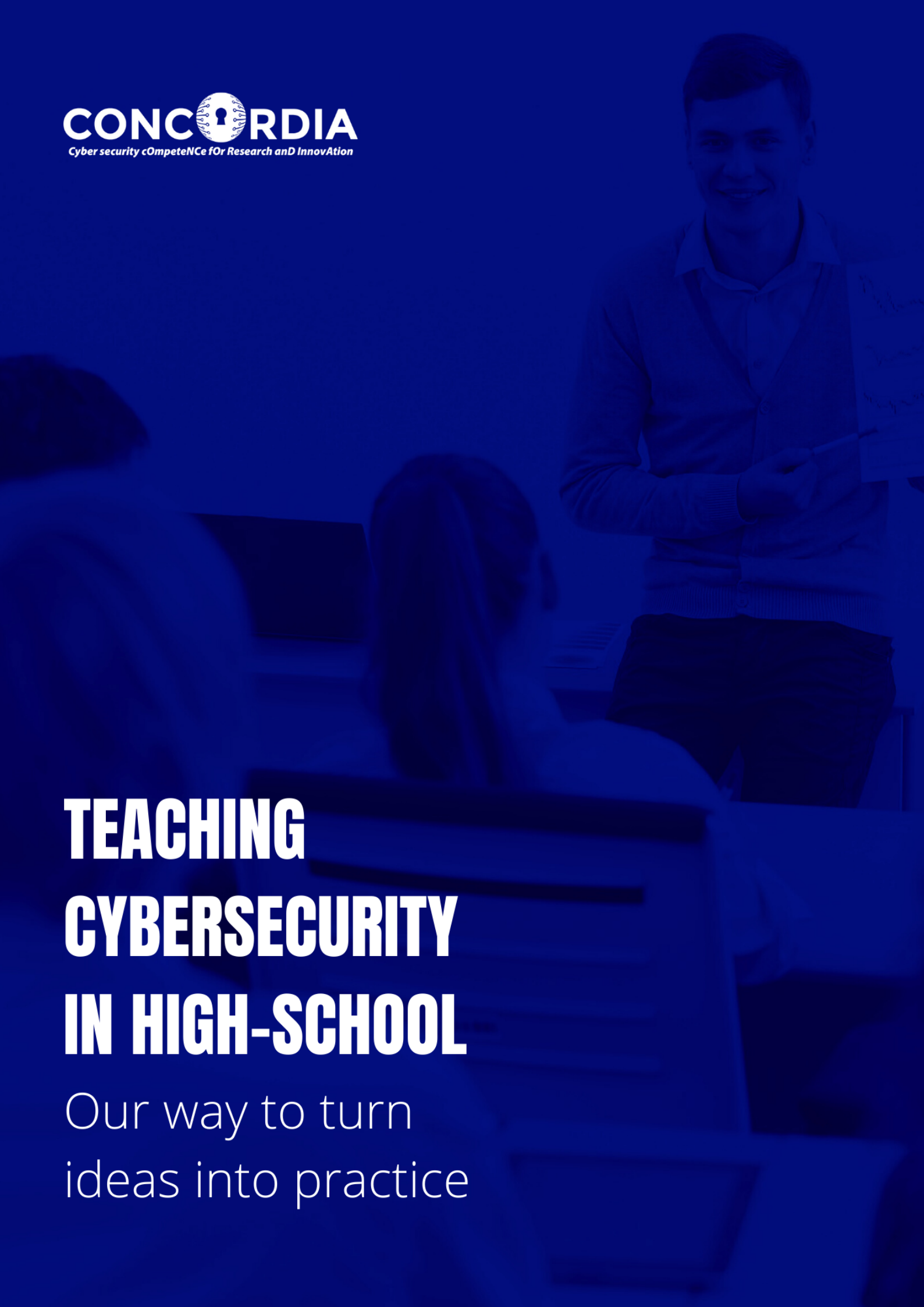
CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion



TEACHING CYBERSECURITY IN HIGH-SCHOOL

Our way to turn ideas into practice

CONTENTS

1. Introduction

Cybersecurity is a major concern for our societies at large. Children start using the internet at an early age and more than 90% of young Europeans are online. Using the internet brings a lot of benefits linked to information and communication but it comes with certain risks: privacy violation, identity theft, ransomware, fraudulent usage of debit cards, etc. It is therefore of paramount importance that new generations are made aware and kept updated about the major threats, new technologies as well as appropriate individual and collective behaviors in order to reduce risks.

Teachers can play a major role in raising awareness among their pupils about Cybersecurity and in spreading and disseminating a risk-prevention culture. While they are more and more sensitive to Cybersecurity issues and have started acquiring fundamental notions in this area, there is a need for a structured approach to teach cybersecurity-related topics to young Europeans.

The Teach-the-Teachers activity subject of this report is part of the CONCORDIA[1] task T3.4 whose overall objective is to build an European Education Ecosystem for Cybersecurity. The work builds on the expertise of the different partners involved in this action and aims at developing a set of tools and a specific methodology for the use of the teachers when teaching cybersecurity and cybersafety to their high-school students.

The present paper summarizes the work performed under this action in 2021, namely the survey and associated interviews. It starts by introducing the approach on the action (chapter 2), continues by presenting the outcomes of the survey (chapter 3) and the associated interviews (chapter 4) and follows with the summary of a complementary research on serious gaming (chapter 5). The document closes with listing the main conclusions and the next steps on the action (chapter 6).

[1] *This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.*

2. The approach

In order to identify the current needs in terms of content and delivery methodologies fit for the high-school level, we decided on applying a funnel approach by starting with collecting structured data via an EU wide survey, followed by interviews with a small group of people. The identified needs are then further validated in live event before moving to the next step in the process, the design of the materials. By the end of the project, we aim at piloting the content created.

In 2020 we setup the CONCORDIA Survey - Teaching cybersecurity in high-schools aimed at collecting information from a large pool of stakeholders, namely teachers, students and their parents, and the management of the high-schools within Europe. The objective of the survey was three-fold: (1) to select the most in need topics to be covered in the materials; (2) to define the most appropriate format for the materials to be developed; (3) to identify areas not (enough) covered by existing programs. The survey was built on the EU Survey platform in English and launched online in December 2020. Starting January 2021, it was translated in some EU official languages such as German, Spanish, French, Italian, Greek and was disseminated on social media, included in the project and European Commission newsletters, and promoted in specialized networks. The results are presented in the chapter "The Survey".

After collecting initial input via the survey, we ran a series of 10 interviews with teachers and parents accepting to help us further in the process. The objective of the interviews was to refine the conclusions of the survey and get more in-depth feedback. A summary of the answers is presented in the chapter "The Interviews"

As a subsequent step to the survey and interview phases, in order to validate the findings and test the motivation of the teachers and students to some existing solutions within the consortium in view of developing them further, we will organize a webinar.

3. The Survey

The objectives of this Survey were three-fold:

***RELEVANCE**: To select the most needed topics to be covered in the materials.*

***EFFECTIVENESS**: To define the most appropriate format for the materials to be developed.*

***NOVELTY**: To identify areas not (enough) covered by existing programs.*

In order to collect relevant input, we looked into collecting input from the following audience:

- *European high-school Teachers,*
- *European high school Students*
- *European Parents of high school students European*
- *European school Management*

Since the audience of the survey is diverse, the questions have been customized accordingly per audience type. The question regarding the audience is the first one and this affects the rest of the questions pack accordingly.

Independent of the audience, the elements covered by the survey are:

- *Demographics (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' 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 of courses already existing*

The Survey has been published since December 2020 and is still active. This document has been drafted based on the information collected during the period December 2020 – September 2021.

Within this period, 342 responses were collected. From these, 339 are further processed and are included in this report. 3 responses were discarded because the respondents were located outside Europe.

3.1. Demographics of the survey

In the demographic section, we asked the participant to define if he/she is a high-school student, a parent of a high-school student, a high-school teacher, a high-school management representative. The table below shows the responses. Since the number of school management representatives in the sample is very small, for the rest of this report we merge the groups of school management representatives and teachers under one group, the teachers' group.

What are you?	***Number***	***Percentage of participants***
A high-school teacher	*75*	*22%*
A high-school student parent	*48*	*14%*
A School Management Representative	*9*	*3%*
A high-school Student	*207*	*61%*
Total participants	*339*	*100%*

Furthermore, we asked for the gender of the participants who belong under the groups of high-school teachers, school management representatives, and parents. Due to the fact that students are minors, we tried to minimize the demographic and personal data we collected from them, so we don't ask for the gender of the students. The responses in the table below show that the majority of the participants in a per group notion, but also in total are females.

Gender of Participants per group		
	Number	***Percentage***
A high-school teacher		
Female	*52*	*69%*
Male	*23*	*31%*
Prefer not to say	*0*	*0%*
A parent of a high-school student		
Female	*29*	*60%*
Male	*15*	*31%*
Prefer not to say	*4*	*8%*
A School Management Representative		
Female	*6*	*67%*
Male	*3*	*33%*
Prefer not to say	*0*	*0%*
All (teachers/school management representatives/parents)		
Female	*87*	*66%*
Male	*41*	*31%*
Prefer not to say	*4*	*3%*

3.2. Countries statistics overview

In the demographics part of the survey, the analysis is based on the country of residence of the respondent. The aim of the analysis is to find out to which extent the answers to the questions could differ based on country specificities.

The following table depicts the distribution of the responses per country and per type of respondent.

Country where the respondent is based?	Type of respondent	Total
Austria	A high-school teacher	3
	A School Management representative	1
Austria Total		**4**
Cyprus	A high-school student	9
	A high-school teacher	23
	A parent of a high-school student	9
	A School Management representative	3
Cyprus Total		**44**
Germany	A high-school teacher	1
	A parent of a high-school student	3
Germany Total		**4**
Greece	A high-school student	12
	A high-school teacher	21
	A parent of a high-school student	12
	A School Management representative	2
Greece Total		**47**
Italy	A high-school teacher	2
Italy Total		**2**
Romania	A high-school student	129
	A high-school teacher	15
	A parent of a high-school student	1
	A School Management representative	1
Romania Total		**146**
Slovenia	A high-school student	55
	A high-school teacher	8
	A parent of a high-school student	22
	A School Management representative	2
Slovenia Total		**87**
Spain	A high-school student	2
	A high-school teacher	2
	A parent of a high-school student	1
Spain Total		**5**
Grand Total		**339**

Distribution of responses per country and per type of respondent

As shown by the table information contained in Table 1., some countries have a very small number of respondents. The information shown in the rest of the document is only limited to countries and types of respondents with at least five (5) entries. (e.g. Information from respondents based in Austria is completely omitted, since there are only four (4) responses in total and Information from parents of a high-school student or from school management representative based in Slovenia are omitted since there is only one (1) response per type of respondent.

3.3. Survey Results: general and country-based analysis

Q1. Which are the Digital Services used by high-school students in general?

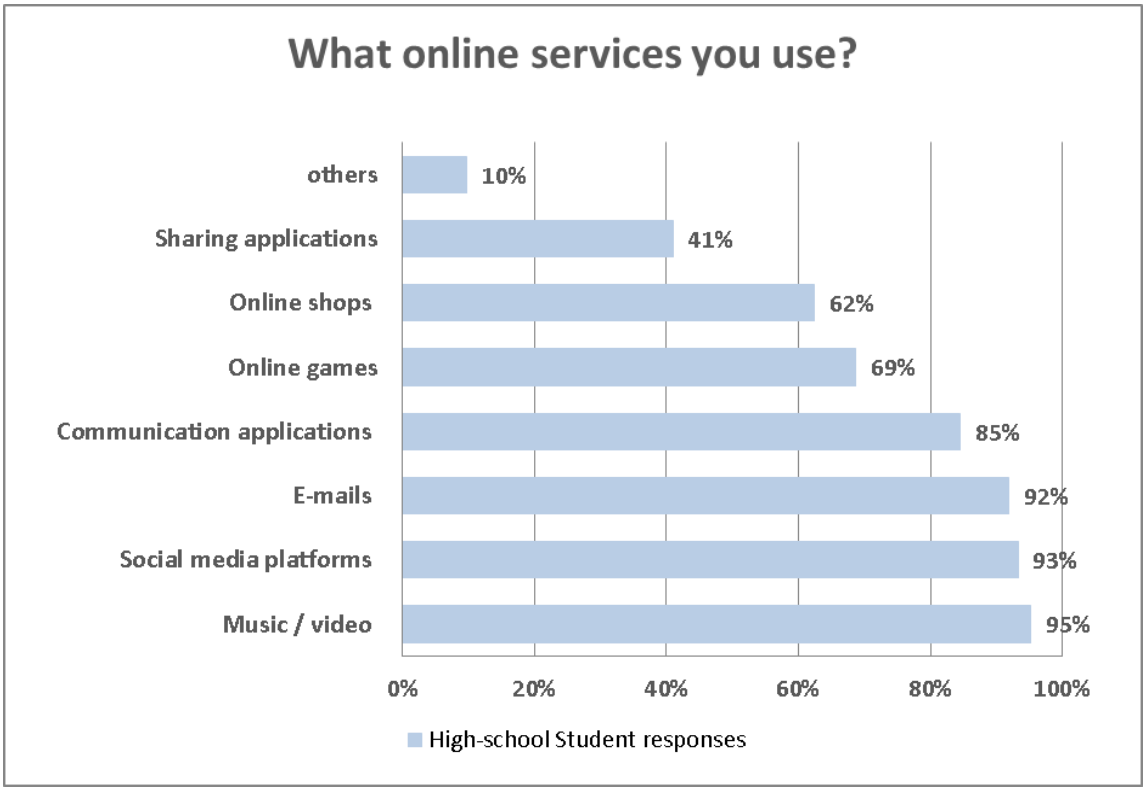
Type of Question: multiple choice

Possible answers:

- *Online games (e.g. Minecraft, Fortnite, Animal Crossing, WoW, LoL, etc.)*
- *Communication applications (e.g. WhatsApp, Viber, QQ, WeChat, etc.)*
- *Social media platforms (e.g. Facebook, Instagram, Messenger, etc.)*
- *Sharing applications (e.g. Dropbox, WeTransfer, etc.)*
- *E-mails (e.g. Gmail, Hotmail, etc.)*
- *Music / video (e.g. YouTube, Spotify, TikTok, etc.)*
- *Online shops (e.g. eBay, Amazon, etc.)*
- *Others*

Q1. General analysis

High-school Students' Responses:

