sustainability

MDPI

Article

Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity

Borka Jerman Blažič [1,*] and Andrej Jerman Blažič [2]

[1] International Postgraduate School Jožef Stefan, 1000 Ljubljana, Slovenia
[2] Laboratory for Open Systems and Networks, Josef Stefan Institute, 1000 Ljubljana, Slovenia; andrej.jerman@gmail.com
* Correspondence: borka@e5.ijs.si

Abstract: Cybersecurity has increasingly become a headline feature in news media in recent years, generally prompted by spectacular security breaches in various information systems. The importance of cybersecurity awareness for the sustainable development of society is now recognized widely, but the problem of how to build an educational ecosystem which will include the most relevant target audiences that need to develop cybersecurity skills, is not yet solved. This paper elaborates the state of cybersecurity skills and knowledge in European high-school students by collecting data from the students, their teachers and parents by means of surveys and interviews in nine European countries. The analysis of the information collected has revealed the required topics from the area of cybersecurity that need to be introduced in high school educational programs and the most suitable delivery methods for educational content, such as videos and serious games. A selection of thirteen serious games related to cybersecurity was evaluated and then presented to a class of high-school students. The study of the collected data has shown that cybersecurity education at high school level requires innovative and interactive approaches that build the required skills for a more effective sustainable education and social development.

Keywords: education; high-school level; cybersecurity; sustainability; serious games

Citation: Jerman Blažič, B.; Jerman Blažič, A. Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity. *Sustainability* **2022**, *14*, 4763. https://doi.org/10.3390/su14084763

Academic Editors: Qusay Al-Maatouk and Waleed Mugahed Al-Rahmi

Received: 18 February 2022
Accepted: 12 April 2022
Published: 15 April 2022

1. Introduction

Cybersecurity has increasingly become a headline feature in news media in recent years, generally prompted by spectacular breaches of various information systems, including airlines, health organizations, credit agencies, administrations, financial institutions, telecoms, and many others [1]. Until recently, cybersecurity was considered an information communication technology (ICT) challenge rather than a business risk.

This finding is now driving the long-term changes in the approach to the methods used to teach cybersecurity skills. The importance of cybersecurity awareness for sustainable society development is now recognized widely, but how to build an educational ecosystem that will include all target audiences that need to develop cybersecurity skills is not clear yet. In that context, skills are understood to represent a combination of abilities, knowledge, and experience that enable an individual to successfully complete a task when working in a digital environment and using digital services [2]. The failure to address the missing cybersecurity skills of the European labor force has a negative impact on the capacity of a modern, digitized society to successfully react to the rising number of cybercrime cases. Cybersecurity skills are becoming especially important as most experts of economic development claim [3] that the digital economy's winners and losers will be determined by who has these skills. Another problem in this area is that the skills required are changing at a faster pace than usual within advanced-technology fields, due to the changes introduced by the new digital technology and fast digitalization of society.

According to several authors [4,5], only a sustainable education for sustainable social development aims at giving people the skills and knowledge that enable them to face the challenges of the fast development of the digital economy [6]. Sustainability in that context is defined as "the ability to continue an activity continuously and by pursuing the adopted goals for sustainable development". In that context sustainability of education focuses on the implementation of practices through educational development, leadership, and innovation [7]. According to Alkali and Gutiérrez [8], the interest in sustainable education is focused on students and innovative pedagogies that bring those involved in the educational process closer to social reality and its main conflicts. The main goal is to enable the students to better understand the environments where they will act every day or where they will work.

Social and economic changes have now made the issue of sustainable development more pressing than ever. As several studies have found [9], education and training in universities in several areas including ICT are very technocratic, and the educational approach is not promoted in line with sustainability requirements [10]. According to recent studies carried out in Europe [3], education for developing sustainable skills is not sufficiently integrated with European High Educational Level programs (HEI). The active pedagogical activities that help strengthen this vision are not yet included within the majority of HEI cybersecurity programs. Actions for addressing the increased cybersecurity skills shortage have been launched in Europe in the last few years [11,12] but as reported by the European Cyber Security Organization (ECSO) [12], and by other organizations [13], they are not sufficiently viewed by the European HEI as an emerging discipline important for developing the sustainability of the digital society. This finding comes from the analysis [9] of the contents of European HEI programs; it was found that these programs focus mainly on traditional cybersecurity topics as part of classical academic courses. Modern learning methodologies with hands-on training and range platforms that help in building skills have been left behind in the European HEI [5,9]. However, several actions and efforts have recently been taken and launched by the EUC, through the activities of funded Competence Centers for Cybersecurity [14], to help restructure cybersecurity programs in the HEI and among professional educational providers with the aim to overcome the existing skill gap.

A large audience among the EU population and the educational ecosystem has been left behind, as specific targeted actions to improve the missing situation were not undertaken.

The building of cybersecurity skills among high-school students and the related topics of cybersecurity within high school programs have not yet been studied at large in Europe, even though children start using the internet at an early age and more than 90% of young Europeans are online every day. The use of internet by teenagers brings many benefits linked to information and communication but comes with risks too, including privacy violation, identity theft, ransomware, fraudulent usage of debit cards, etc. It is therefore of paramount importance that a sustainable education is provided for new generations to acquire skills that make them aware of major threats, new technologies and the appropriate individual and collective behavior that helps reduce cybersecurity risks. The rapid evolution of cybersecurity attacks in connection with the static nature or even nonexistence of cybersecurity topics in school curriculums has contributed to emerging discrepancies between the knowledge taught within educational programs and the skills expected to be developed by most of the European population [15,16].

This paper addresses the issues related to the problem of building cybersecurity skills in European high-school students, the provision of relevant content and appropriate delivery methods. For this purpose, we firstly provide an analysis of the results of a survey taken at the EU level among high-school students, their teachers, and parents. This survey was aimed at identifying the current needs in terms of content and delivery methodologies fit for the secondary school level. The collected structured data of the EU-wide survey followed by interviews with a group of people provide information about the identified needs for content and educational methodology. The findings are further validated with the evaluation of one of the most popular delivery technologies that was identified by the

survey—serious games; to achieve this, several cybersecurity games offered on the web were examined. Three of these were offered to students at a high school class to obtain their opinions about the merit of these games for acquiring cybersecurity skills and knowledge.

The paper is organized as follows: after the introduction, there is a short review of the status quo, followed by the description of the methodology applied. The results and the findings from the survey are presented in the next section, followed by an analysis of suggested educational tools—serious games from the domain of cybersecurity. The paper ends with a discussion and concluding section.

2. Previous Work and Applied Methodology

2.1. Approaches in Cybersecurity Education

Cybersecurity encompasses a broad range of specialty areas and working roles, and this is the reason that no single educational program can cover all specialized skills and sector-specific knowledge desired by each audience in the digital society. However, there are certain knowledge sets and skills that are essential for most of the population in an individual's everyday life, in participating in the process of studies or in performing a critical working role they need to adopt. Considering the broad range of specialty areas, it is not surprising that cybersecurity education has been addressed differently by various countries that build cybersecurity strategies with different focuses. The educational part of these strategies is mostly formulated as strategies for improving the general state of cybersecurity in the country, which also includes the educational system [3].

Cybersecurity is taught in most of the developed countries in the upper-level undergraduate computer science courses to students who have already learned the fundamentals of computer science [17]. A current study [18] of the curriculums and cybersecurity courses taught at universities in the EU at graduate and undergraduate level has highlighted the missing topics within the on-going programs and the lack of practical training that enable the building of cybersecurity skills [19]. The education of cybersecurity within high schools was not addressed at all. More studies in this area were carried out by US researchers that found that one of the main bottlenecks in building awareness about cybersecurity and adopting relevant knowledge later within the undergraduate programs is in the inequities of the computer science education for K-12 students [20]. Another author has studied the undergraduate computer science curriculum programs taught in the top 100 UK universities with focus to the cybersecurity [21]. The study revealed that important cybersecurity concepts in mandatory and optional courses are not sufficiently covered. In USA, Wen [21] found that current programs of computer science in USA undergraduate courses do not reach 10% of security content. A study and proposal for a new cybersecurity educational model has been proposed in one EU member state. In December 2019, ENISA, the EU Cybersecurity Agency delivered an exhaustive report describing the state of development of cyber-skills in the EU [22], stressing the ever-growing lack of cybersecurity skills and cybersecurity professionals in most EU member states. However, high schools were not part of these studies and programs. The only exception is the UK, where the current UK cyber policy is to incorporate cybersecurity at all levels of education, starting at the age of 11. Other developed nations, for example Australia and New Zealand, have launched similar strategies and approaches [23]. However, most EU countries have been left behind in the domain of secondary schools due to the uneven distribution of educational programs in cybersecurity or because cybersecurity content is not included in their high-school programs at all. More recent works on the subject have been provided by Ackerman [24], Ruiz [25], Catota [26], and Conklin et al. [27]. They have also identified that the biggest concerns in the education on cybersecurity are the lack of hands-on experience in students, which results in a skills mismatch between the needs of the emerging digital society in this regard and the skills that the majority population needs to adopt to effectively use digital services. The ways to provide effective cybersecurity education have also been discussed by Conklin [27]. The problem of the sustainable education in high schools has also been addressed by Garanina [28].

The research presented in the next sections attempted to find answers to the following questions: "What are the cybersecurity contents taught at the high school level? What are the missing topics and what are the best delivery methods for an efficient and sustainable educational program that will help build skills in the domain of cybersecurity?" In looking for answers to these questions, the survey analysis presented below examined the key missing items in on-going cybersecurity educational programs. The results will be further used in actions that will contribute to build a higher awareness of the issues and to improve the cybersecurity education with the aim of narrowing the identified skill gap.

