Lesson Plan

2023-1-SK01-KA220-SCH-00015112

Topic	Security and Digital Tools	
Block Title	**Cyber Guardians: Exploring Security through Digital Tools**	
Age category 9-16	**Duration (min)** 100 min	**Number of teaching hours** 3

Student-oriented educational goals (content and performance standards)

Main Goal: Understanding the Importance of Cybersecurity. Students will learn about different types of digital security threats and how technology can be used to protect information and data. The 3D World will be used to simulate cybersecurity scenarios and students should be able to solve them, preferable working in teams, promoting teamwork and innovative problem-solving.

Didactic materials and didactic techniques

Computers with access to the internet or a local network where the 3D World environment will be hosted.

References/Sources (videos, methodologies

Motivational phase

Duration (min): 10 minutes

The objective is to make an Introduction about digital security and get students thinking about the

importance of protecting information online. This can be achieved with an activity in the Virtual World that resembles a Maze.

The students will arrive at a great maze with a sign at the beginning "The Cyberworld Maze". Inside the Maze they will find different obstacles representing common security threats such as phishing emails, malware, or password hacking. For each obstacle they will encounter challenges like puzzles and quizzes that will require them to identify ways to avoid or mitigate these digital threats. Solving these challenges will allow the students to find the exit of the maze.

Exploratory phase

Duration (min): 20 min

The objective is to encourage students to explore how cybersecurity tools work, allowing them to discover key principles of digital security through interactive learning. The proposed activity during this phase has the name "Building Your Virtual Security System". Students should work in teams to design a virtual security system for a fictional company or organization, addressing potential security threats and proposing solutions.

Students will explore different types of cybersecurity threats, such as viruses, phishing attacks, and data breaches. They will also research basic security tools, such as firewalls, encryption, and multi-factor authentication. Using the virtual world platform, students will create a digital representation of a secure office environment or data center. They will incorporate elements such as password-protected entry, encrypted data vaults, and firewalls. Teams will simulate potential security breaches in their virtual world (e.g., hackers attempting to steal data), and demonstrate how their security system protects the organization. After completing the design, each team will discuss the security features they chose to include and how they address specific threats.

The following are some key elements that should be included in the planned activity:

- Understanding of how viruses, malware, and other cyber threats work on a technical level.
- Application of security tools like encryption, firewalls, and password protection.
- Designing a functional, virtual security system to solve real-world problems.
- Calculating encryption keys, data transmission rates, or determining how secure a password is.
- Creating an engaging, user-friendly interface for the security system.

Fixation phase (consolidation and deepening)

Duration (min): 30min

The proposed activity is titled "Cybersecurity Challenge: Safeguarding the Future"

The objective is for students to be presented with a real-world cybersecurity problem and they will be tasked with designing a digital solution to protect a fictional organization or group from a cyberattack.

Three alternative Scenarios will be available:

- Design a security system to protect a smart home with internet-connected devices (IoT), such as smart speakers, cameras, and appliances. The solution must address threats like unauthorized access and data breaches.
- Develop a cybersecurity plan for a school's network, focusing on protecting student data, preventing hacking, and ensuring secure communication between teachers, students, and parents.
- Create a cybersecurity solution for a healthcare organization that handles sensitive patient data. The system should protect against hacking, unauthorized access, and data breaches while ensuring privacy.

The steps for the students are the following:

1. Students select a scenario and identify the specific cybersecurity risks involved (e.g., hacking, data theft, ransomware).
2. Teams brainstorm solutions, considering which cybersecurity tools (e.g., encryption, firewalls, authentication systems) can be applied. They will design a prototype in the virtual world platform.
3. Using the virtual world, students will simulate a cyberattack scenario (e.g., a hacker attempting to break into a system). Teams will demonstrate how their security solution protects the organization from the attack.
4. Teams present their digital security prototype to the class, explaining how it works and how it addresses the threats posed by the scenario. Feedback from the teacher and peers can help them refine their solutions.

Student Assessment

- Participation in the virtual maze and finding the way out of it.
- Creativity and functionality of the digital security system designed in the virtual world.
- Presentations and ability to explain how their security solution addresses specific threats using digital tools.

Annexes:

This project was implemented with the support of the European Commission. The support of the European Commission for the production of this publication does not constitute an endorsement of the content which reflects only the views of the authors, and the Agency and the National Commission cannot be held responsible for any use that may be made of the information contained therein.