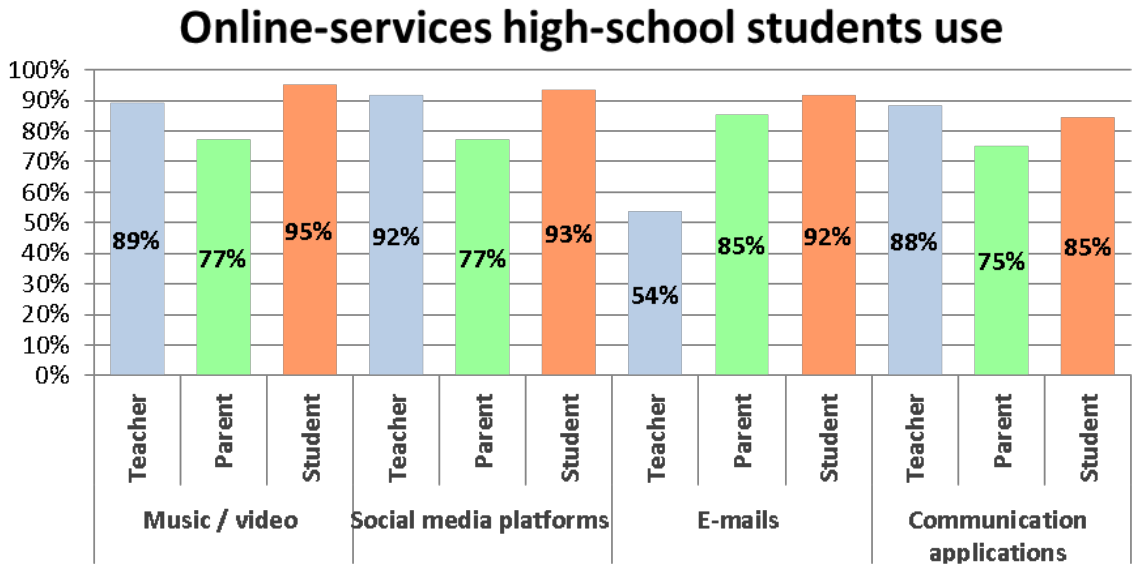


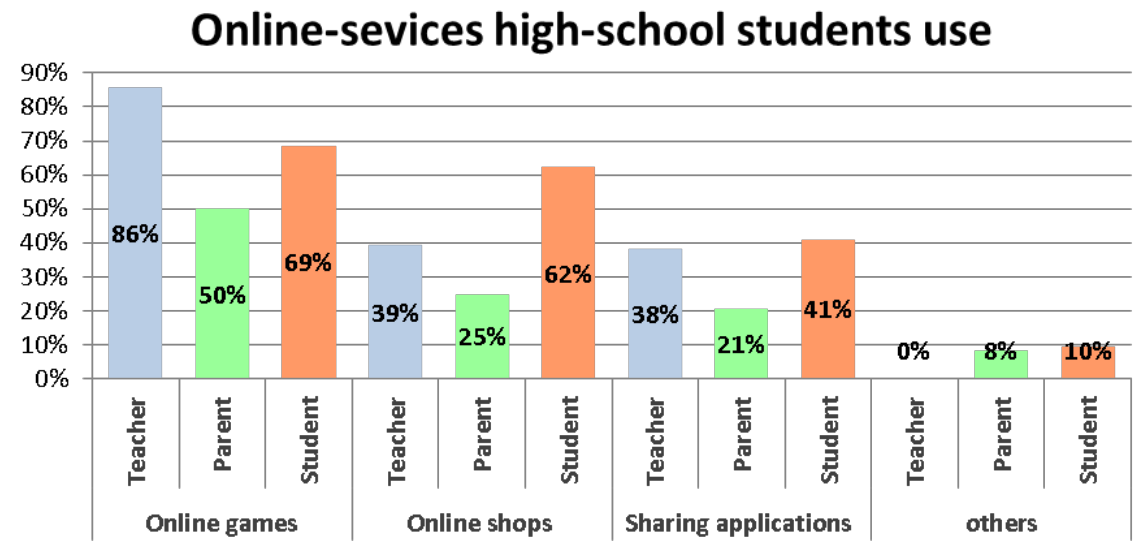
Comments:

A very high percentage (above 85%) of students mentioned Music/video applications, Social media platforms, E-mail applications, and Communication applications as online services they use. Other applications such as Online shops and Online games applications come next with percentages of 62% and 69% accordingly. In the last place with a percentage of 41%, students mentioned Sharing applications.

Teachers and Parents responses

We asked the same question to teachers and parents to understand their perception of what online-services high-school students use. The plots below depict the responses per group of participants for each online-service type.



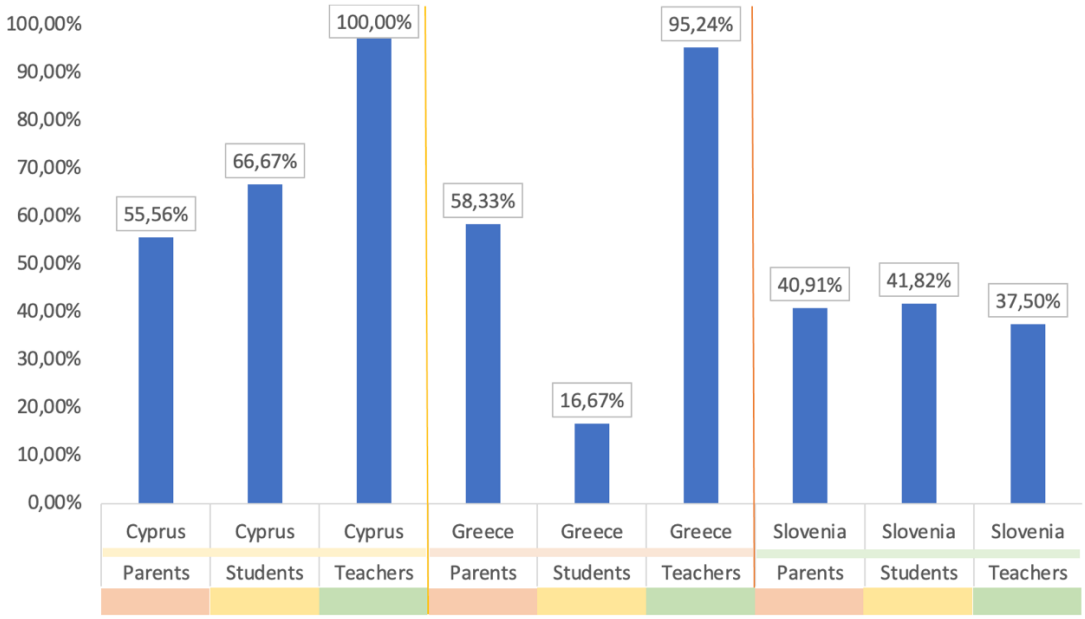


Comments:

The teachers' responses are similar to the students', which shows that teachers' perception of what students' use is more accurate than the one of the parents. The three groups mostly agree on the three types of applications Music/Videos, Social Media Platforms, and Communication. Teachers mentioned the E-mail Applications with a lower percentage than parents and students and Online Games with a higher percentage than the rest.

Q1. Country analysis

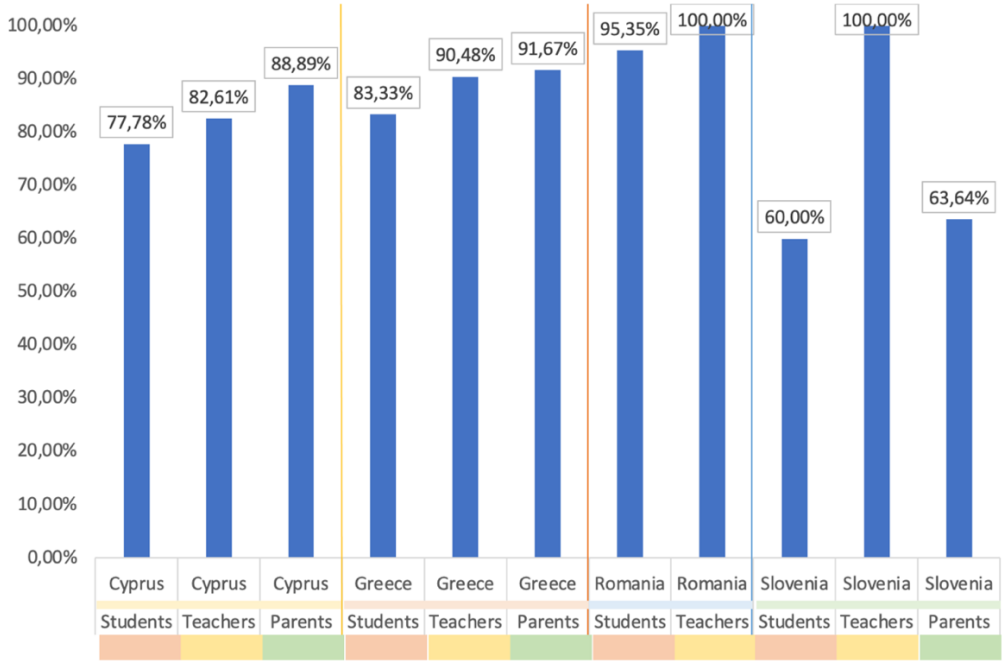
Online games (e.g. Minecraft, Fortnite, Animal Crossing, WoW, LoL, etc.)



Comments:

The above diagram shows that there is a difference between the perception (in average values) regarding the use of online games by high-school students in Cyprus and Greece. This difference of perception is not observed in the case of Slovenia. The average value of Online games utilization (by the high school students) is almost 67% in Cyprus, 17% in Greece and 42% in Slovenia. The average value of Online games utilization (as perceived by the high school students' parents) is almost 56% in Cyprus, 58% in Greece and 41% in Slovenia. On the other hand, the average value of Online games utilization (as perceived by the high school students' teachers) is 100% in Cyprus, 95% in Greece and almost 38% in Slovenia

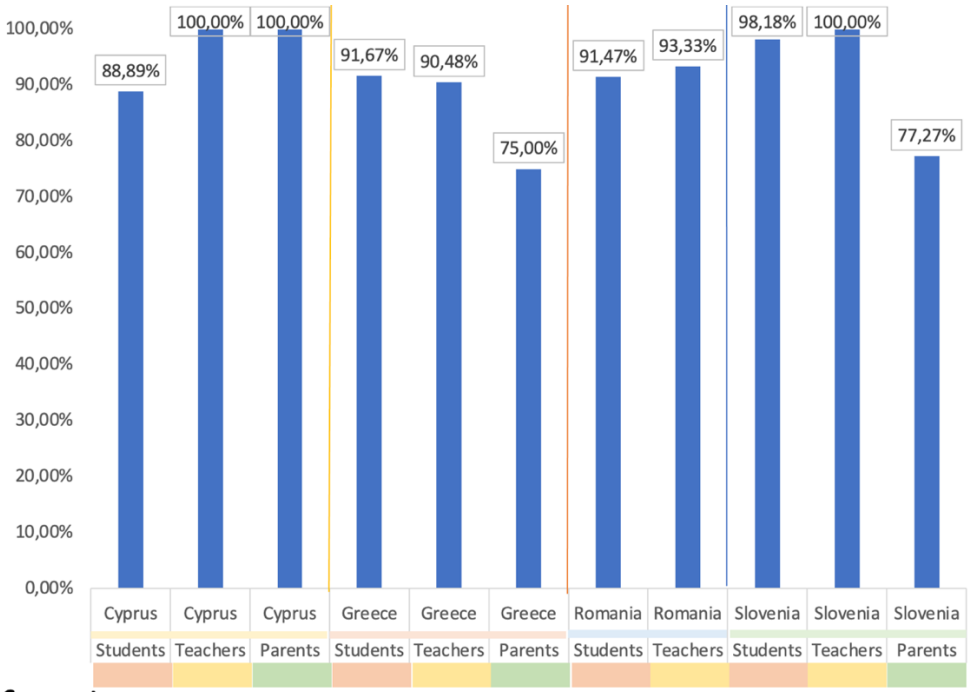
Communication applications (e.g. WhatsApp, Viber, QQ, WeChat, etc.)



Comments:

The above diagram shows that there is a difference between the perception (in average values) regarding the use of communication applications by high-school students in Slovenia from the teachers standpoint. In all other cases, the perception regarding the use of communication applications by students is close to the percentage professed by the high-school students. It is worth to mention that in Cyprus, Greece and Romania the average percentage is between 77% and 92% where as the one in Slovenia is 60 %. Also, there the perception of the teachers in comparison to the professed behavior of the high-school students is always higher (e.g. in Cyprus ~80% by students ~89% by teachers, in Greece ~83% by students ~90% by teachers etc), with the greatest difference in Slovenia where the difference in average values is 40%). The same trend is also exhibited in the perception of parents.

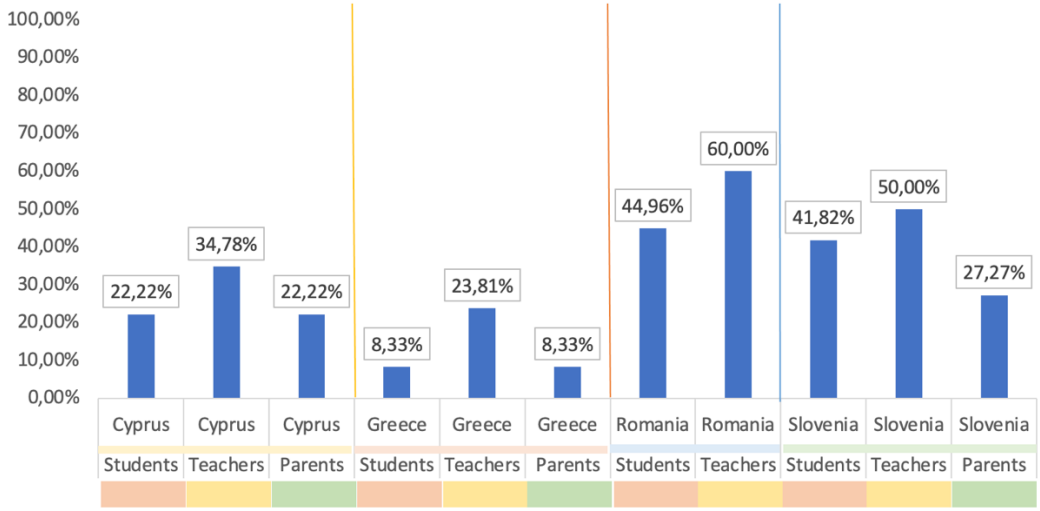
Social media platforms (e.g. Facebook, Instagram, Messenger, etc.)



Comments:

The above diagram shows that there is a difference between the perception (in average values) regarding the use of Social media platforms by high-school students in all countries although the difference is not substantial in all countries. In any case and for all countries, Social media platforms rank within the first two digital services used by high-school students.