2.2. The Applied Approach

Two of the four cybersecurity competence centers established by the European Commission in 2019—Concordia and Cybersec4Europe have tasks in their action program that focus on the re-shaping of the cybersecurity educational ecosystem. The undertaken actions are still on-going. The Concordia Consortium consists of 52 participating partners coming from different sectors, with industry being represented by 26 entities and the HEIs represented by 21 European universities and 5 research centers from all over Europe [9,14]. The focus of the educational task recently launched by the Concordia team is addressing the needs to "teach the teachers" by providing knowledge about the content and delivery methods for sustainable education among the high-school community. The first step of the activity is oriented to provide a clear identification of the needs for content and delivery methodology for the high-school level education from involved stakeholders. In 2020, a "Survey—Teaching cybersecurity in high schools" was set up aimed at collecting information from a large pool of stakeholders, namely teachers, students and their parents, and the managements of high schools all over Europe. The performed work included the expertise of the different partners involved in this action and was aimed at developing a set of tools and a specific methodology to be used by the teachers when teaching cybersecurity and cyber-safety to their high-school students. The main goals of the carried study were two-fold: (1) to identify the high-school students awareness about cybersecurity and confidence in their self-protection when facing risk associated with the use of digital services and (2) to find the most appropriate format of instrument for delivering cybersecurity education. The survey was built on the EU Survey platform in English and launched online in December 2020. Starting from January 2021, it was translated into some EU official languages such as German, Spanish, French, Italian, and Greek and disseminated on social media, included in the project and European Commission newsletters, and promoted in specialized high school networks.

The survey was designed to provide an initial collection of information about the high-school student's awareness regarding cybersecurity risk and to get an indication from the high-school students about the most desired delivery method for teaching and learning cybersecurity topics. The initiative that launched the research is a continuation of the Concordia competence center activities that developed a cybersecurity educational ecosystem in EU that addressed different audiences and provided complementary learning possibilities. In the first year of activity, modular courses were offered for practitioners in the industry that answered to the needs for cybersecurity education in the industrial sector (14). The next year efforts were dedicated to high-school students and subjects dealing with cybersecurity in the high school regular program. The first step was to perform a survey within the EU members' states using the Europa platform. The initiative is still on-going and the work on the program design started in 2022. We expected, from the preliminary knowledge collected from the survey answers, that our study might help topics that should be addressed and included in the program. Similarly, it was expected the high-school students to identify as the most desired instruments for delivery of cybersecurity educational content.

2.3. The Applied Methodology

The main target audience of the survey was composed of teachers, students and their parents, and the management of high schools within Europe that were invited to interviews. Until November 2021 the Concordia team has collected input from 366 participants, out of which more than half were high-school students (63% of the sample). The contributors came from nine EU member states, mostly from Romania, Slovenia, Greece, Cyprus, Italy, Spain, Germany, Netherlands, and Poland. A funnel approach was applied that makes it possible to identify the current needs in terms of content and delivery methodologies by collecting structured data with an EU-wide survey, followed by interviews with a small group of people. The survey results discussed below are based on the collected data from the countries that provided sufficient number of answers.

To complement and further understand the results obtained from the survey, follow-up interviews were designed and provided. The target audiences of the interviews were high-school teachers, parents, and school management representatives. The interviewees were reached through contact established by the participating countries who contacted adult participants to retrieve their contact details and their consent for their contribution to the survey efforts, efforts that represent a first EU-based initiative in the context of the high-school program dealing with cybersecurity topics. The contact information from the participants that was shared with the research team was used to send e-mail invitations asking about the potential participants availability to participate in the interviews phase. Four parents and five teachers replied positively to the interview invitations. The nine interviews took place using online meeting platforms in June 2021. All the interviewers replied first with answers to the list of 15 interviewer's questions before the face-to-face interviews took place. The interviews were recorded with the consent of the participants and they were later transcribed anonymously by the persons that did the coding. The coding was provided by two persons. The interview was structured in three main sections as follows: information about the interview participants (5 questions), existing practices about cybersecurity programs in the children's school (7 questions) and questions on the future needs in that context (2 questions). In-depth analysis of the parents' and teachers' interviews followed as a per-questions notion and the general comments on the interviews' results are provided on the Concordia report "Teaching the Teachers", available on Concordia platform [14].

The outcomes of the survey provided by the addressed groups showed the preferred type of educational methodology to be used for a cybersecurity education at high school level—the use of videos and serious games. To meet the needs for designing courses and programs for that audience, serious games intended for learning cybersecurity topics that are freely available on the market were collected and analyzed for their technical and educational properties that could be applied as part of high-school cybersecurity courses. Three from the set of 13 games were offered to a class of high-school students in third year for an on-site evaluation.

3. Results and Findings

3.1. The Survey among EU High-School students, Teachers, and Parents

A detailed presentation of the survey can be found on the Concordia web page in the report "Teaching cybersecurity in high school—Our way to turn ideas into practice" [14,29]. In the section that follows a summary of the analysis of collected results is presented. Due to the diverse audience composed of European high school teachers, European high school students, European parents of high-school students, and European school management, the questions were customized accordingly per audience type.

The elements covered by the survey questions were:

- Demographics, membership to one of the three groups, gender (anonymized)
- Digital services used by high-school students in general
- Digital services used by high-school students in the school environment
- Devices used by high-school students in general

- Devices used by high-school students in the school environment
- Degree of confidence of high-school students during specific online activities
- Degree of awareness of high-school students regarding online risks
- Incidents experienced by high students related to online risks
- Possible subjects that could be discussed within a relevant cybersecurity course for high-school students
- Type of methods/instruments to be used while teaching cybersecurity at high school level
- Cybersecurity subjects in already existing courses.

At the beginning of the survey, each participant had to reveal which audience he/she belongs by specifying whether he/she is a high-school student, a parent of a high-school student, a high school teacher, or a high school management representative. Among the participants only in the group of parents some of the members (3% of the whole group) selected to not provide an answer to this question. Students represent 61% of the sample, teachers 22%, parents 14% and school management 3%. Since the number of school management representatives in the sample was very small, they were merged with teachers into one group, the teachers' group. In terms of gender, women dominated in each of the groups with 60–69% of the sample. Details about the sample and the processed data and the report about this project task are available on the web page of the CONCORDIA project "Teaching cybersecurity in high-school, "Our way to turn ideas into practice" [30]. The distribution of the participant origin was as follow:

One hundred percent of the participants provided information about their country of origin, 97.6% of them declared that they are based in an EU country. One hundred percent of the participants also provided information to which group they belong: high school teacher, student, school manager or parent. All questions in the survey were answered by the participants by selecting one of the possible answers offered in the survey. The countries that contributed considerable percentage of the answers were: Cyprus (12.02%,), Germany (12.84%), Greece (8.24%), Italy (11.58%), Slovenia (10.88%), Romania (23.12%) and the 21.32% were received from the rest of participating countries. EU member states that did not provide answers or where the numbers were very low, were not included in the data processing. Statistical tests were performed that confirmed the coherence of the high-school student answers collected from students with different country of origin. The answers obtained were coherent and the identified small differences between the student's answers from the participating countries were low. The confidence interval for the answer means included zeros, which indicates that the differences between the answers are not statistically significant. The means numbers of the student groups from different countries are similar. The residual plots are normal and they do not show any scattering or randomly distributed residuals. The simultaneous confidences were found to be 95%".

The first collected data were the answers to the question "Is cybersecurity taught at the survey participant's high school at all". The answers presented below in Figure 1 were not very encouraging as cybersecurity is not really part of the high school program, and in those schools where it is included, the time dedicated to topics dealing with cybersecurity is scarce.

The majority of teachers (55%) replied to the question with Yes, but with the comment that cybersecurity content is a part of computer courses with 2–3 h per month. The majority (48%) of parents replied with "I don't know" and 38% of students replied negatively. The results show that even if cybersecurity topics are part of the curriculum and are taught in high schools in other forms, students and parents are unaware of it.

The next question addressed the type of digital services used by high-school students. The results are presented in Figure 2.

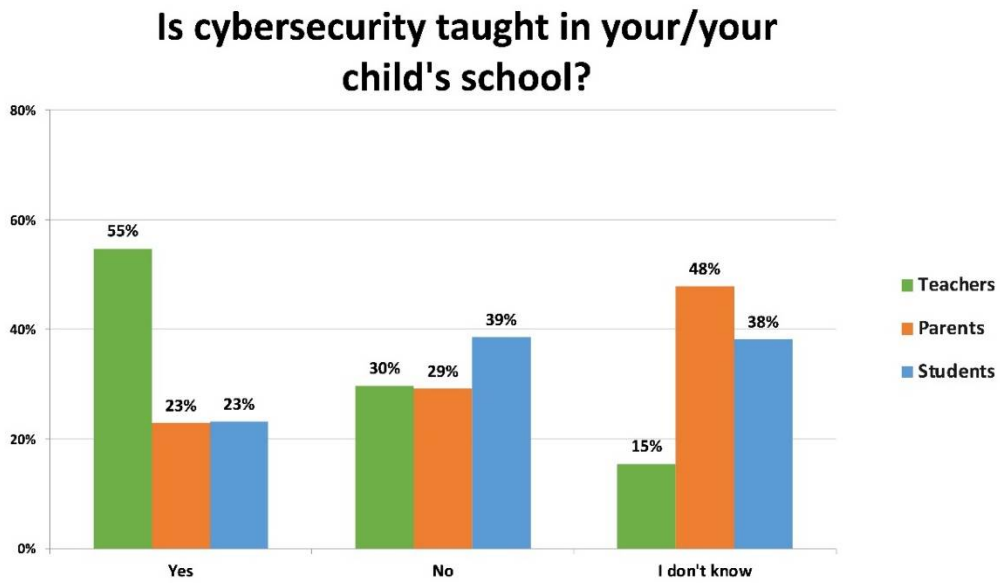

Figure 1. Answers to the question "Is the cybersecurity taught in your/school?".

