/students) and (parents/students) in asking and answering questions.

Recommended age for the Game

4-6 years (Primary School)

Game Goals:

1. Teach young students new and simplified cybersecurity terms and ideas.
2. Develop linguistic and cognitive skills in the cybersecurity field for students.
3. Establish cognitive foundations in the field of information technology for young students through a blend of entertainment, competition, and learning.
4. Provide students with doses of fun and entertainment and a sense of accomplishment through various interactive competitions.

Game Components:

1. 30 competition cards in 5 main cybersecurity and technology topics (6 colored cards in one color for each topic).
2. Game board.
3. Model answer
4. Game guide.

Game Mechanics:

1. The game relies on individual performance and can be played by two or more students, where each student competes with their classmates to answer as many questions as possible.
2. One of the students/parents acts as the referee to distribute the cards to the students and evaluate their answers using their respective model answer.
3. Initially, the referee shuffles the cards randomly and places them on the game board.
4. The first round of the game begins with each student randomly choosing one card without seeing the questions.
5. Then everyone starts answering the questions on their cards at the same time, individually and without assistance.
6. The winner of the first round is the student who answers their question correctly and is the first to do so.
7. After all students have finished solving their first question, the referee collects the used cards and puts them in the designated place on the game board.
8. The students start a new round with new cards and using the same previous method.
9. The game continues in this manner until all the cards are used or until everyone decides to end the game.
10. The referee keeps track of the number of rounds each student has won, and the winner at the end is the student who has won the most rounds. If a student manages to win 5 rounds, which is the highest number among their classmates, they are declared the winner.

Assessment Criteria for Student Performance in Training Games

Training games have several goals, the most important of which are training and evaluation goals. Through the performance of students in the games, it is possible to conduct an initial evaluation of their benefit from the training and educational content provided to them during the training workshops. The ability of the student to progress in the games and win them depends primarily on their cognitive knowledge in the field of cybersecurity. Therefore, students who are able to reach advanced stages in the games and win them are considered to have achieved a high level of cognitive benefit from the training workshops, and vice versa.

Therefore, when students play the game, the trainer must evaluate their performance through a pre-organized table, which records the type of the game and the names of the participating students in a single round. For each student, the trainer records their observations on the performance of each student. The following is an explanation of the details of the collective evaluation cards dedicated to the training games.

Game Name							
Trainer's Name:				Educational Stage:			
Serial	Student Name	Evaluation Criteria					
		Consistency with peers	Understanding the game and grasping its rules	Ability to progress in the game	Ability to answer game questions	Ability to benefit from training workshops in dealing with the game	Trainer's Notes
1							
2							
3							
4							

Regarding the evaluation criteria, according to the scientific methodologies adopted in this field, the higher the number of rating scale points, the more accurately the evaluation process reflects reality. The evaluation card is based on a four-point scale, as shown below:



Indicator	Indicator Meaning	Indicator Symbol	Indicator Meaning	Indicator Symbol	Indicator Meaning	Indicator Symbol	Indicator Meaning	Indicator Symbol
Consistency with Peers	Not consistent at all	(-)	Minimally consistent	(+)	Moderately consistent	(+ +)	Very consistent	(+ + +)
Understanding the Game and Grasping Its Rules	Did not understand the game at all	(-)	Adequate understanding of the game	(+)	Moderate understanding of the game	(++)	Complete understanding of the game	(+ +)
Ability to Progress in the Game	Unable to make progress in the game	(-)	Able to make slight progress in the game	(+)	Able to make moderate progress in the game	(+ +)	Able to make excellent progress in the game	(+ + +)
Ability to Answer Game Questions	Unable to answer game questions	(- -)	Able to answer game questions to some extent	(-)	Able to answer game questions at an average level	(+)	Able to answer game questions at an excellent level	(+ +)
Ability to Benefit from Training Workshops in Dealing with the Game	Did not demonstrate the ability to benefit from training workshops in dealing with the game	(- -)	Demonstrated limited ability to benefit from training workshops in dealing with the game	(-)	Demonstrated moderate ability to benefit from training workshops in dealing with the game	(+)	Demonstrated excellent ability to benefit from training workshops in dealing with the game	(+ +)

According to the above encoding table, when the trainer observes that a student is moderately consistent, they would mark it as (+ +), and similarly for the other evaluations, each of which has its own corresponding symbol.