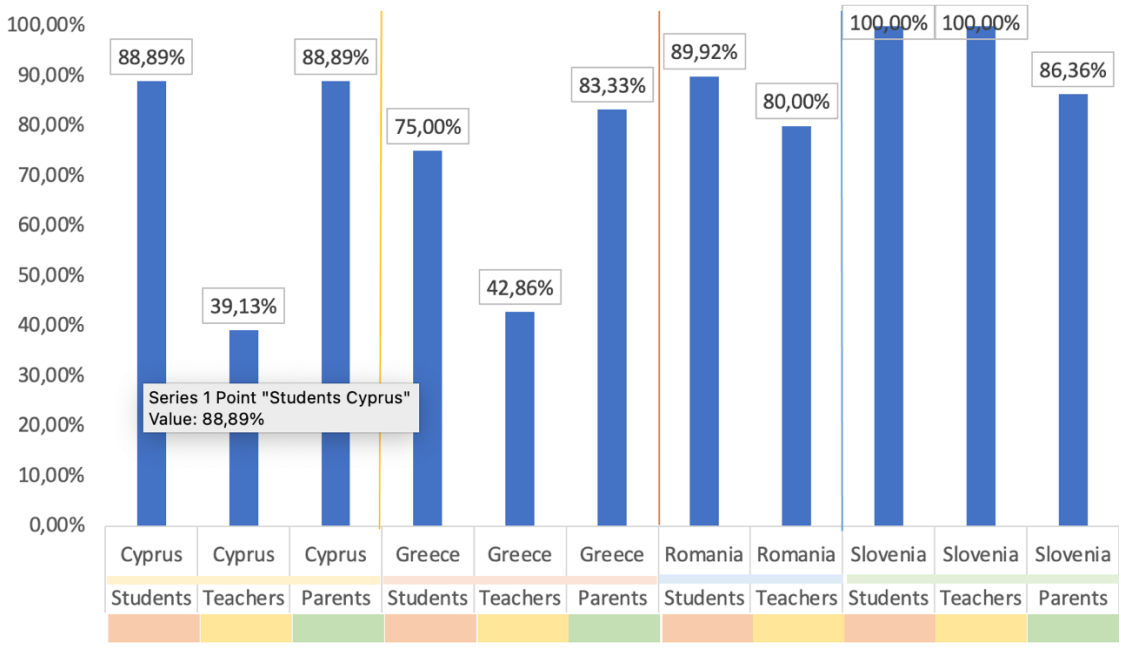
Sharing applications (e.g. Dropbox, WeTransfer, etc.)



Comments:

The above diagram shows that high school students do not, in their majority use Sharing applications. The highest percentage is identified in Romania (almost 45%). Also, in this case there is a difference between the perception of teachers regarding the use of such digital services by the high-school students.

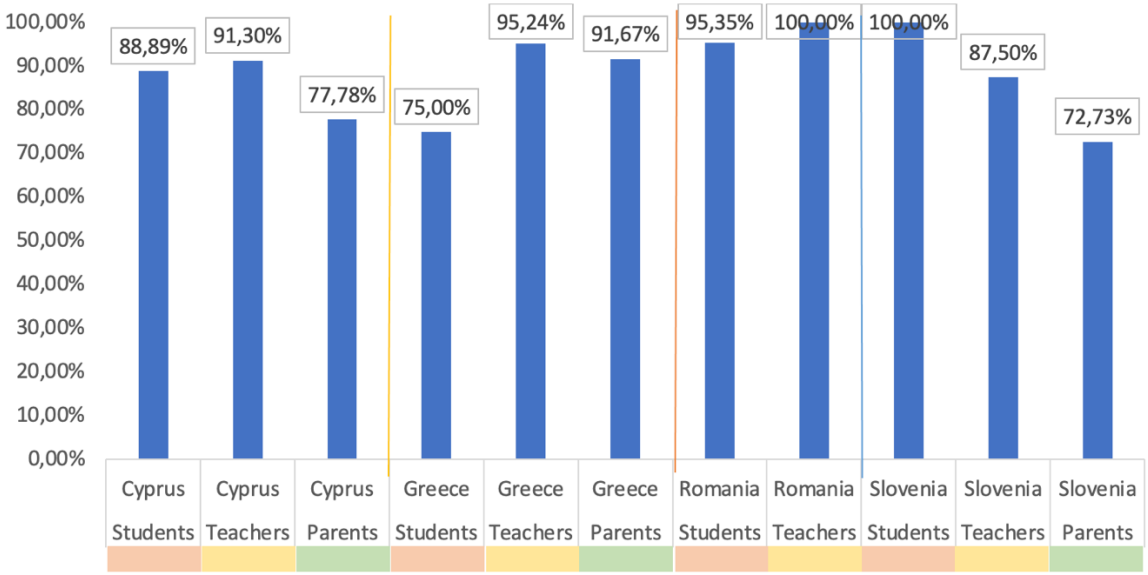
E-mails (e.g. Gmail, Hotmail, etc.)



Comments:

The above diagram shows that high school students, in their majority use Emails. The highest percentage is identified in Slovenia – 100% although the average values from the other countries do not differ significantly (89%, 75%, 90%). Also, in this case there is a difference between the perception of teachers regarding the use of such digital services by the high-school students, especially in Cyprus and Greece.

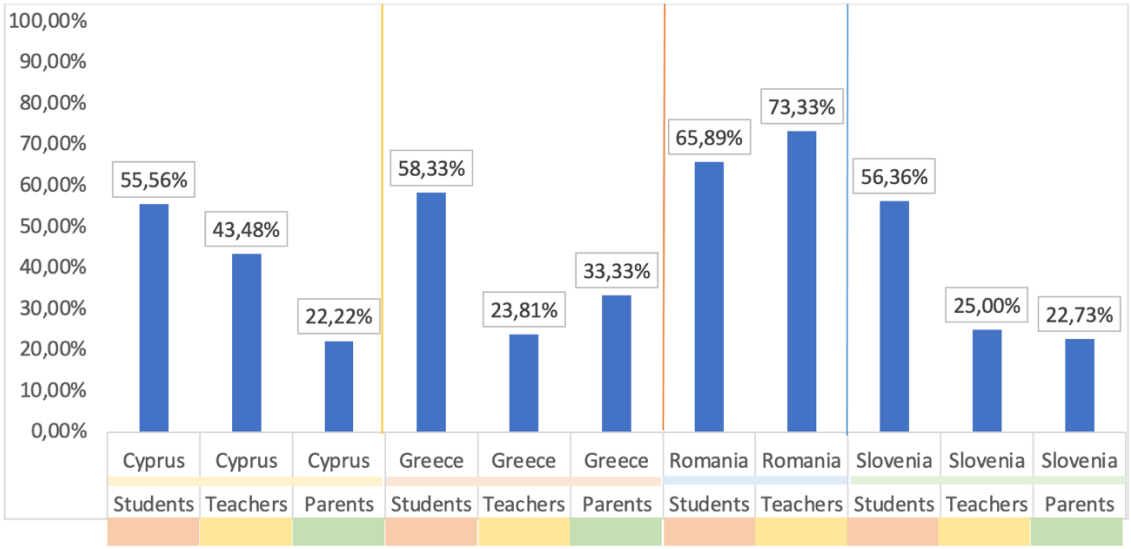
Music / video (e.g. YouTube, Spotify, TikTok, etc.)



Comments:

The above diagram shows that high school students, in their majority, use Music and video services online. The highest percentage is identified in Slovenia – 100% although the average values from the other countries do not differ significantly (89%, 75%, 95%). In this case there is a difference of about 20% between the perception of teachers regarding the use of such digital services by the high-school students and the actual values professed by students.

Online shops (e.g. eBay, Amazon, etc.)



Comments:

The above diagram shows that on average 50% of high school students use Online Shops. The highest percentage is identified in Romania (almost 66%). Also, in this case there is a difference between the perception of parents regarding the use of such digital services by the high-school

students. At this point, it should be noted that the use of such services requires credit cards, which is not usually something that a high school student is expected to have or use without the parent's consent. This is why this difference in perception between students and parents is interesting and should be further investigated.

Q2. Which devices are used by high-school students in general?

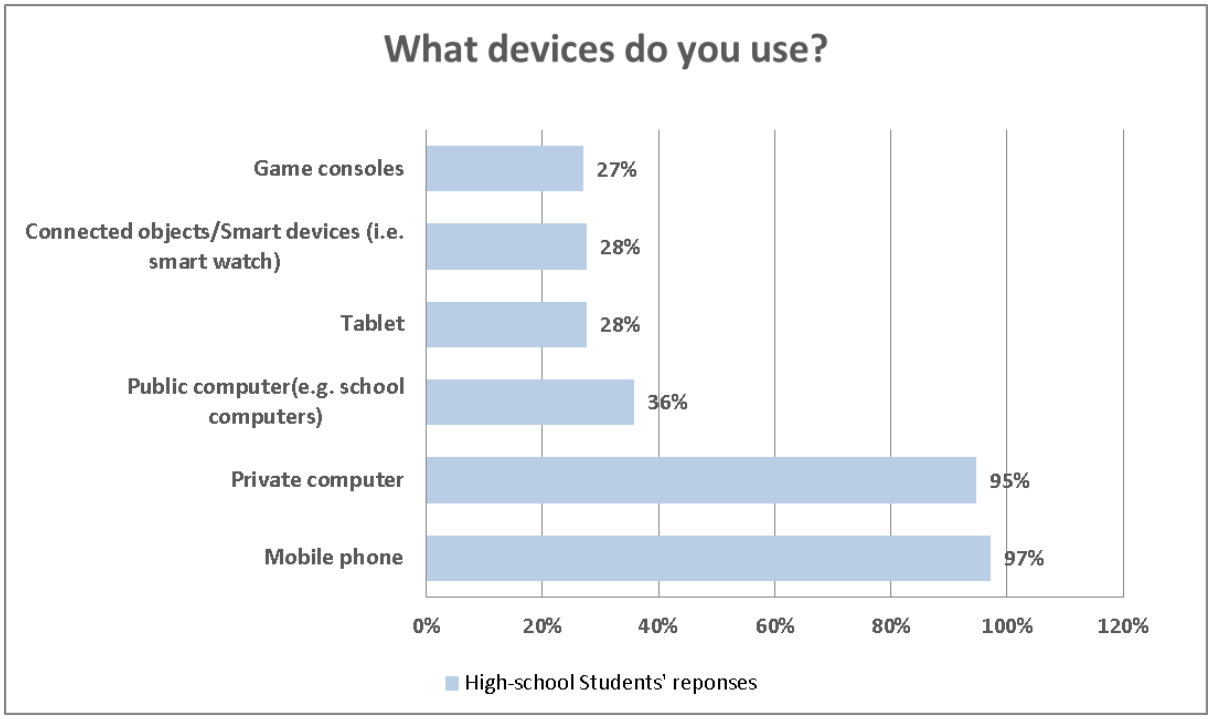
Type of Question: multiple choice

Possible answers:

- *Private computer*
- *Mobile phone*
- *Tablet*
- *Public computer(e.g. school computers)*
- *Game consoles*
- *Connected objects/Smart devices (i.e. smart watch)*

Q2. General analysis

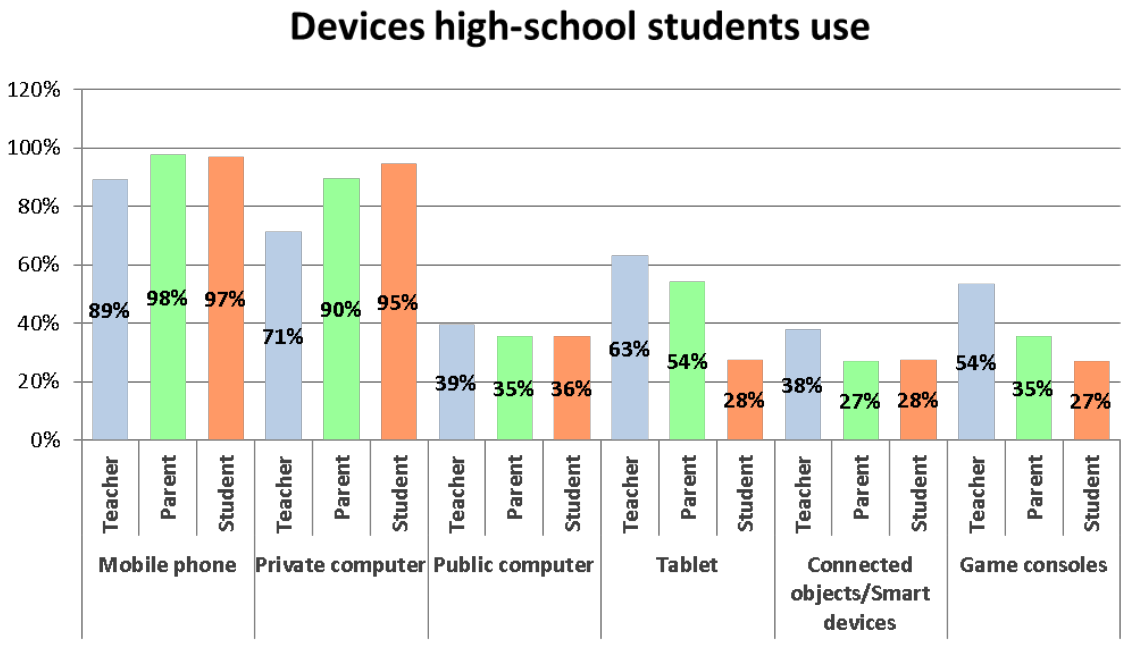
High-school Students' Responses:



Comments:

The plot above shows the responses of high-school students on what devices they use. The results show that almost all participants use mobile phone devices (97%) and private computer devices (95%). A range of percentages between 27%-36% is observed for the other options of devices.

We asked the same question to teachers and parents to understand their perception on what devices high-school students use. The plot below depicts the responses per group of participants for each device type.

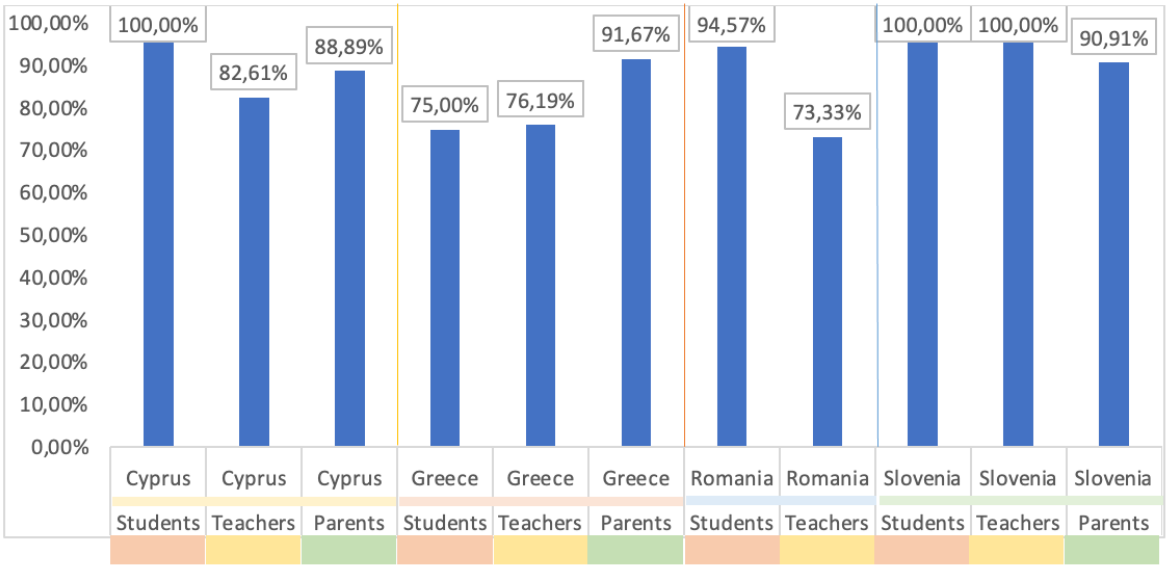


Comments:

We can observe that the groups mostly agree on the type of devices high-school students use. Moreover, teachers and parents mentioned tablets and game consoles more often than the students.