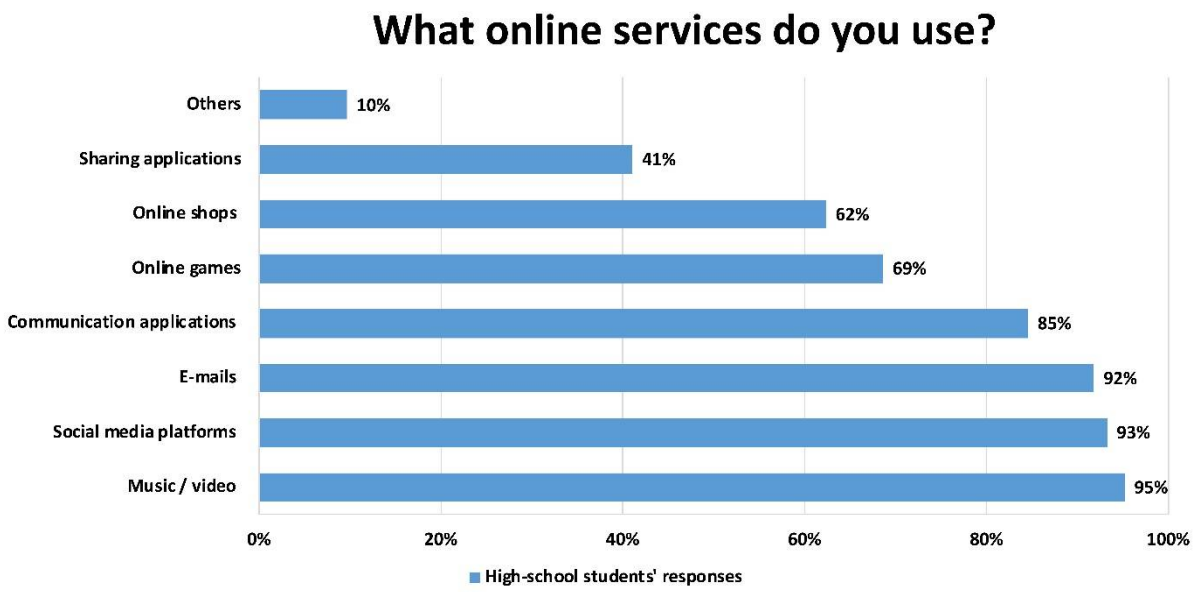

Figure 2. Answers to the question "What online services student use?".

A very high percentage (above 85%) of students mentioned music/video applications, social media platforms, e-mail applications, and communication applications as the online services they use. Other applications such as on-line shops and on-line game applications come next with percentages of 62% and 69% respectively. In last place, with a percentage of 41%, were students who mentioned sharing applications. The same questions have been given to teachers and parents with the aim to test their perception about what online services high-school students use. The teachers' responses were similar to those of the students, which show that the teachers' perception of what students use is quite accurate, especially if compared with the parents' answers where the use of online games is dominating. As the differences between the three groups were not very high, it can be concluded that the three types of applications that are most frequently used are: Music/Videos, Social Media Platforms, and Communication. Teachers mentioned e-mail applications with a lower percentage than parents and students, and online games with a higher percentage than the other two groups.

The collected answers from the three groups that took part in the survey are presented in Figure 3.

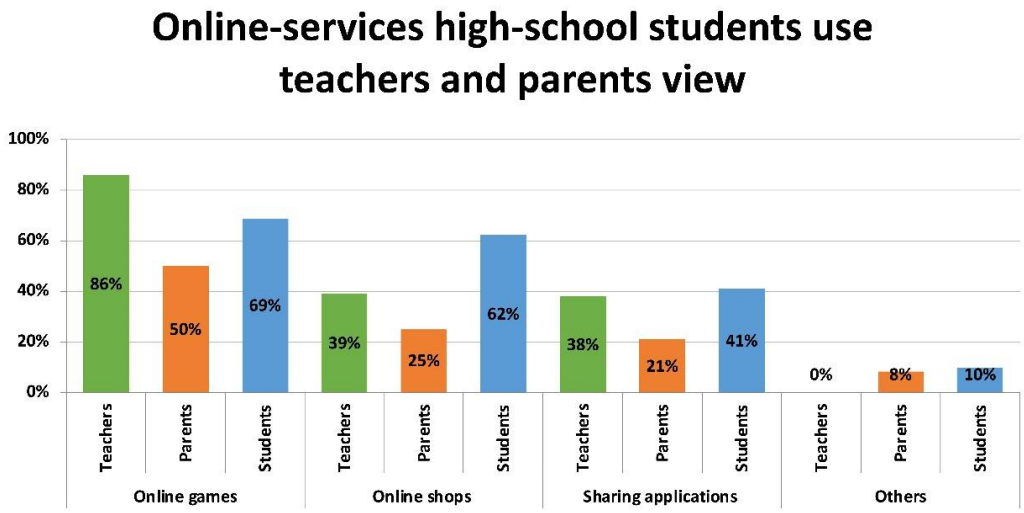

Figure 3. Teachers and parent views about use of on-line service by the high school students.

Country analysis: differences were identified between the perceptions (in average values) about the use of on-line games by high-school students in two countries only: Cyprus and Greece. The average value of on-line games utilization (by the high-school students) is 67% in Cyprus, 17% in Greece. The average value of on-line games utilization (as perceived by the high-school students' parents) is 56% in Cyprus and 58% in Greece. On the other hand, the average value of on-line games utilization (as perceived by the high-school students' teachers) is 100% in Cyprus, 95% in Greece. Other countries have values close to the general average. The perception regarding the use of communication applications (e.g., WhatsApp, Viber and the other listed in the question) by students is close to the percentage professed by the all high-school students. It is worth mentioning that in Cyprus, Greece and Romania the average percentage is between 77% and 92% where that in Slovenia is somehow lower at 60%. The perception of the teachers in comparison to the behavior of the high-school students is higher but close to the group value (e.g., in Cyprus ~80% by students ~89% by teachers, in Greece ~83% by students ~90% by teachers).The same trend is also exhibited in the perception of parents.

Regarding social media platforms (e.g., Facebook, Instagram, email), high-school students primarily use email. The highest percentage is identified in Slovenia with 100% although the average values from the other countries do not differ significantly (89%, 90%). High-school students, in their majority, use music and video services online. The use of on-line shops has an average of 50% of high-school students as credit cards are required and they usually are not owned by high-school students. Somehow, a higher percentage that does not differ much is identified in Romania (66%).

The next question addressed the devices used by high-school students. The answers are presented in Figure 4:

Figure 4 clearly shows that the devices most frequently used by students are the mobile phone and private computer. The other two groups in the survey agree on the same type of devices the high-school students most frequently use: mobile phone and private computers. Moreover, parents mentioned tablets and game consoles somehow more often than the use of these devices that was declared by students. The statistical analysis has shown that more teachers use tablets and game consoles than expected, but fewer use a personal computer. On the other hand, more high-school students use their computer than expected, but fewer use a tablet.

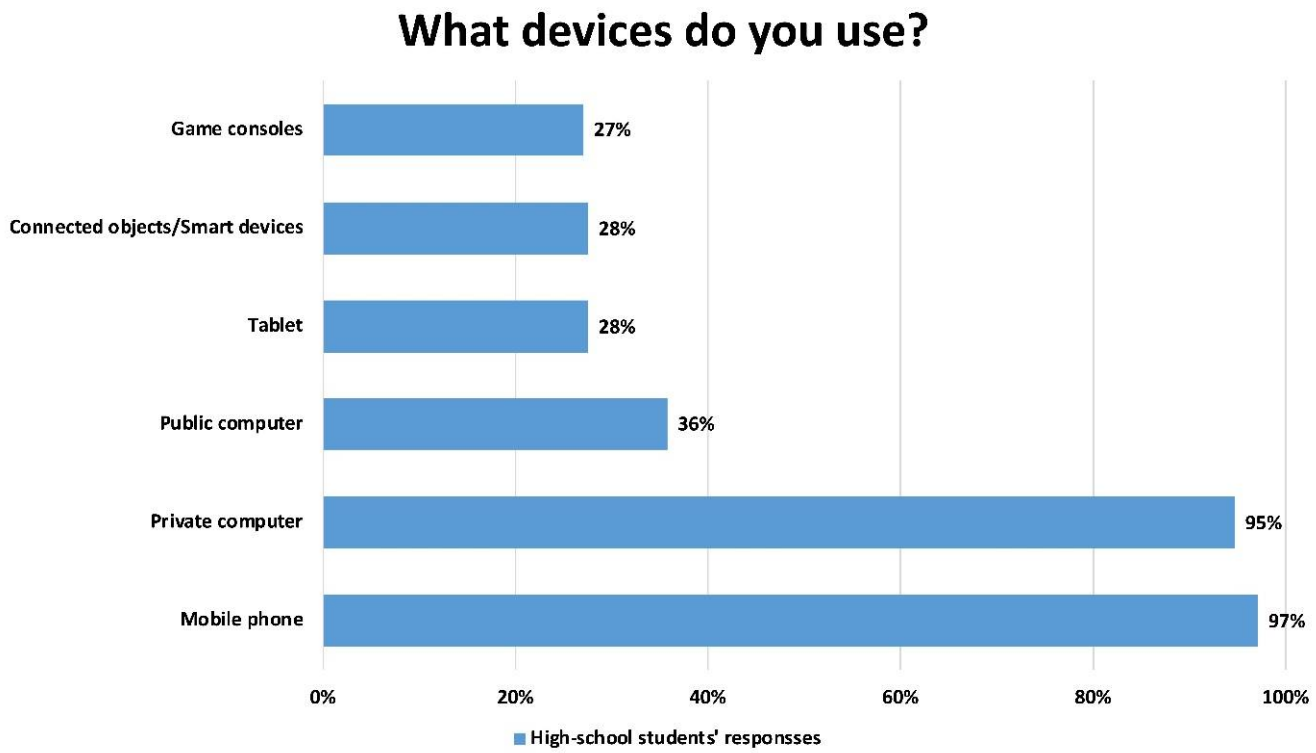

Figure 4. Answers that reveal the most popular device use by high school students.