Q2. Country analysis

Private computer

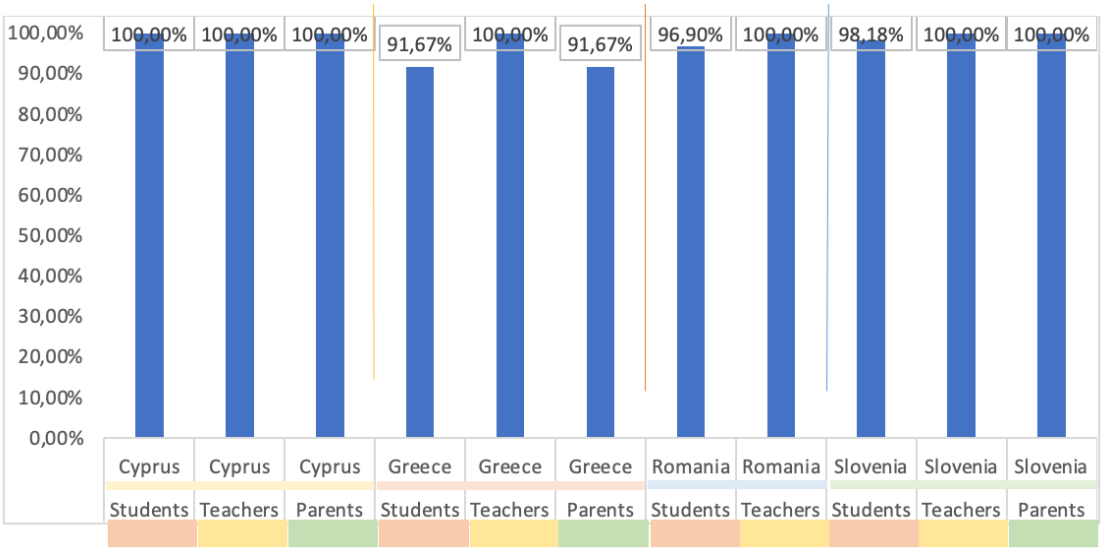


Comments:

The above diagram shows that a private computer is used by the majority of the high-school students. There is a difference between the perception (in average values) regarding the use of

private computers by high-school students in all countries, although the difference is not substantial in all cases.

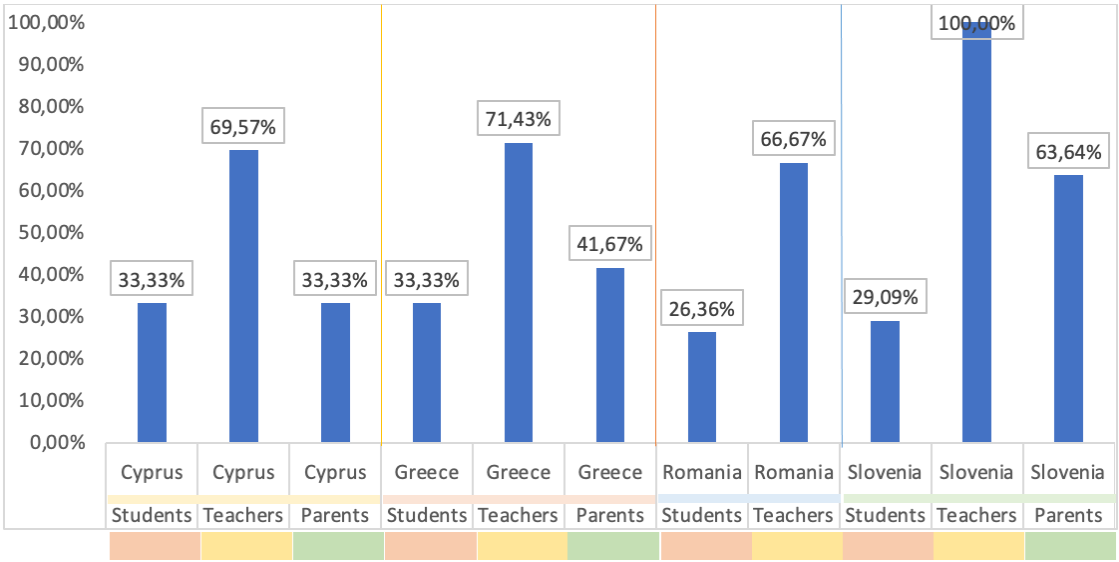
Mobile phone



Comments:

The above diagram shows that a mobile phone is used by the majority of the high-school students. The above diagram shows that there is a almost no difference between the perception (in average values) regarding the use of mobile phones by high-school students in all countries by their parents and teachers.

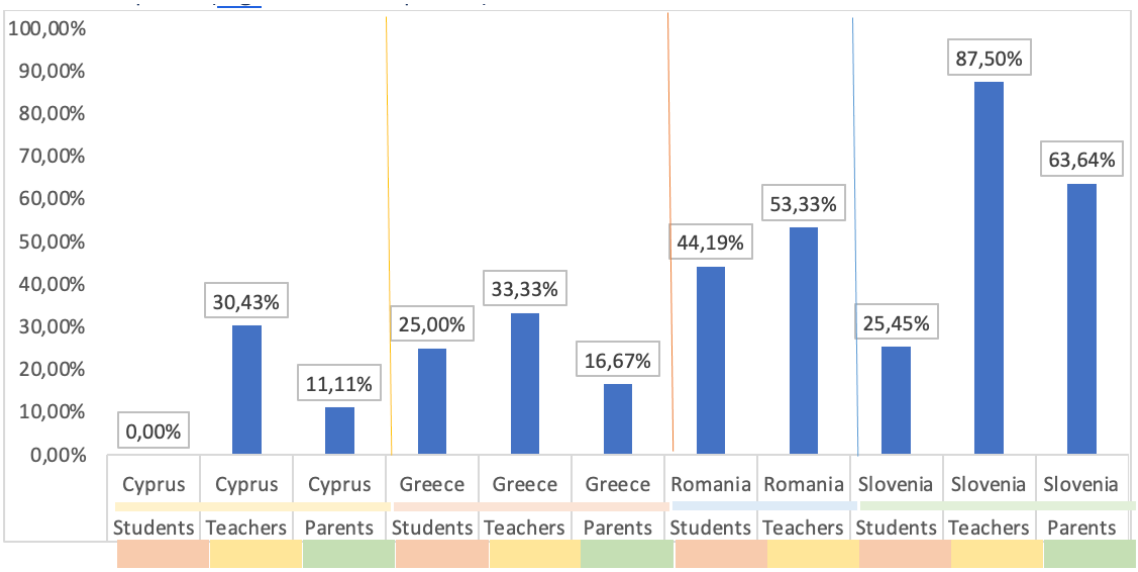
Tablet



Comments:

The above diagram shows that tablets are not used by the majority of the high-school students. In average values, the percentage of high-school students that claim using a tablet is not more than 30%. The above diagram shows that there is a significant difference between the perception (in average values) regarding the use of tablets by high-school students in all countries.

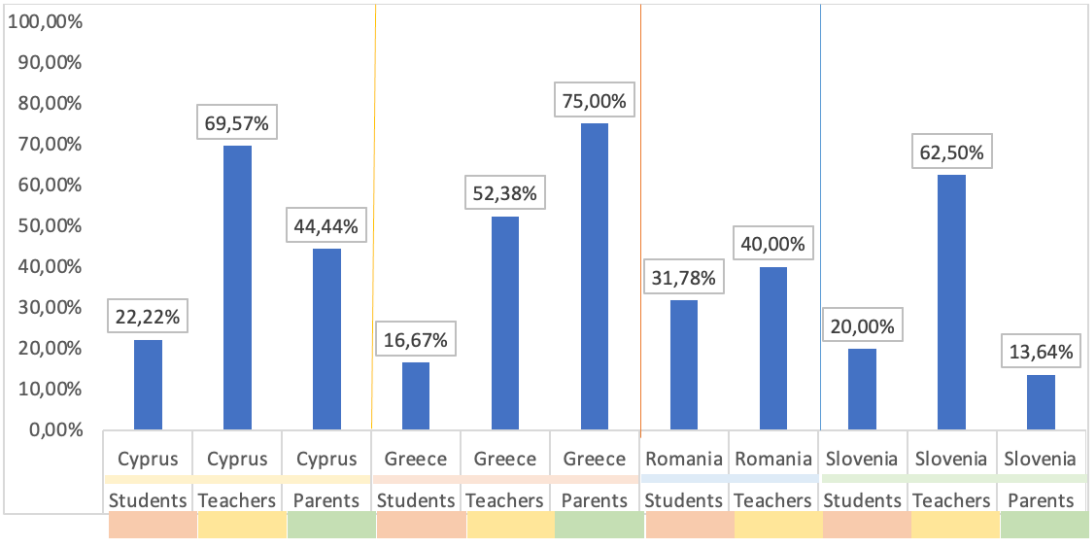
Public computer (e.g. school computers)



Comments:

The above diagram shows that public computers are not used by the majority of the high-school students. In average values, the percentage of high-school students that claim using a tablet is not more than 30%. The above diagram shows that there is a significant difference between the perception (in average values) regarding the use of public computers by high-school students in all countries.

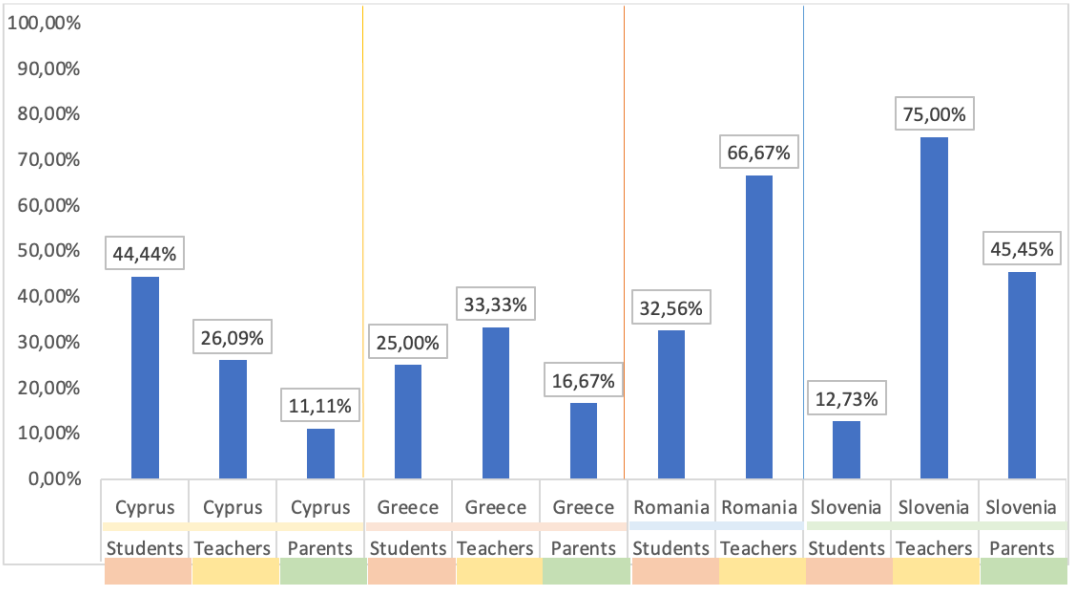
Game consoles



Comments:

The above diagram shows that game consoles are not used by the majority of the high-school students. In average values, the percentage of high-school students that claim using a tablet is not more than 30%. The above diagram shows that there is a significant difference between the perception (in average values) regarding the use of game consoles by high-school students in all countries.

Connected objects/Smart devices (i.e. smart watch)



Comments:

The above diagram shows that connected objects / smart devices are not used by the majority of the high-school students. In average values, the percentage of high-school students that claim using a tablet is not more than 40%. The above diagram shows that there is a significant difference between the perception (in average values) regarding the use of connected objects / smart devices by high-school students in all countries.

Q3. How confident are high-school students in the following online activities?

Type of Question: multiple choice

Possible answers:

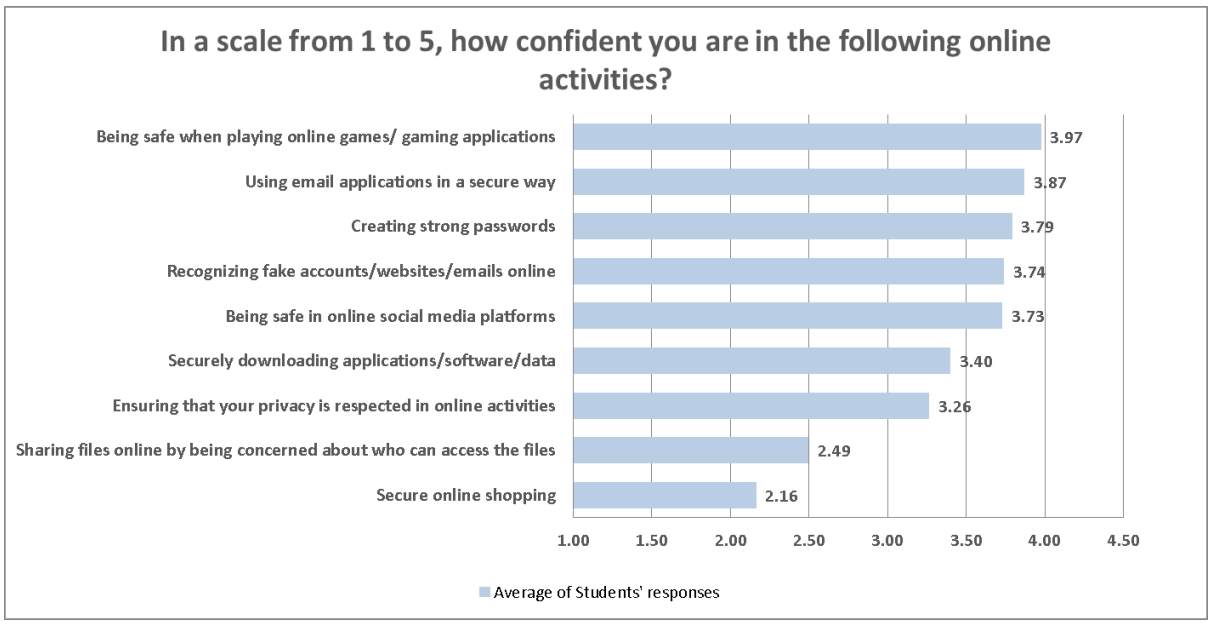
- *Creating strong passwords for online accounts, devices, etc.*
- *Being safe in online social media platforms (e.g. Facebook, Instagram, Twitter)*
- *Using email applications in a secure way (e.g. avoiding spams, checking attachments)*
- *Sharing files online (e.g. Dropbox, OneDrive) by being concerned about who can access the file*
- *Securely downloading applications/software/data*
- *Ensuring that your privacy is respected in online activities (e.g. handling of cookies, statin*
- *Recognizing fake accounts/websites/emails online*
- *Being safe when playing online games/ gaming applications*
- *Secure online shopping*

The participants were asked to provide their feedback using the following scale:

- *1 - Not Confident*
- *2 - Little Confident*
- *3 - Neutral*
- *4 - Confident*
- *5 - Very Confident*

Q3. General analysis

High-school Students' Responses:

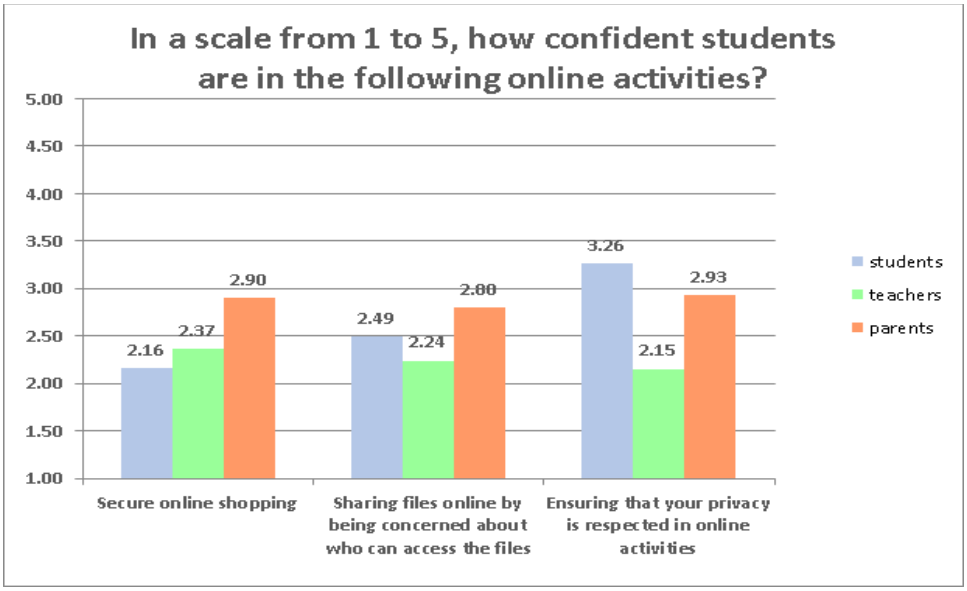


Comments:

Students seem to feel confident in being safe when playing, using email applications in a secure way, creating strong passwords, recognizing fake accounts, and being safe in online social

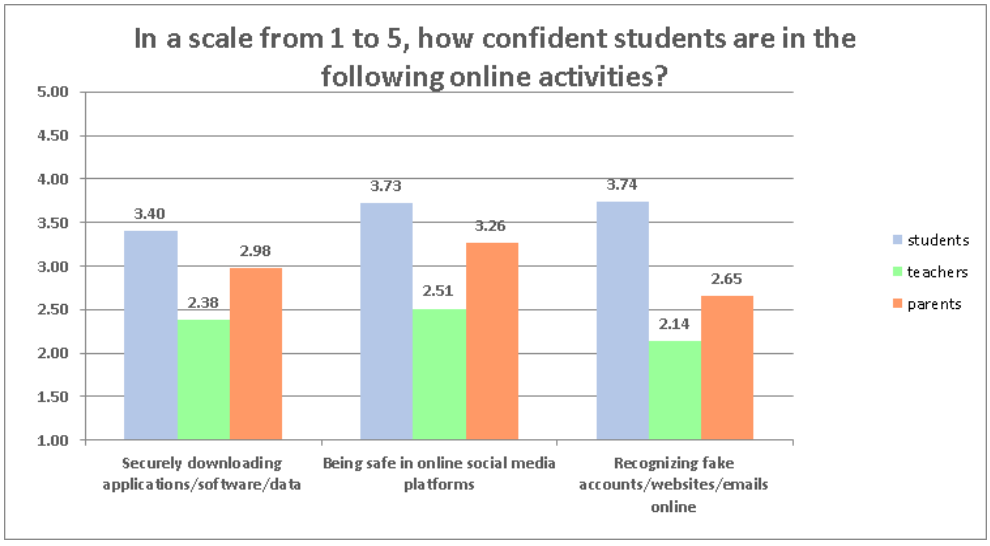
media platforms. Other than that, their responses show that they feel neutral-confident in securely downloading online content and ensuring their privacy is preserved when being online. The online-activities students mentioned feeling a little confident are sharing files online and shopping securely.

We asked the same question to teachers and parents to understand their perception of how confident high-school students are in those online-activities. The plots below depict the responses per group of participants for each online activity in the list of answers options.



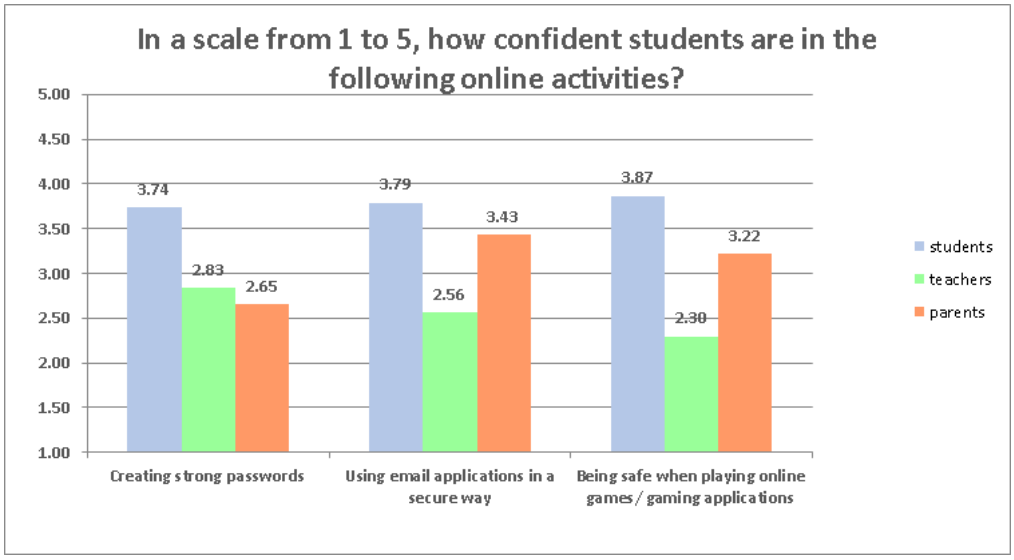
Comments:

From the plot above, we see the three activities students feel less confident with and we notice that for secure online-shopping and sharing files online teachers' perception is similar to the students (little confident) while parents replied with neutral-confident. For ensuring their privacy, parents' perception is similar to the students' (neutral-confident) while teachers replied with little confident. We can observe here that parents seem to be more optimistic about their children's confidence with online activities than the teachers.



Comments:

The plot above shows that for securely downloading online content parents' perception is similar to the students' responses (neutral-confident) while teachers replied with little confident. For being safe in online social media platforms and recognizing fake online-content students seem to be confident, while their teachers and parents look to be less optimistic with parents replying with neutral-confident for both the activities and with teachers replying with neutral-confident and little confident accordingly. We can observe in general that students seem to be the more optimistic about their confidence level according to those online activities while their teachers seem to be less optimistic than both the students and the parents.



Comments:

In the plot above we can see the online activities the students feel more confident with. We can observe that parents' and teachers' perceptions for creating strong passwords and using email applications are similar (neutral-confident), while for securely playing online games teachers replied with little confident and parents with neutral-confident.

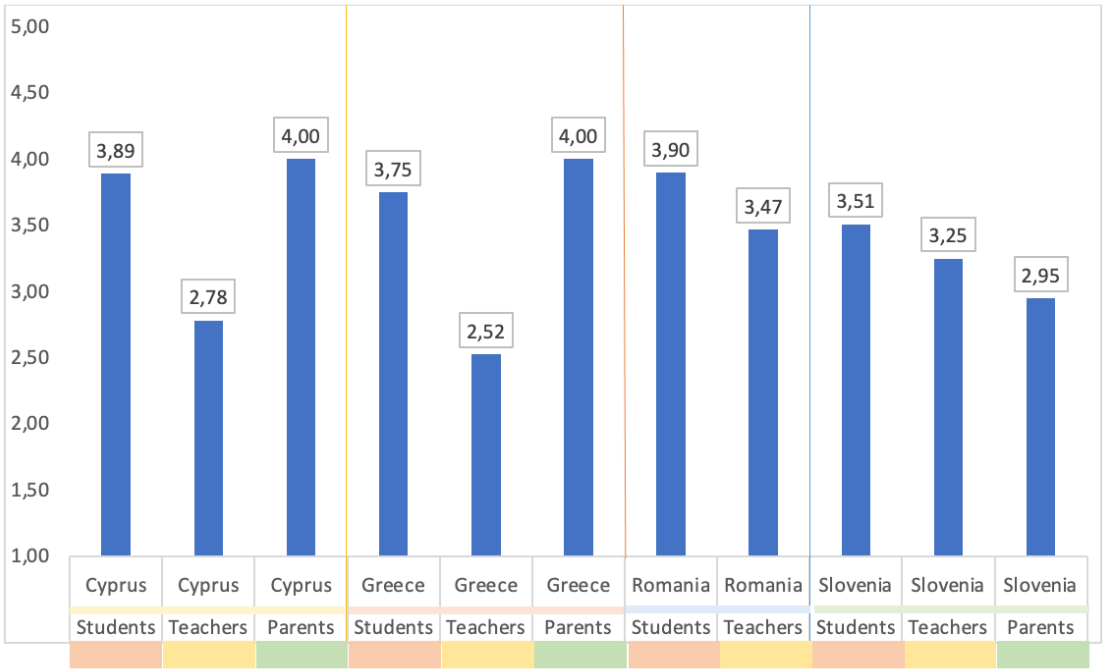
In general, we noticed that none of the groups' average confidence level for any of the online-activities falls under the not-confident or very-confident.

The following table contains the average value of confidence per audience irrespective of the country.

Audience	*Average Value %*	*Characterization*
High School Students	*3,54 %*	*Neutral to Confident*
Teachers of High School Students	*2,50 %*	*Little Confident to Neutral*
Parents of High School Students	*3,21 %*	*Neutral to Confident*

Q3. Country analysis

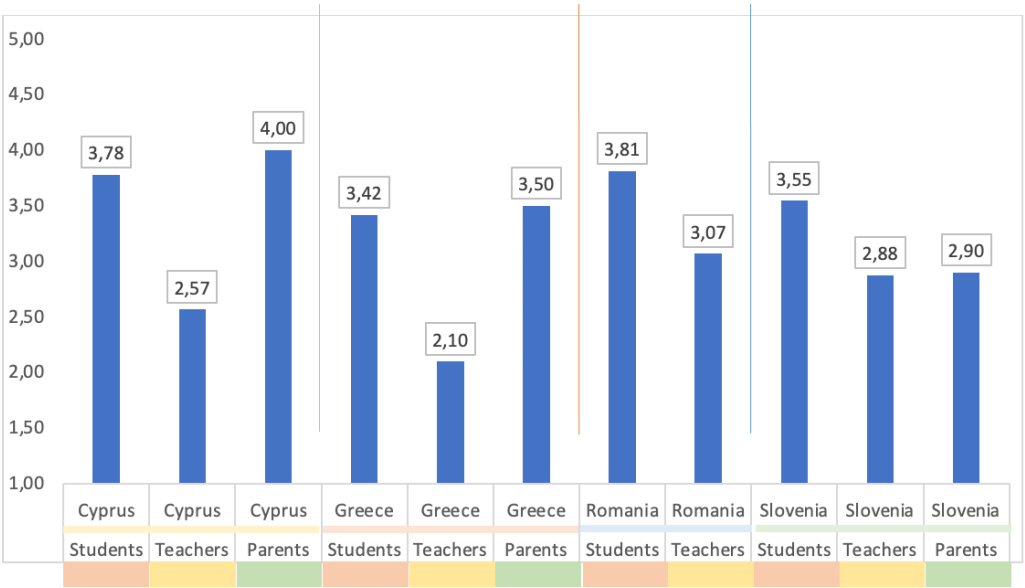
Creating strong passwords for online accounts, devices, etc.



Comments:

The average value regarding the confidence that the students claimed they have regarding the creation of strong passwords for online accounts, devices etc 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.

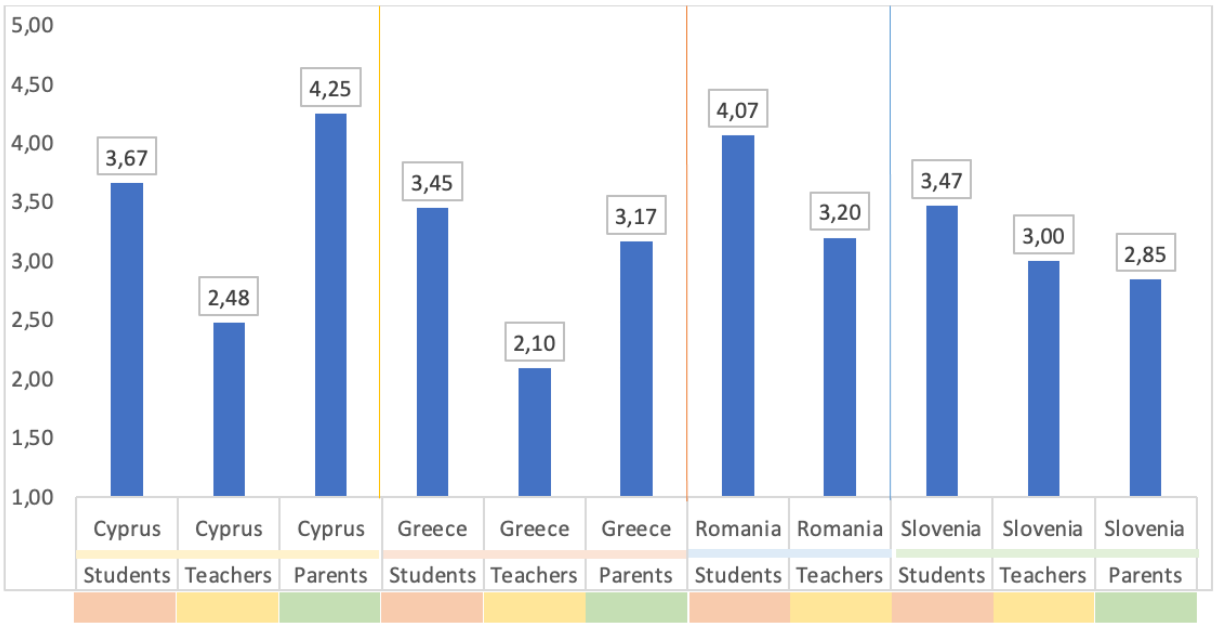
Being safe in online social media platforms (e.g. Facebook, Instagram, Twitter)



Comments:

The average value regarding the confidence that the students claimed they have regarding Being safe in online social media platforms is situated between neutral and confident (3,64 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 Confident to Neutral (2,65) and Neutral to Confident (3,47) respectively.