Country analysis: There are small differences between the perceptions (in average values) regarding the use private computer by high-school students in all countries, although the difference is not substantial in all cases.

The next question asked how confident the high-school students are when they are engaged in online activities. Figure 5 provides the statistics of the collected answers:

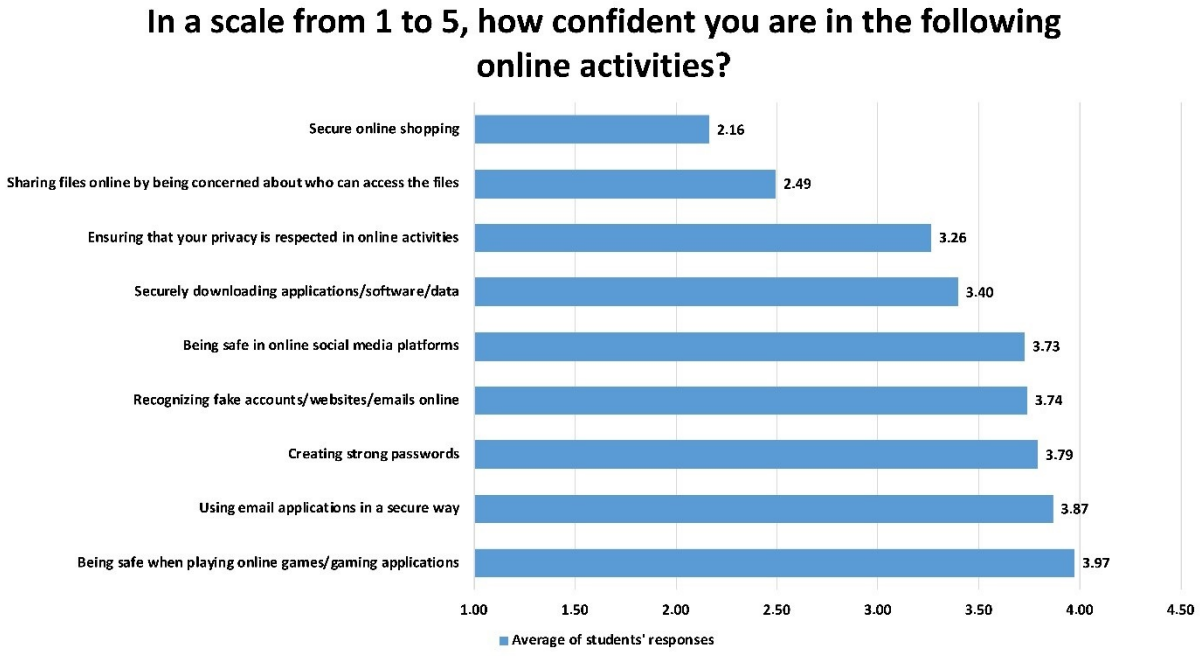

Figure 5. The student answers about their confidence in using online activities.

On Figure 5 the student confidence is displayed. Students seem to feel confident in being safe when playing, using e-mail applications in a secure way, creating strong pass-

words, recognizing fake accounts, and being safe on online social media platforms. Other than that, their responses show that they feel neutrally confident in securely downloading online content and are sure that their privacy is preserved when being online. The online activities where students mentioned they feel less confident are sharing files online and shopping securely. The answers collected from the parents show that their perception about securely downloading online is similar to the students' responses but more oriented to be neutrally confident while teachers replied with a lower confidence rate. For being safe on online social media platforms and recognizing fake online content, students seem to be confident, while their teachers and parents seem to be less optimistic, with parents replying with neutral confidence for both activities and with teachers replying with neutral confidence and little confidence, respectively. In general, it can be observed that students seem to be more optimistic about their confidence level during online activities, while their teachers seem to be less optimistic than both the students and the parents.

The average value regarding the confidence that the students claimed they have regarding the creation of strong passwords for online accounts is situated between neutral and confident (3.76 from entries in all countries). At the same time, when the teachers and parents were asked the same questions regarding the confidence of students the average values were neutral (3.01) and neutral to confident (3.65) respectively. The average value regarding the confidence that the students claimed they have regarding use of email applications in a secure way is situated between neutral and confident (3.67 from entries in all countries). At the same time, when the teachers and parents were asked the same questions regarding the confidence of students the average values were neutral to confident (3.42) respectively. The average value regarding the confidence that the students claimed they have regarding sharing files online (from a perspective of who can access the file) is situated between neutral and confident (3.35 from entries in all countries). At the same time, when the teachers and parents were asked the same questions regarding the confidence of students the average values were little confidence to neutral (2.34) and little confidence to neutral (2.81).

Country analysis: No audience (mainly parents) from all countries that provided answers believe that high-school students are confident or very confident in securely handling specific areas of online services, indicating a clear need for action (parents and teachers). In all countries the perception of high-school students about their confidence has a distinct difference from that of the of high-school teachers. No differences were noticed between the students' answers coming from different countries.

The next question addressed the awareness of the risks when students engage in online activities according to the opinions of their parents and teachers. The answers of all groups are presented in Figure 6.

Figure 6 shows that students agree and strongly agree that they are aware of the risks, that they can detect the risks, and can avoid the risks, but they are neutral in the statement that they can handle the risks. The teachers are less optimistic about the students' ability regarding the risk statements, since on average they replied that they disagree or have neutral opinions about whether the students can handle the risk. Parents seem to be more optimistic than the teachers since they agree that students are aware of the risks and are neutral about the rest of the statements. The general finding is that students can handle online risks.

Country analysis: Student answers on the risk related question do not show differences related to students' country of origin. The average values regarding the awareness of high-school students is situated between agree and strongly agree (4,38 from entries in all countries). At the same time, when the teachers and parents were asked the same questions regarding the risk awareness of students the average values were neutral (3,00) and neutral to confident (3,90) respectively. A distinct difference between the perspective regarding risk of the high-school students and the teachers of high-school students was noticed in all countries and especially in Greece.

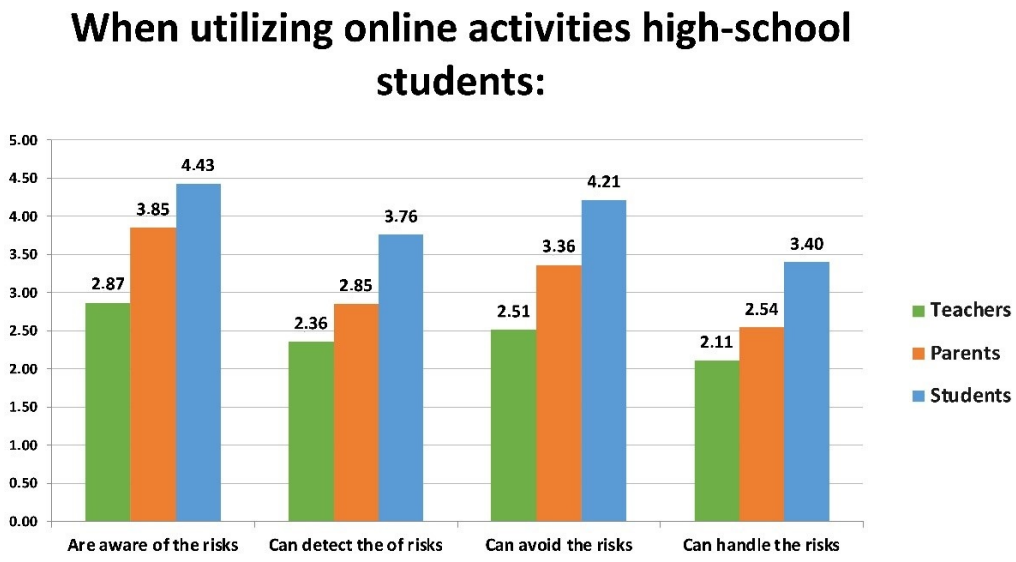

Figure 6. The level of awareness of the teachers, students and parents regarding the risk in using online activities.

The next question asked whether the students have ever experienced an online risk. The majority of high-school students replied with "Yes", while part of them replied with "No" and "I am not sure" with similar percentages being 24% and 23%, respectively. Having most of the participants mentioning that they experienced an online risk is an indication of how important it is to take action and educate the minors to ensure their online security and safety. Important information from the survey was the finding that most students did not share the online risk that they have experienced either with their parents or with their teachers. In relation to the experienced risk, an additional question addressed the playing of online games. The students were asked whether they have ever experienced any of the risks while playing games online. The answers are presented in Figure 7.