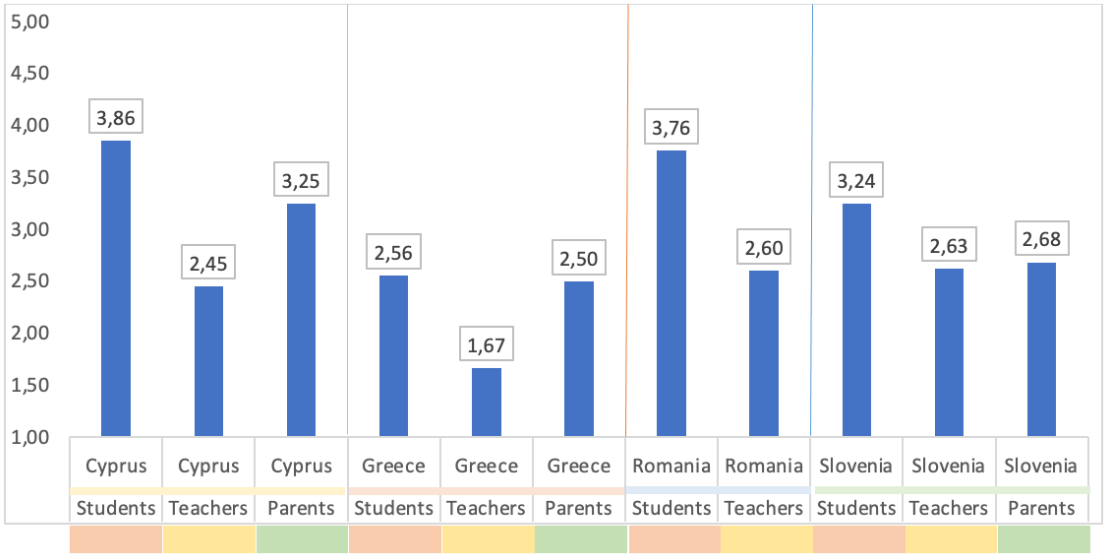
Using email applications in a secure way (e.g. avoiding spams, checking attachments)



Comments:

The average value regarding the confidence that the students claimed they have regarding Using 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 Little Confident to Neutral (2,69) and Neutral to Confident (3,42) respectively. It is worth to mention, that great differences are observed between respondents from different countries (e.g. Parents in Greece are neutral (3,17) regarding the confidence of students in using email applications in a secure way, where as Parents in Cyprus are Confident (4,25))

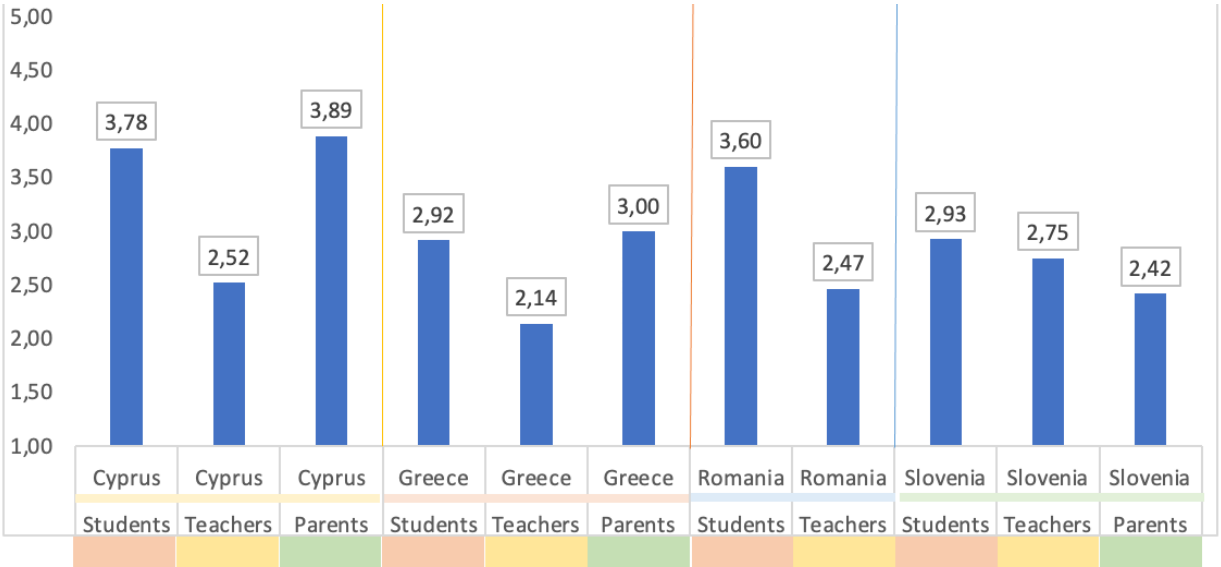
Sharing files online (e.g. Dropbox, OneDrive) by being concerned about who can access the file



Comments:

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 Confident to Neutral (2,34) and Little Confident to Neutral (2,81) respectively.

Securely downloading applications/software/data

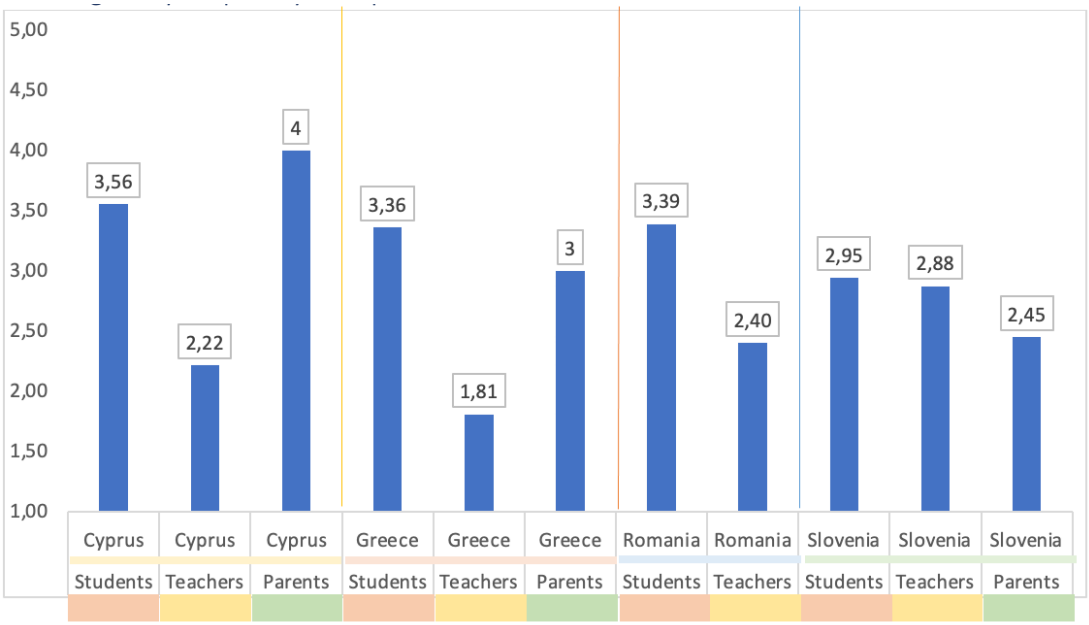


Comments:

The average value regarding the confidence that the students claimed they have in Securely downloading applications/software/data is situated between neutral and confident (3,31 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 Confident to Neutral (2,47) and Neutral to Confident (3,10) respectively.

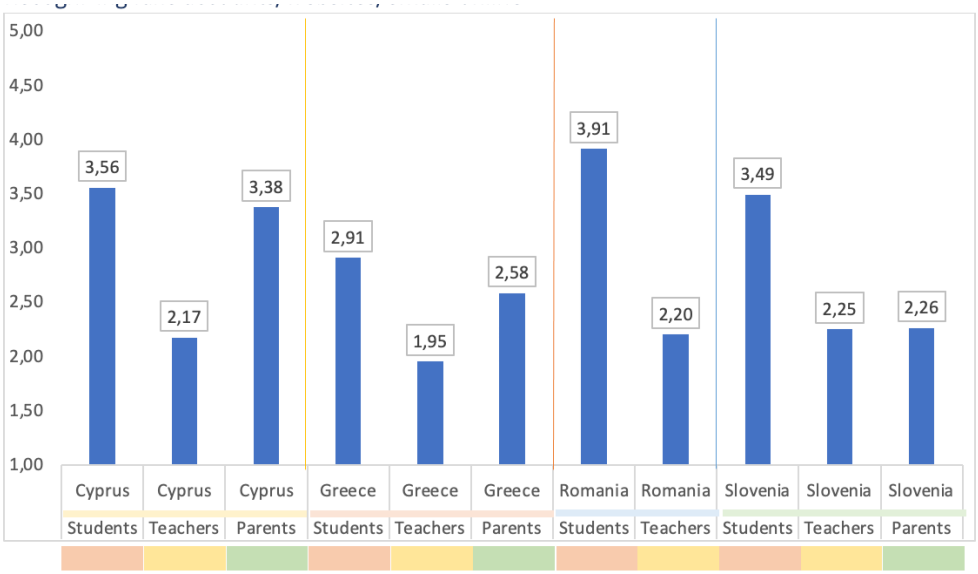
Ensuring that your privacy is respected in online activities



Comments:

The average value regarding the confidence that the students claimed they have in ensuring their privacy is respected in online activities is situated between neutral and confident (3,31 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 Confident to Neutral (2,33) and Neutral to Confident (3,15) respectively. It is worth mentioning that the parents' replies cover a wide range depending on the country. E.g., in Cyprus believe that the students are Confident regarding this activity where as in Greece they believe that they are Little Confident (1,95).

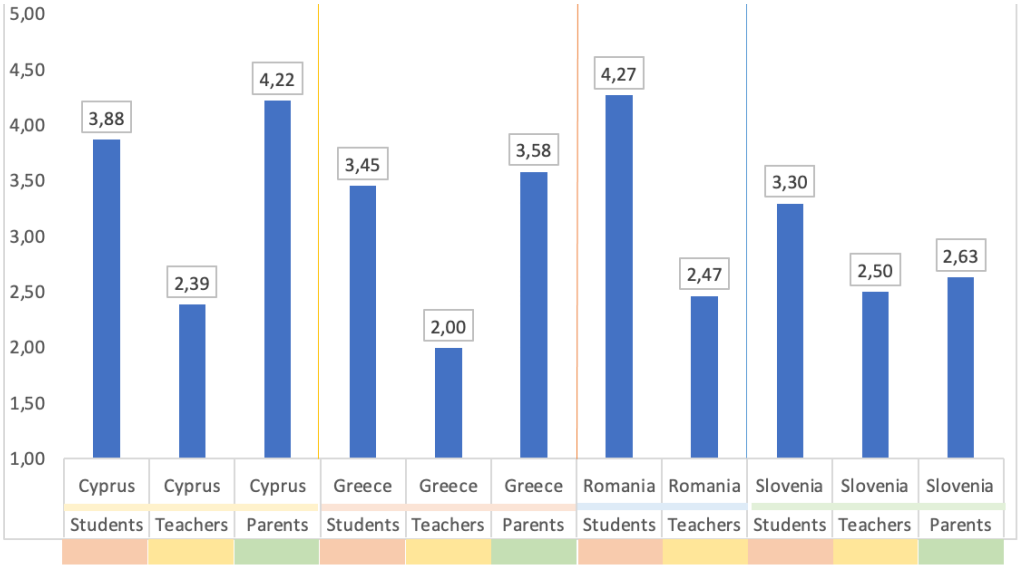
Recognizing fake accounts/websites/emails online



Comments:

The average value regarding the confidence that the students claimed they have in Recognizing fake accounts/websites/emails online is situated between neutral and confident (3,47 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 Confident to Neutral (2,14) and Little Confident to Neutral (2,67) respectively.

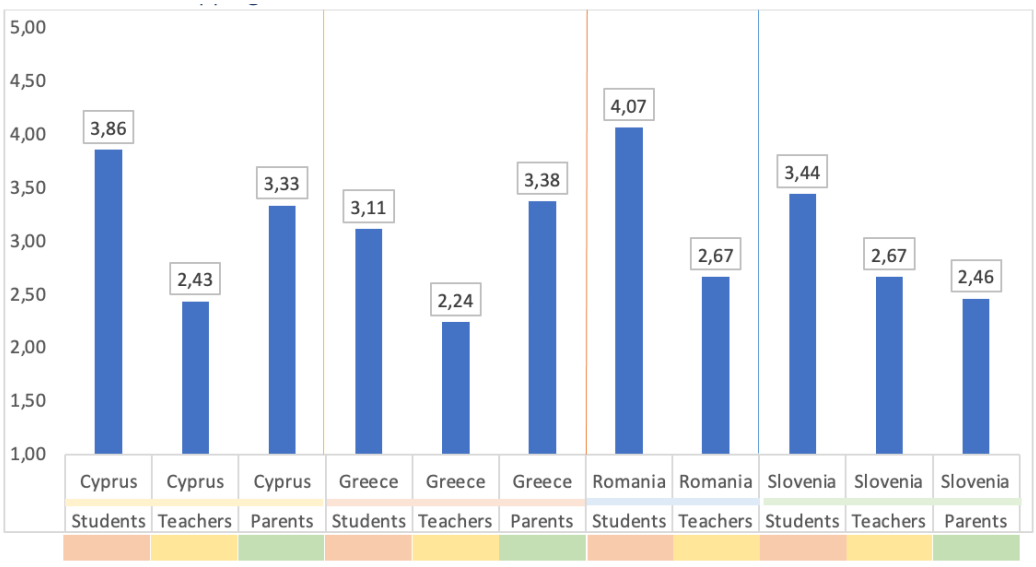
Being safe when playing online games/ gaming applications



Comments:

The average value regarding the confidence that the students claimed they have in Being safe when playing online games/ gaming applications is situated between neutral and confident (3,73 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 Confident to Neutral (2,34) and Neutral to Confident (3,48) respectively.