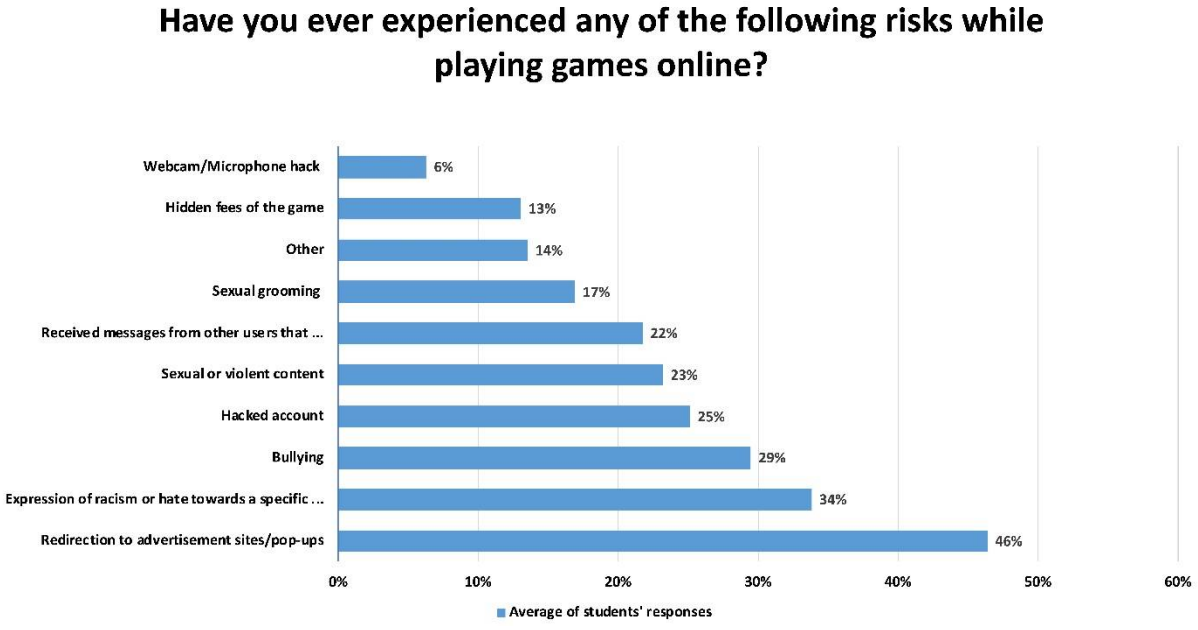

Figure 7. Experienced risk when students of high school play online games.

Figure 7 shows the experienced risk while playing games. The most common risk retrieved within the answers was 'Redirection to advertisement sites/pop-ups' with a percentage of 46%. In the second and third place are 'Expression of racism or hate' and 'Bullying' with percentages of 34% and 29% respectively. With percentages from 22% to 25%, students replied to 'Hacked Account', 'Sexual or Violent Content', and 'Received messages from other users that asked you for personal information". Microphone hack got only 6% of answers, and sexual grooming 17%.

Country analysis: Most parents and teachers from all of the participating countries replied with a no to this question. The negative answer here can mean two things, students do not experience any online risks to share or they do not share their experiences with their parents or teachers. The students' responses on whether they have experienced any online risks when playing games show that the second assumption is the valid one since the majority of students replied positively. There is a need to change that fact since it is desirable for the students to trust their teachers and parents and collaborate with them in handling cybersecurity risks.

The previous question was complemented with the question about the importance of discussing online activities and the associated risks with the teachers at school. The answers provided by the students are presented in Table 1.

Table 1. On-line topic proposed to be discussed in a school program.

On-Line Activities That Students Proposed to Be Discussed in the Class to Ensure Being Safe When Using Them	% of the Students from the Students Sample That Voted for the Particular Activity
On-line social media platforms (e.g., Facebook, Instagram, Twitter)	84%
Recognizing fake accounts/websites/emails	70%
Creating strong password for on-line accounts and devices	49%
Securely downloading applications/software/data	49%
Ensuring that the privacy of students is respected in on-line activities	45%
Using email applications in a secure way (e.g., avoiding spams)	38%
Being safe when playing on-line games	31%
Provision of secure on-line shopping	29%
Sharing files on-line (e.g., Dropbox, OneDrive) and being safe regarding who can access the files	21%

Table 1 shows the online activities for which the students voted to be discussed during cybersecurity courses, in descending order. A high percentage (85%) of students choose "Being safe in social media platforms"; this is obviously the most important topic that needs to be addressed in a cybersecurity course for high-school students. "Recognizing fake online content" comes second with a percentage of 70%. Ensuring online privacy, securely downloading online content, and creating strong passwords are on the list of the top-five online activities that students voted to be discussed in a cybersecurity course, with percentages between 45–49%.

Country analysis: A high percentage (73%) of all teachers from participating countries selected "Being safe in social media platforms" indicating that this is the most important topic that needs to be addressed in a cybersecurity course for high-school students. "Ensuring online privacy" comes second with a percentage of 67%. With percentages between 43–45%, recognizing fake content, using email applications securely, and creating strong passwords made the list of the top five online activities that teachers voted for to be discussed in a cybersecurity course. Similar to the selection teachers made, a high percentage (79%) of parents chose "Being safe in social media platforms" indicating that this is the most important topic that needs to be addressed in a cybersecurity course for high-school students. "Recognizing fake content" comes second among the parents' answers with a

percentage of 54%. With percentages between 38–52%, being safe when playing online games, using email applications securely, and ensuring online privacy are among the top-five online activities voted for by parents to be discussed in a cybersecurity course.

The last question in the survey asked about the content delivery methodology: "Which type of methods/instruments would be more effective to be used when teaching cybersecurity at high school level?" The answers are presented in Table 2.

Table 2. Selection of delivery methods for teaching cybersecurity.

Selection of Delivery Methods for Teaching Cybersecurity	% of the Students from the Student Sample That Voted for Particular Delivery Method
Interactive presentations	64%
Videos	57%
Games	56%
Websites with relevant content	40%
Live chats	28%
Fishes (paper material)	15%
Massive Open On-Line Courses (MOOCS)	14%

The most popular instrument with a percentage of 64% is 'Interactive presentations'. Second and third are 'Videos' and 'Games/Platforms' with percentages of 57% and 56% respectively. It was an important message that, for teaching cybersecurity courses, most teachers and parents select the same delivery methods and in the same descending order as high-school students, although with a slightly lower percentage of the sample. The most popular instruments were 'Videos' and games. The student answers were very coherent; they did not differ in relation to the country origin. The chi square values are: *p*-value 0.13829137 and the statistics 3.9567849.

Country analysis: The results obtained from the teachers of the participating countries differ. For example, in Cyprus the two most preferred methods/instruments that participants believed would be most effective while teaching cybersecurity to high-school students are interactive presentations and live chats, whereas the preferred methods among the teachers in Greece are videos and games/platforms, in Romania videos and interactive presentations and in Slovenia websites and games/platforms. On the other hand, the picture is clearer regarding the least preferred methods/instruments for teaching cybersecurity to high-school students which are MOOCs (Cyprus and Slovenia), Fishes (paper materials) (Greece, Romania) and live chats (Greece, Romania and Slovenia). Other countries did not provide significant results.

The survey results and the statistics showed that the high-school students' responses are very coherent in all participating countries in three aspects: the use of the digital devices (mobile phone and computer), the high level of confidence in protecting themselves regarding cybersecurity risk and the instruments they like for teaching and learning cybersecurity: videos and games. The parents and teachers have expressed more diversified answers especially in case of teaching delivery instruments. The interviews with these two groups were expected to provide more clarification for their stand points.

3.2. The Interviews

The interviews with parents revealed more details about how cybersecurity is taught in their children's high schools. Despite the indicated low/medium level of awareness about cybersecurity topics, parents revealed that the practices applied in the schools attended by their children were diverse. In some places the topics related to cybersecurity are part of the curriculum, in some places they are taught without a fixed schedule by the schoolteacher outside the curriculum or just offered in special courses that are organized occasionally, and in some places they are not taught at all. It was also pointed out that

important topics regarding cybersecurity were not sufficiently taught at the schools because they were embedded in other courses. The parents suggested that these topics become an obligatory part of the high-school curriculum. They also proposed for the lessons from the selected topics to be elaborated weekly in at least one to two hours as part of the regular courses. Regarding the delivery methods, their opinion was that they have to be efficient by giving real facts, accompanied with tailored campaigns about awareness, especially regarding the contents in social media. They also suggested that they could be led by influencers or other guests. Another suggestion was to use serious games with active participation from students and simulating real-life situations with potential dangers as a regular teaching method. Hands-on tasks or sessions with an interactive platform enriched with training exercises and real examples in a controlled environment were another desired delivery method.

The interviews with teachers were carried out with similar questions to those in the survey but also some more specific content was addressed. Regarding the time they spent on cybersecurity topics, the interviews revealed that teachers usually have just a few hours per year dedicated to cybersecurity in specific classes, but some teachers spent more time on teaching these topics outside the curriculum. Regarding the topics they think were very relevant, they listed the following: cyberbullying, spam, phishing, viruses, strong passwords, data encryption and data safety, safe data transfer, protection of personal data, sexual grooming, fake accounts in social networks, and cyber privacy. Regarding the delivery methods, they listed the following methods as more effective: videos, class discussion, doing group research together, sharing personal or friends' experiences/stories, learning by doing, peer tutoring, interactive seminars where older students teach younger students, documentaries about sexual grooming, and theatre games where students are role playing. They also provided information about possible activities outside the regular curriculum that can be offered by invited experts and from specialized organizations such as the police, telecommunication companies, psychologists, safe internet day campaigns, presentations by school IT specialists, thematic weeks with relevant topics, and gaming competitions. The teachers gave positive answers to the question "Are the students very interested in cybersecurity topics?" However, their interviews ended with this final comment: "The level of activity of a school also depends on the principal of the school, but new programs and courses enriched with modern delivery instruments are very welcomed and needed".