Secure online shopping



Comments:

The average value regarding the confidence that the students claimed they have in Secure online shopping is situated between neutral and confident (3,62 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 Confident to Neutral (2,50) and Neutral to Confident (3,06) respectively.

The following table contains the average value of confidence per audience per country.

Country	*Audience*	*Average Value %*	*Characterization*
Cyprus	*High School Students*	*3,76 %*	*Neutral to Confident*
Cyprus	*Teachers of High School Students*	*2,45 %*	*Little Confident to Neutral*
Cyprus	*Parents of High School Students*	*3,81 %*	*Neutral to Confident*
Greece	*High School Students*	*3,21 %*	*Neutral to Confident*
Greece	*Teachers of High School Students*	*2,06 %*	*Little Confident to Neutral*
Greece	*Parents of High School Students*	*3,19 %*	*Neutral to Confident*
Slovenia	*High School Students*	*3,32 %*	*Neutral to Confident*
Slovenia	*Teachers of High School Students*	*2,75 %*	*Little Confident to Neutral*
Slovenia	*Parents of High School Students*	*2,62 %*	*Little Confident to Neutral*
Romania	*High School Students*	*3,87 %*	*Neutral to Confident*
Romania	*Teachers of High School Students*	*2,73%*	*Little Confident to Neutral*

As shown from the values in the table, no audience believe that high-school students are confident or very confident in securely handling specific areas of online services, indicating a clear need for actions. Also, in all cases the perception of high school students about their confidence has a distinct difference from that of the teachers of high-school teachers.

Q4. When utilizing online activities high-school students:

Type of Question: multiple choice

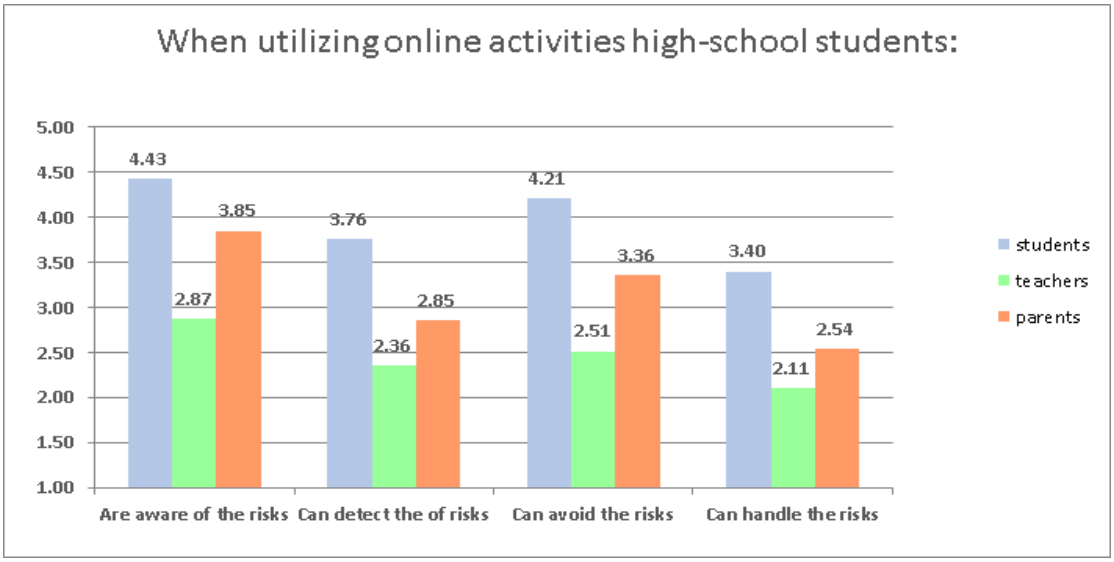
Possible answers:

- *Are aware of the online risks*
- *Can detect the online risks*
- *Are cautious and try to avoid online risks*
- *Know how to handle an online risk, If they experience one*

The participants were asked to provide their feedback using the following scale:

- *1 - Strongly Disagree*
- *2 - Disagree*
- *3 - Neutral*
- *4 - Agree*
- *5 - Strongly Agree*

Q4. General analysis



Comments:

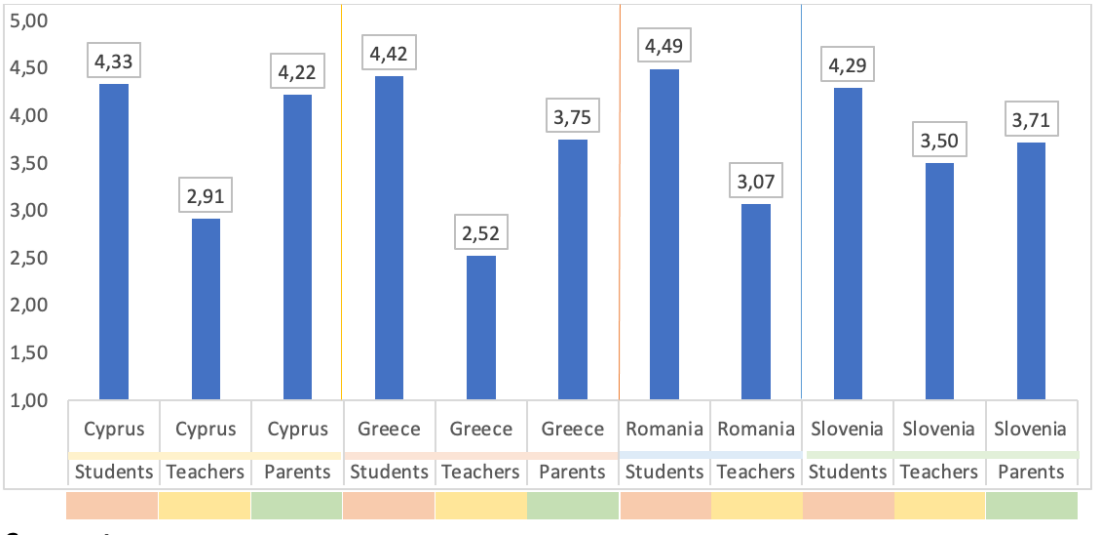
The plot above shows that students agree that they are aware of the risks, can detect the risks, and can avoid the risks, but they are neutral in the statement that they can handle the risks. Again, we can also observe that the teachers are less optimistic about the students' ability regarding these statements since on average they replied with the disagree and neutral options. 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 statement that all the groups of participants agreed with the least was that students can handle the online-risks.

The following table presents the average values of belief from each perspective that a high-school student is aware, can detect and react to online risks irrespective of the country.

Audience	*Average Value %*	*Characterization*
High School Students	*3,89 %*	*Neutral to Agree*
Teachers of High School Students	*2,53 %*	*Disagree to Neutral*
Parents of High School Students	*3,30 %*	*Neutral to Agree*

Q4. Country analysis

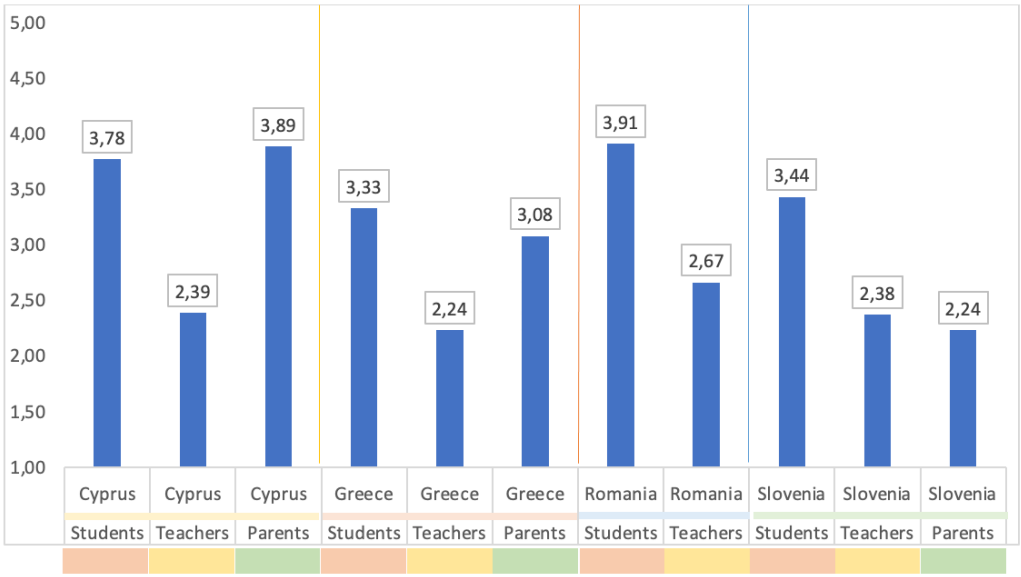
Are aware of the online risks



Comments:

The average value 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 awareness of students the average values were Neutral (3,00) and Neutral to Confident (3,90) respectively. As before (Question 3 above) there is a distinct difference between the perspective of the high school students and the teachers of high school students in all countries and especially in Greece. This difference is not so pronounced in the case of parents.

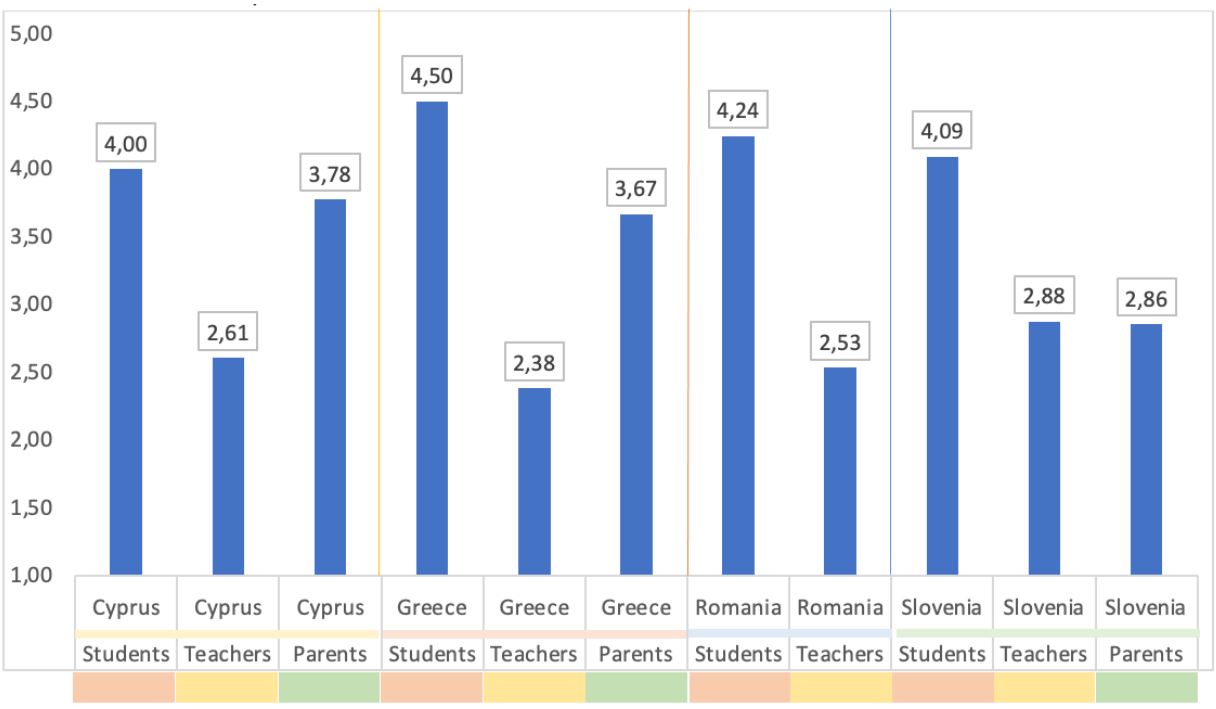
Can detect the online risks



Comments:

The average value regarding the ability of high school students to detect online risks is situated between Neutral and Agree (3,62 from entries in all countries). At the same time, when the teachers and parents were asked the same questions regarding the ability of students the average values were Disagree to Neutral (2,42) and Neutral (3,07) respectively. As before there is a distinct difference between the perspective of the high school students and the teachers of high school students in all countries.

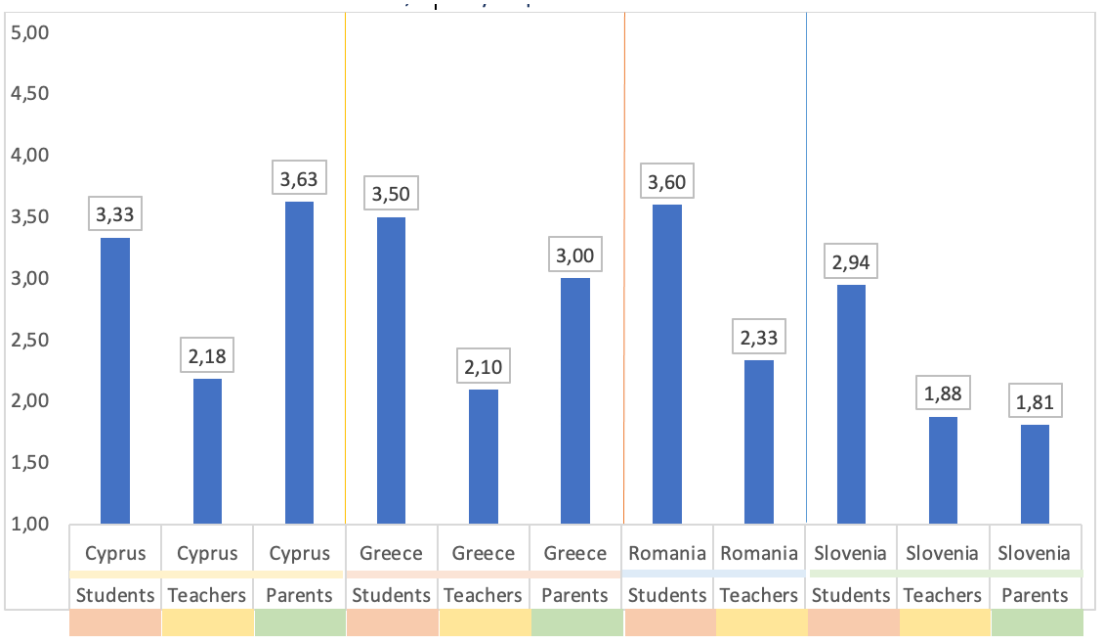
Are cautious and try to avoid online risks



Comments:

The average value regarding the ability of high school students of being cautious and avoiding online risks is situated between Agree and Strongly Agree (4,21 from entries in all countries). At the same time, when the teachers and parents were asked the same questions regarding the ability of students the average values were Disagree to Neutral (2,60) and Neutral to Agree (3,42) respectively. As before there is a distinct difference between the perspective of the high school students and the teachers of high school students in all countries.