4. Introducing Serious Games in Cybersecurity Education for High-School Students

4.1. Assessment of the Selected Cybersecurity Games

The findings of the Concordia team survey have shown that one of the most desired delivery methods for teaching selected by all involved audiences were serious or educational games. Serious games aim at providing and engaging and in this way motivate and educate the players [30]. They are both engaging and interactive due to the in-built learning design. With their highly immersive nature where a student can learn for a longer time in a relaxing environment, the games contribute to the bridging of the gap between teachers and students. They also help students develop the relevant skills. According to some authors [31], serious games promote the strengthening of the student curriculum through the development of key professional skills for sustainability [30]. In the same study, they reported that this type of active educational methodology ensures that the training enables the acquiring of the necessary knowledge that contributes to a sustainable development. The recognition of these findings has led to the designing of many serious games that address different areas of sustainability focused on climate change and related changes in the economic, political, social, environmental areas and technologies. Among the most addressed are information communication technologies. However, when looking at the abundance of offered serious games [32], one can come to the conclusion that the field of cybersecurity is somehow neglected by the game designers. Most of these games were developed within military institutions dealing with education and are not suitable to be used in the non-military society for general education. The new demand for a skilled

population in all EU countries has contributed to a change that is about to happen in the area of serious cybersecurity games, as it has been found that cybersecurity education seems especially well-suited to educational delivery methods that use environments for teaching that are the same as where cyber-attacks happen—in networks and computer applications. Another useful property of these tools is the applicable interactivity in the training process that leads the learner to take decisions about his/her behavior when she/he uses digital services [33,34]. It is very indicative that the survey among high-school students, parents and teachers showed that they have selected videos and serious games as the most desired vehicle for learning and training. Currently, games have been developed to be used in education and are available on the market, however not all of them are designed with very clear educational goals and target audiences. Taking this in account, a search for cybersecurity games on the web was performed and the freely available games were selected for further analysis. The games were selected according to their properties and popularity. The technical properties as well as the game content and the audience addressed were used as a guide for selecting the games from different sources available on the internet [35] and from the ten best security games that were proposed by the blog owners of web site [36]. The parameters for categorizing the games used in these sources [37] were compared with the properties used in the evaluation that followed after the selection, and most of these were found to be already included in the games' applied evaluation methodology. The set of selected games consists of includes the following:

- Targeted Attack
- Cybersecurity Lab
- ThreatGen: Red Vs. Blue
- CyberSIEGE
- Permission Impossible
- Data Center Attack
- CS4G Netism
- Firewall administration: The Game
- Cyber Awareness Challenge
- Keep Tradition Secure
- Zero Threat
- Cyber Threat Game
- Risko!

The evaluation analysis that followed after playing all games from the set showed that the games differ in their purpose, educational goal and in their technical properties. Some of them are made for a single player and some of them involve multiplayer strategies where teams of players compete against each other, head-to-head in order to take control or maintain control of a computer network or the computer itself. Most of the games are dedicated to players from the industrial environment but some of them are applicable for training learners from the wide public audience interested to learn more in order to raise the awareness about cybersecurity threats and to learn how to protect themselves. Special attention during the game evaluation was paid to their learnability and suitability for training or educating high-school students.

The whole selected set together with the properties, source, potential audience, and availability is presented in Appendix A.

The technical properties considered in the evaluation of the games are:

- Platform: Web-based or stand-alone.
- Operating System: PC or Linux or macOS.
- Distribution: Whether the game is freeware or needs a license for playing, is it on CD-ROM or run only by downloading.
- Application/client: The year of publishing—when the game became available for public use.
- Label: The name of the team that has developed the game.
- Is it a single or multi-user game: Whether the game is played by one or several players

- Dimension: Whether the game is presented in a 2D or 3D environment.
- Group: To which main group the game belongs (according to TULIP classification): Table-top or Networking, or Firewall, or General topics.
- Genre: Whether the »game-flow« has been played in a form of Roleplay-Character, as an Adventure, as a team Competition or as a game of Playing cards.

The e-learning properties and the learnability of the game considered in the evaluation are the following:

- Competitive or Non-Competitive: Whether the game is based on taking decisions by the player of the game or by the other »outside« participants (for example: the bots participating in the game).
- The Degree of complexity: The complexity of the computer model that is underlying the game scenario.
- The Feedback system: Whether the results are shown with the scores achieved during the progress of the game based on the collected experience points collected by the learner, or are they presented as the upgrade level in the game summary reports prepared for the learner.
- Deterministic or stochastic: Whether the game is stochastic by nature or prepared as a deterministic game that has a fixed rule scenario.
- Background knowledge: The kind of background knowledge required for playing the game (basic knowledge of ICT, intermediate, advanced or a pure beginner knowledge level (general public).
- Learnability and the learning outcome: Whether the game shows a clear learning goal in order to be classified as educational or a serious game. It should include a known and recognized learning process (e.g., based on some known educational theories) and the »game-playing« should assure that the educational goal can be achieved when the player finishes the game with a positive outcome or a certain level of scores.
- Clear goal: The game has to clearly show the purpose of cybersecurity gaming. It should be clear whether the game is dedicated to training cybersecurity skills, just learning a single cybersecurity topic or solely building the awareness of cybersecurity.
- Target audience: The target audience of the game can vary depending on the level of cybersecurity education the game is designed for. Cybersecurity games have different target audiences, such as: General (Public), High-school students, IT Professionals (employees, educators, mentors, teachers, trainees); their usage depends on the level of background knowledge each audience should have.

4.2. High-School Student Class and the Playing of Serious Games about Cybersecurity

The evaluation process that was aimed at finding games that can be applied in the context of high school education resulted in a smaller set of three games that promised be useful in the teaching of high-school students about some fundamental cybersecurity topics. The games selected were: Target Attack, Permission Impossible and Keep Tradition Secure. Each of the selected games is briefly described below:

(a) Target Attack

This game is a type of immersive simulation game created by Trend Micro Ltd. It can be used to help students acquire system cybersecurity skills and to prepare the student to make the right decisions for avoiding the devastating consequences of a major data breach. The game is based on the principle of adventures where the player takes a fantasy role in an episodic adventure story. More than any other genre, adventure games depend heavily upon the underlying story and lead the single player to acquire experience in dealing with modern digital technology. The player steps into someone else's shoes and is exposed to a challenge of a data breach. The actions to be performed by the player are supported by an internal security team helping the player to solve the tasks correctly.

(b) Permission Impossible

Permission Impossible is an online game designed to teach students without any background in cybersecurity to understand and learn about firewalls. The aim of the game is to introduce the firewall terminology to students and present the concepts of how computer protection can be provided with a firewall application.

The player of the game learns by passing different levels of knowledge. The initial levels are supported with detailed instructions, while the higher levels require to apply more knowledge to solve the tasks. The learner gets an avatar called Roboto who guides him/her through the game by providing hints how she/he can complete the tasks and achieve the required level.

(c) Keep Tradition Secure

Keep Tradition Secure is an online game that can be played anywhere using a laptop, desktop, tablet or a mobile device. The game is designed as a set of tasks that help the hero of the game known as "Good_Bull" to track a hacker named "Bad_Bull". The game resembles a quiz with questions about cybersecurity. If the questions are answered correctly, the player gets a clue intentionally left by the hacker and can continue the game. The game is a learning tool for acquiring basic cybersecurity knowledge. It helps the students to become aware of everyday threats when browsing the internet.

The three games were offered to a third-year class of 25 students of the high-school Poljane in Ljubljana to be played for a month. The students' trial process was carried out the One-group Pretest-Posttest approach [38]. More than one half of those involved in the trial sent answers to the trial questions. The involved two experts and the class teacher evaluated the understanding of the game topics and the satisfaction with playing games by evaluating the responses to the following questions:

(a) Which game property did you like most? Possible answers: Playfulness, Good scenario, Possibility to learn.
(b) Did you find the games to be fun? Possible answers: Yes, So-so, No.
(c) Did you manage to learn something by playing the games? With possible answers; Yes, A little, No.

The Likert scale associated with the answers was rated as follows:

2.51 to 3.00: indicates a high satisfaction level, or clear positive answer like "yes".
1.51 to 2.50: indicates a moderate satisfaction level, or a "so-so" answer.
1.00 to 1.50: indicates a low satisfaction level.

The results have shown that the satisfaction of playing games was high, as it was assessed with an average score of 2.74. A similar level of satisfaction was shown for playfulness, as the students liked this most with an average score of 2.93. Among the games offered, the game that was found to offer most fun was the "Target attack" game, compared to the two others that received less positive scores. The last question had the intention to reveal how well the students are able to understand the subject taught by the game scenario. The positive answer received an average score of 2.11 which indicates that the cybersecurity topics of the games were understood by the students. These results are in line with the main current trends of e-learning where serious games are becoming part of the sustainable environment [38].

5. Discussion and Limitations of the Study

The sample size of collected answers was not as large as expected because the audience from nine European countries was initially invited to participate, and this can be understood as an indication that this target group cannot be easily reached through the usual means of communication and information channels. Even though there is a confirmed concern for cybersecurity and cyber safety among parents and teachers, they do not seem to be prepared to pre-emptively look into a search for relevant content. More coordinated actions with campaigns and e-mails through school networks should continue with the support and permission of governmental agencies (e.g., ministry of education or associations of

high schools). The number of people that accepted to give an interview was not as high as expected, which shows the participants' reluctance to further engage with an online survey. Yet we can claim that the analysis of the survey data provided general observations on the existing status of cybersecurity topics taught in high schools in the EU. The interviews reveal various diversities, not only in the level of cybersecurity/cyber safety in education, but also in the way it is addressed among different institutes. Some schools have already included courses in their curriculum while others have not. That some schools have not specified a reason for not offering courses, such as a lack of knowledge/experts/materials to teach such courses, gives the impression that there is also a lack of interest in school principals to deal with the matter. External courses (outside school hours) were found in some cases, but these are independent efforts (e.g., support from the Munich police) and not a common practice across the EU. Another aspect not equally treated within schools is handling incidents such as, for example, online harassment. Answers indicate that there is not always a protocol to follow the incidents, and in the institutes that have these protocols, the actions to be followed in case of an incident differ very much. Finally, participants gave diverse answers when asked about their opinion about what should be changed in the existing teaching, courses, and curriculums. There were answers stating that considerable changes are needed, but also an answer was received that changes were not needed as she/he strongly supports their school's current curriculum. Despite the many differences between the participants and their high schools, the current status suggests further actions need to be taken for promoting cybersecurity/cyber safety in high school education as the various topics pointed out by the participants' answers seem to converge. All participants seem to agree on the importance of cybersecurity in education and the need to form a long-term mission instead of providing some additional courses in a curriculum. Furthermore, they all agree that there is a need for more interactive courses (hands-on experience) which would simulate actual circumstances and demonstrate how to properly react to them. Another point of agreement was that all parents and/or teachers believe that students overestimate their skills and ability when it comes to protect themselves from online risks. At the same time students feel that they are more capable to address online risks than their parents/teachers think they are. This can be attributed to the generation gap, however it can be argued that in many cases younger people are more familiar with technology and they can in fact be capable of better understanding these risks as they are more familiar with the digital technology. The study of the selected games among high-school students was somewhat restricted as it was limited to one class and to only three games and by the time offered for playing the games. The students' reaction was generally positive, they liked very much the simplest game which resembles a quiz, but the one designed as adventure received the most positive replies from the students. The trial shows that the process for making the decision about which of the games on the web should be selected and used in the teaching process [39] is very complex. The evaluation of game properties can help, but the most important aspect that must be considered along with the learnability of the selected topic is how the students will react and whether the game answers the needs for training special cybersecurity skills that should be part of the new curriculum [40,41].

If we summarize the findings, the following points can be highlighted. Firstly, there is a high interest in cybersecurity among teachers, parents, and students but there is a gap between education and the community of cybersecurity experts, and the high school audience is somehow neglected. This gap affects the communication between these two groups and consequently the ability to design and apply context-specific solutions. The second point is that participants describe very diverse practices in the cybersecurity education across European institutes, but they all seem to agree on the necessary steps that must be made to provide sustainable education in this important area. An indicative example is that all participants agree on the need for interactive courses on cybersecurity to be introduced into the education, with the support of games with relevant cybersecurity topics that need to be introduced in the education [36]. The designing of such tools is very demanding.

The selection from the available range of serious games to be used in the teaching process requires much more efforts from specialized fields, i.e., technical, pedagogical and social expertise, if compared with other educational materials. Another aspect that has been identified has to do with the lack of coordinated actions and initiatives across the EU to support schools and their students as an active part of the EU population that needs to acquire cybersecurity skills. Currently, cybersecurity education is either provided as an additional topic inside computer science courses or through independent activities organized by external providers and agencies [29]. Furthermore, the lack of central coordination and well-defined protocols and strategies also affects the ability to identify and respond to incidents and assure the smooth development of a sustainable digitalized society.

6. Conclusions

The presented study about teaching cybersecurity in high school should be understood as an input to help build sustainable education in the area of cybersecurity. The study has revealed the most important topics that need to be introduced into the high-school educational program. They are: "Being safe in online social platforms, "Recognizing fake accounts", "Ensuring privacy in online activities", "Creating strong passwords", and "Using email applications in a secure way". The topics "Secure online shopping", "Sharing files online" and "Securely downloading" that were not selected as important topics by the students were added to the list of topics to be taught due to parents' requests. The most appropriate format for the materials that need to be developed was identified as videos, interactive presentations, and serious games. During the interviews, teachers and parents insisted on having interactive instruments in which real facts are presented to the students. However, these tools require a specific assessment of properties, educational goals, and suitability before being introduced into the educational process [40]. The areas not sufficiently covered by existing programs were identified as well as the missing protocols about how to detect and handle online risks when they occur. The limited time spent in relevant courses and seminars and the lack of the students' experiences with real threats makes it difficult to adequately cover the detecting and handling of online risks. Making the students confident regarding the detection and protection from cybersecurity risks is another task that needs to be undertaken in line with the envisaged education. Increasing the time and the frequency of cybersecurity courses and presenting the threats in a more practical than theoretical way can help improve the effectiveness of existing programs. Additionally, during the interviews, it became evident that cyber-safety topics, such as cyberbullying, sexual grooming, privacy, etc. are more discussed than cybersecurity topics such as cyber-attacks, spam, and viruses. This is an indicator that existing programs focus more on the spreading of the awareness on cyber-safety topics than real cybersecurity stuff.

The studies presented in the paper have also shown that the cybersecurity education requires innovative approaches for building the skills for sustainability development by introducing cyber ranges and serious games that have proven to be more effective in developing the required cyber-related skills. These approaches enable the required interactivity in the training process that leads the learner to take decisions in a safe environment which is similar to real life; this accelerates the learning process. However, the designing and the selection of appropriate serious games is a long and demanding process.

Author Contributions: Conceptualization, B.J.B.; Investigation, A.J.B.; Methodology, B.J.B.; Resources, A.J.B.; Supervision, B.J.B.; Visualization, A.J.B.; Writing—original draft, A.J.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Slovenian Research Agency under the contract P2-0037. Both authors were funded under the same contract. The participation of the authors in the CONCORDIA center activities (the survey) were not funded as the author organization acted in the consortium as no funded partner.

Institutional Review Board Statement: "The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Ethics Committee) of H2020 CONCORDIA

Competence center for cybersecurity" for studies involving humans. The document was provided to mdpi editorial office.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the interviews/they answered to.

Data Availability Statement: Data used in the study (the survey results) can be found in reference [14].

Acknowledgments: The survey study was carried out within the EU H2020 Concordia's competence center for cybersecurity where the authors are members and contributed to the survey results. The study part dedicated to cybersecurity serious games is their original contribution. The support of all Concordia team members for task T3.3 is highly appreciated.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Evaluation of available serious games for cybersecurity education.

	Target Attack	Cybersecurity Lab	ThreatGen: Red vs. Blue	CyberSIEGE	Permission Impossible	Data Center Attack	CS4G Netism	Firewall Administration	Cyber Awarness Challenge	Keep Tradition Secure	Zero Threat	Cyber Threat Game	Risko!
TECHNICAL PROPERTIES													
Game type/platform	Web Based	Web Based	Stand Alone/PC/ Linux/macOS	Stand Alone/PC/	Web Based	Web Based	Web Based	Web Based	Stand Alone/PC/MAC	Web based	Web Based	Web Based	Desk/card game
Distribution	Free To Play	Free	Free	Free	Free	Free	Free	Free	For Academic users	Free	Free	Free	Free
Year of publishing	2015	2020	2019	2004	2018	2017	2017	2017	2019	2018	2017	2016	
Label	Trend Micro	NOVA labs	Derezzed	Naval postgraduate School	Sibylle Sehl	Trend Micro	Atwater and Bocovich	GitHub	LivingSecurity	Texas A&M	GRC	UTSA	University of Southampton
Single/Multi user	Single	Single	Multiplayer	Single	Single	Single	Single	Single	Single	Single	Single	Multiplayer	Multiplayer
Dimension 2D/3D	2D	2D	2D	3D	2D	2D	2D	2D	2D	2D	2D	2D	2D
Group/Security Topic	General	General	Captrure The Flag	Network	Firewall	Network	Network	Firewall	General	General	Network	General	Genral
GENRE: quiz, roleplay	Roleplay	Adventure	Competition	Roleplay									Playing Cards, Roleplay
E-LEARNING PROPERTIES/LEARNABILITY													
Competitiv/Non Competitive	Non Competitive	Non Competitive	Competitive	Competitive	Non competitive	Non competititive	Non Competititve	Competititve	Competititve	Non Competitive	Non Competititve	Competitive	Competitive
Degree of complexity	Low	Medium	Low	Low	Medium	Medium	Low	High	Low	Low	Medium	Medium	Medium
Feedback system/awards and raitings	Score points	Level Score/progress bar	Score points	Level upgrade	Level upgrade	Level upgrade	Score points	Score points	Level upgrade	Level upgrade	Level upgrade	Level upgrade	Score points
Deterministic/stohastic	Stohastic	Stohastic	Deterministic	Stohastic	Stohastic	Deterministic	Stohastic	Deterministic	Deterministic	Deterministic	Deterministic	Deterministic	Deterministi
Background knowledge	Basic	Intermedia	Basic	Advanced	Intermedia	Intermedia	Advanced	Advanced	Basic	Basic	Intermedia	Intermedia	Intermedia
Learning outcome	Data protection/to combat a simulated attack, at an executive level	Crack passwords, craft code/computer coding, logical reason-ing/critical thinking	Understanding about cybersecurity controls, technology, methods, and strategies	Indentifying the vunerabil-ity/firewall configura-tions/VPNs/link encryptors/	How to make a Firewall config-uration/how to build a firewall rule set to enable incoming and outgoing packet traffic	Critical think-ing/Strategy/ decision making	Network attacks/IP Spoof-ing/stealing packets/Basic DoS/Smurf Attack/Man in the middle/	Firewall commands for the iptables application	To capture an unnamed hacker/learning about attacks such as social engineering, email phishing, viruses/malware, identity theft	Learning about cybersecurity basics/stay safe on the internet	Defend the data/Firewall Configuration/	Cybersecurity terminology, reinforce un-derstandings of a network infrastruc-ture, learn about the relationships between cyber-attacks and defence counter measures	To increase cybersecurity awareness for people with a non-technical background/ spoofing/phishing
Clear Goal/	TRAINING:	EDUCATION:	TRAINING—	TRAINING	TRAINING—IT	TRAINING—	AWARENESS/	EDUCATION	TRAINING/—	AWARENESS/	TRAINING—	EDUCATION/	AWARENESS/
Target Audience	PROFESSIONALS	LEARNERS	PROFESSIONALS	LEARNERS	PROFESSIONALS	LEARNERS	GENERAL PUBLIC	GENERAL PUBLIC	Professionals/employees	GENERAL PUBLIC	PROFESSIONALS	LEARNERS	GENERAL PUBLIC

References

1. EU. Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU, Cybersecurity for the EU. 2017. Available online: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450 (accessed on 25 March 2021).
2. Caulkins, B.; Marlowe, T.; Reardon, A.C. Cybersecurity Skills to Address Today's Threats. In *Advances in Human Factors in Cybersecurity, Proceedings of the International Conference on Applied Human Factors and Ergonomics, Orlando, FL, USA, 21–25 July 2018*; Ahram, T., Nicholson, D., Eds.; Advances in Intelligent Systems and Computing; Springer: Cham, Switzerland, 2018; pp. 782–788. Available online: https://link.springer.com/chapter/10.1007/978-3-319-94782-2_18 (accessed on 12 December 2020).
3. Blažič, B.J. Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Educ. Inf. Technol.* **2022**, *27*, 3011–3036. [CrossRef]
4. Zhang, T.; Shaikh, Z.A.; Yumashev, A.V.; Chłąd, M. Applied Model of E-Learning in the Framework of Education for Sustainable Development. *Sustainability* **2020**, *12*, 6420. [CrossRef]
5. Castro, M.P.; Zermeño, M.G.G. Challenge Based Learning: Innovative Pedagogy for Sustainability through e-Learning in Higher Education. *Sustainability* **2020**, *12*, 4063. [CrossRef]
6. Oliveira, P.M.; Gomes de Souza, K.; Reis, C.; Souza, W.M. Gamification in E-Learning and Sustainability: A Theoretical Framework. *Sustainability* **2021**, *13*, 11945. [CrossRef]
7. Sayaf, A.M.; Alamri, M.M.; Alqahtani, M.A.; Al-Rahmi, W.M. Information and Communications Technology Used in Higher Education: An Empirical Study on Digital Learning as Sustainability. *Sustainability* **2021**, *13*, 7074. [CrossRef]
8. Alcalá del Olmo, M.J.; Gutiérrez Sánchez, S.J. El desarrollo sostenible como reto pedagógico de la universidad del siglo XXI. *Anduli* **2020**, *19*, 59–80. [CrossRef]
9. Cybersec4Europe Competence Center, Enablers and Components, Report. Available online: https://cybersec4europe.eu/wp-content/uploads/2022/02/D3.13-Updated-version-of-enablers-and-components-v3.0-submitted.pd (accessed on 30 July 2021).
10. Michael, P. Closing the Information Security Skill Gap. 2018. Available online: https://www.michaelpage.co.uk/our-expertise/technology/closing-information-security-skills-gap (accessed on 30 September 2019).
11. Blair, T. Investigating the Cybersecurity Skills Gap, Utica College, ProQuest Dissertations Publishing. 2017. Available online: https://search.proquest.com/docview/1989786177?pq-origsite=gscholar&fromopenview=true (accessed on 8 March 2020).
12. ECSO. Gaps in European Cyber Education and Professional Training. 2019. Available online: https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf (accessed on 5 December 2019).
13. Hentea, M.; Dhillon, H.S.; Dhillon, M. Towards changes in information security education. *J. Inf. Technol.* **2006**, *5*, 221–233. Available online: https://www.learntechlib.org/p/111542/ (accessed on 15 September 2020).
14. CONCORDIA Cybersecurity Competence Center. Available online: https://www.concordia-h2020.eu/concordia-reports (accessed on 15 March 2021).
15. McGettrick, A. Towards effective cybersecurity education. *IEEE Secur. Priv.* **2013**, *11*, 66–68. [CrossRef]
16. Malan, J.; Lale-Demoz, E.; Rampton, J. Identifying the Role of Further and Higher Education in Cyber Security Skills Development. Skills: Concepts, Measurement and Policy, Approaches. *J. Econ. Surv.* **2018**, *32*, 985–992.
17. Svabensky, V.; Vykopal, J.; Celeda, P. What are cybersecurity education papers about: A systematic literature review of SIGCSE and ITiCSE conferences. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE), Portland, OR, USA, 11–14 March 2020; Available online: https://dl.acm.org/doi/abs/10.1145/3328778.3366816?casa_token=F4ZnMuFM6uQAAAAA:fCvpD2-bBdWmpikS367OiQ1Y6B2VIvM9ONHwmVkMAecA3UpAaesNLOuGcCUeGASb06258a9FgDn (accessed on 7 November 2021).
18. Dragoni, N.; Lafuente, A.L.; Massacci, F.; Schlichtkrull, A. Are We Preparing Students to Build Security in? A Survey of European Cybersecurity in Higher Education Programs. *IEEE Secur. Priv.* **2021**, *19*, 81–88. [CrossRef]
19. Saharinen, K.; Backlund, J.; Nevala, J. Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework. In Proceedings of the ICETC'20, 12th International Conference on Education Technology and Computers, London, UK, 23–26 October 2020; pp. 172–176. [CrossRef]
20. Wen, B. Towards a cyber security curriculum model for undergraduate business schools: A survey of AACSB-accreditated institution in United States. *J. Educ. Bus.* **2017**, *92*, 1–8.
21. UK Cabinet Office. The UK Cybersecurity Strategy Protecting and Promoting the UK in the Digital World. 2011. Available online: https://connections-qj.org/article/uk-cyber-security-strategy-protecting-and-promoting-uk-digitalworld (accessed on 2 September 2019).
22. ENISA. Cybersecurity Skills Development in the EU. 2020. Available online: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/ (accessed on 7 April 2020).
23. AUG. Australian Government, Update, Innovation, Growth & Prosperity. 2017. Available online: https://cybersecuritystrategy.pmc.gov.au/assets (accessed on 5 September 2019).
24. Ackerman, A. Too Few Cybersecurity Professionals Is a Gigantic Problem for. 2019. Available online: https://techcrunch.com/2019/01/27/too-fewcybersecurity-professionals-is-a-gigantic-problem-for-2019/ (accessed on 22 July 2019).
25. Ruiz, R. A study of the UK undergraduate computer science curriculum: A vision of cybersecurity, IEEE international conference on global security, safety and sustainability (ICGS3). In Proceedings of the 12th IEEE International Conference on Global Security, Safety and Sustainability, London, UK, 16–18 January 2019; pp. 1–8. [CrossRef]

26. Catota, F.E.; Morgan, M.G.; Sicker, D.C. Cybersecurity education in a developing nation: The Ecuadorian environment. *J. Cybersecur.* **2019**, *5*, tyz001. [CrossRef]
27. Conklin, W.A.; Cline, R.E.; Roosa, T. Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. In Proceedings of the 47th Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 6–9 January 2014. [CrossRef]
28. Garanina, Z.G.; Balyaev, S.I.; Ionova, M.S. The Role of Self-Attitude in the Personal and Professional Development of High School Students. *Educ. Sci. J.* **2019**, *21*, 82–96. [CrossRef]
29. Hassan, L.; Dias, A.; Hamari, J. How motivational feedback increases user's benefits and continued use: A study on gamification, quantified-self and social networking. *Int. J. Inf. Manag.* **2019**, *46*, 151–162. [CrossRef]
30. CONCORDIA, Teaching the Teachers Report. Available online: https://www.concordia-h2020.eu/news/cybersecurity-in-high-school-survey-from-concordia-available-now-in-7-languages/ (accessed on 18 October 2021).
31. Liarakou, G.; Sakka, E.; Gavrilakis, C.; Tsolakidis, K. Evaluation of serious games as a tool for education for sustainable development. *Eur. J. Open Distance E-Learn.* **2021**, *46*, 391–411. Available online: https://old.eurodl.org/?p=special&sp=articles&inum=4&article=546 (accessed on 17 February 2022).
32. Miguel, N.P.; Lage, J.C.; Galindez, A.M. Assessment of the development of professional skills in university students: Sustainability and serious games. *Sustainability* **2020**, *12*, 1014. [CrossRef]
33. Halinger, P.; Wang, R.; Chatpinyakoop, C.; Nguyen, V.T. A bibliometric review of research on simulation and serious games used in educating for sustainability. *J. Clean. Prod.* **2020**, *256*, 120358. [CrossRef]
34. Stanitsas, M.; Kirytopoulos, K.; Vareilles, E. Facilitating sustainability transition through serious games: A systematic literature review. *J. Clean. Prod.* **2019**, *208*, 924–936. [CrossRef]
35. Winston, A.H., Jr.; Mesafint, F.; Xiachong, Y.; Jinhua, Z.; Sajad, S.J. A survey of serious games for cybersecurity education and training. In Proceedings of the KSU Conference on Cybersecurity Education, Research and Practice, Kennesaw, GA, USA, 5–6 June 2020; Available online: https://digitalcommons.kennesaw.edu/ccerp/2020/Research/ (accessed on 5 November 2021).
36. The Selection of Best Cybersecurity Games. 2021. Available online: https://www.livingsecurity.com/blog/10-best-games-cyber-security (accessed on 22 October 2021).
37. Coenrad, M.; Pellicone, A.; Ketelhut, D.J.; Cukier, M.; Plane, J.; Weintrop, D. Experiencing Cybersecurity One game at time: A sytematic review of Cybersecurity Digital games. *J. Simul. Gaming* **2020**, *51*, 586–611. [CrossRef]
38. Jerman Blažič, A.; Džonova Jerman Blažič, B. Exploring and upgrading the educational business-game taxonomy. *J. Educ. Comput. Res.* **2015**, *52*, 303–340. [CrossRef]
39. Jerman Blažič, A.; Cigoj, P.; Tanja, A.R.H.; Jerman-Blažič, B. Applicability of the learnability attributes in serious game design: The case of digital forensic game design. In Proceedings of the 11th International Technology, Education and Development Conference, Valencia, Spain, 6–8 March 2017; Gómez Chova, L., López Martínez, A., Candel Torres, I., Eds.; PC IASTED Academy: Calgary, AB, Canada, 2017; pp. 8425–8434. [CrossRef]
40. Doney, I. Research into effective gamification features to inform e-learning design. *Res. Learn. Technol.* **2019**, *27*. [CrossRef]
41. Bernik, A.; Vusić, D.; Milković, M. Evaluation of gender differences based on knowledge adaptation in the field of gamification and computer science. *Int. J. Emerg. Technol. Learn.* **2019**, *14*, 220–228. [CrossRef]