Know how to handle an online risk, if they experience one



Comments:

The average value regarding the ability of high school students to handle an online risk, if they experience one is situated between Agree and Strongly Agree (4,21 from entries in all countries). At the same time, when the teachers and parents were asked the same questions regarding the ability of students the average values were Disagree to Neutral (2,12) and Disagree to Neutral (2,81) respectively. As before there is a distinct difference between the perspective of the high school students and the teachers of high school students in all countries.

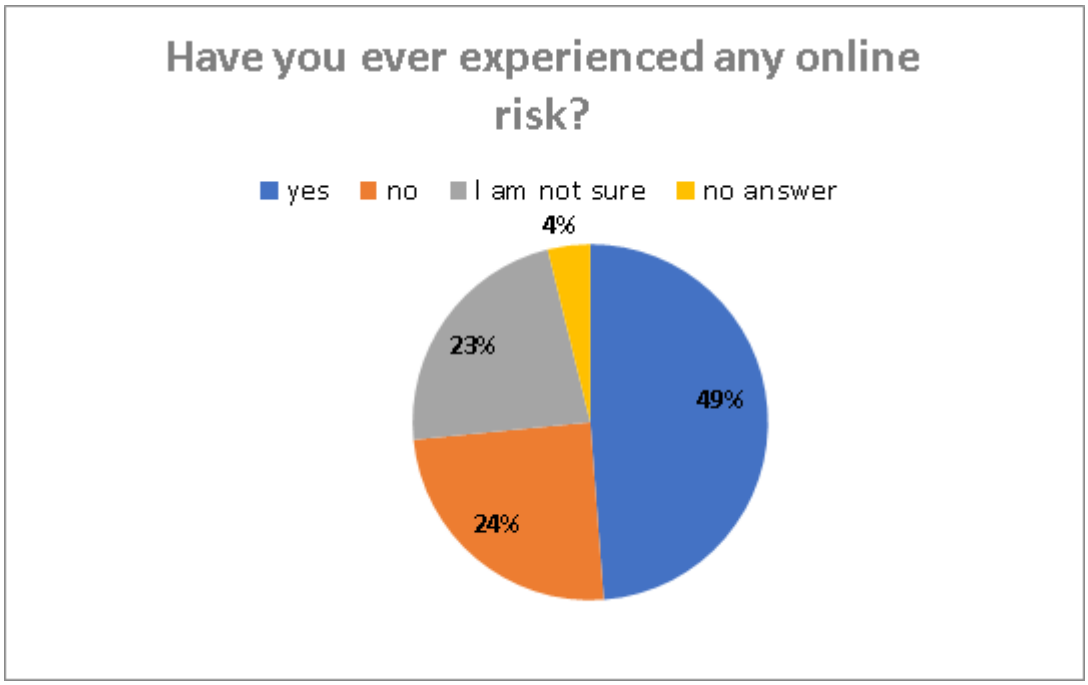
Irrespective of perspective, the average values indicate that there is a need for strengthening the skills of high-school students in their awareness, detection and the ways of handling and avoiding online risks.

Q5. Have you ever experienced any online risk?

<u>Type of Question</u>: multiple choice

<u>Possible answers:</u>

- *Yes*
- *No*
- *I am not sure*
- *No answer*



Comments:

The above figure shows the students' response to whether they experienced any online-risk before. The majority of the high-school students replied with "Yes", while with similar percentages 24% and 23% they replied with "No" and "I am not sure" accordingly. The participants who answered with "I am not sure" might be unaware of the risks or lack the ability to detect online-risks. Having the majority of the participants mention that they experienced an online-risk before shows how important it is to take action and educate the minors for their online security and safety.

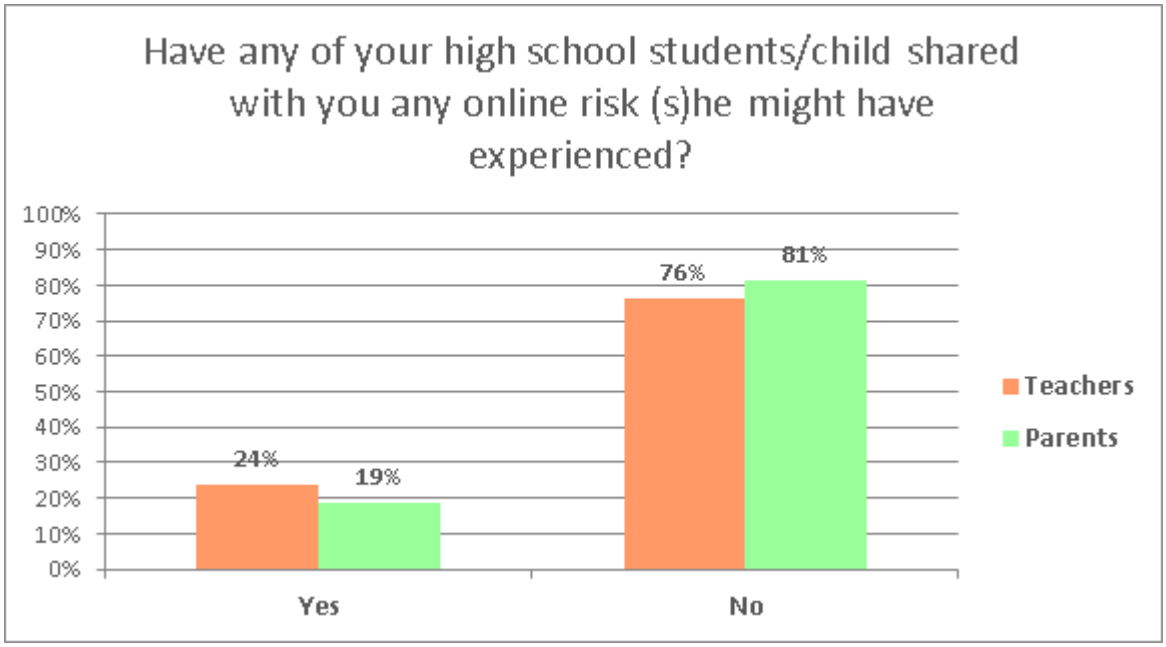
We address a similar question to assess if students share their online risks experiences with their teachers or parents. So we asked parents and teachers the following question.

Q6. Have any of your high school students/children shared with you any online risk (s)he might have experienced?

Type of Question: multiple choice

Possible answers:

- *Yes*
- *No*



Comments:

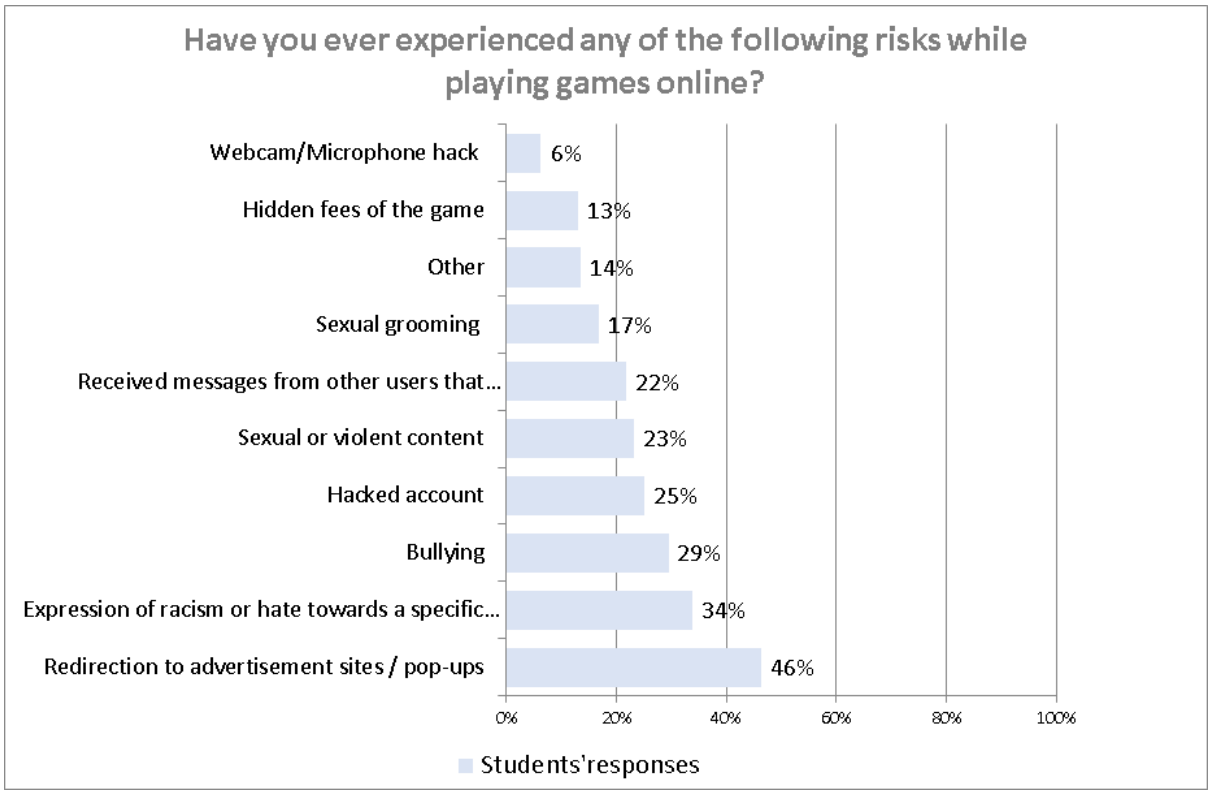
From the plot above, we can see that most parents and teachers replied with a no. The negative answer here can mean two things: students don't experience any online risks to share, or they don't share their experiences with their parents or teachers. The students' responses on whether they have experienced any online-risks, 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 we want students to trust their teachers and parents and collaborate with them in handling the risks.

Q7. Have you ever experienced any of the following risks while playing games online?

Type of Question: multiple choice

Possible answers:

- *Webcam/Microphone hack (your camera/microphone was turned on by someone else)*
- *Bullying*
- *Expression of racism or hate towards a specific group of people*
- *Hidden fees of the game*
- *Hacked account*
- *Received messages from other users that asked you for personal information(email, password, address, phone) with fake excuses*
- *Redirection to advertisement sites/pop-ups*
- *Sexual or violent content*
- *Sexual grooming (an adult send you inappropriate messages through game platform chat)*
- *Other*



Comments:

When we asked the students for the online risks they experienced while playing online games, the most common risk retrieved was 'redirection to advertisement/sites' with a percentage of 46%. In the second and third place, we can see 'Expression of racism or hate' and 'Bullying' with percentages of 34% and 29%. With percentages from 22% to 25%, students replied with 'Hacked Account', 'Sexual or Violent Content', and 'Received messages from other users that asked you for personal information".

Q8. Which online activities do you consider important to be discussed with high school students in school?

Type of Question: multiple choice

Possible answers:

- *Being safe in online social media platforms (e.g. Facebook, Instagram, Twitter)*
- *Recognizing fake accounts/websites/emails*
- *Creating strong passwords for online accounts, devices, etc.*
- *Securely downloading applications/software/data*
- *Ensuring your privacy is respected in online activities*
- *Using email applications in a secure way (e.g. avoiding spams, checking attachments)*
- *Being safe when playing online games*
- *Secure online shopping*
- *Sharing files online (e.g. Dropbox, OneDrive) by being concerned about who can access the files*

High School Students Responses:

Online-Activities to be discussed	% of students' voted
Being safe in online social media platforms(e.g. Facebook, Instagram, Twitter)	84%
Recognizing fake accounts/websites/emails	70%
Creating strong passwords for online accounts, devices, etc.	49%
Securely downloading applications/software/data	49%
Ensuring your privacy is respected in online activities	45%
Using email applications in a secure way (e.g. avoiding spams, checking attachments)	38%
Being safe when playing online games	31%
Secure online shopping	29%
Sharing files online (e.g. Dropbox, OneDrive) by being concerned about who can access the files	21%

Comments:

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

Teachers' Responses:

Online-Activities to be discussed	% of teachers' voted
Being safe in online social media platforms(e.g. Facebook, Instagram, Twitter)	73%
Ensuring your privacy is respected in online activities	67%
Creating strong passwords for online accounts, devices, etc.	45%
Using email applications in a secure way (e.g. avoiding spams, checking attachments)	44%
Recognizing fake accounts/websites/emails	43%
Securely downloading applications/software/data	39%
Being safe when playing online games	37%
Secure online shopping	20%
Sharing files online (e.g. Dropbox, OneDrive) by being concerned about who can access the files	18%

Comments:

The above table shows in descending order the online activities that the teachers voted for to be discussed during cybersecurity courses. A high percentage (73%) of teachers choose "Being safe in social media platforms" showing that this is the most important topic that needs to be addressed in a cybersecurity course for high-school students. "Ensuring online privacy" comes in second place with a percentage of 67%. With percentages between 43%-45%, recognizing fake content, using email applications securely, and creating strong passwords are in the list of the top-five online activities that teachers voted for to be discussed in a cybersecurity course.

Parents' Responses:

Online-Activities to be discussed	% of parents' voted
Being safe in online social media platforms(e.g. Facebook, Instagram, Twitter)	**79%**
Recognizing fake accounts/websites/emails	**54%**
Ensuring your privacy is respected in online activities	**52%**
Being safe when playing online games	**46%**
Using email applications in a secure way (e.g. avoiding spams, checking attachments)	**38%**
Securely downloading applications/software/data	**27%**
Creating strong passwords for online accounts, devices, etc.	**23%**
Sharing files online (e.g. Dropbox, OneDrive) by being concerned about who can access the files	**15%**
Secure online shopping	**8%**

Comments:

The above table shows in descending order the online activities that the parents voted for to be discussed during cybersecurity courses. A high percentage (79%) of parents chose "Being safe in social media platforms" showing that this is the most important topic that needs to be addressed in a cybersecurity course for high-school students. "Recognizing fake content" comes in second place 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 in the list of the top-five online activities that parents voted for to be discussed in a cybersecurity course.

Q9. Which type of methods/instruments would be more effective to be used while teaching cybersecurity at high-school level

Type of Question: multiple choice

Possible answers:

- *Live chats*
- *Games/Platforms*
- *Websites*
- *I don't know*
- *Videos*
- *Interactive presentations*
- *Fiches (paper materials)*
- *Massive Open Online Courses (MOOCs)*

Q9. General analysis

Students' Responses:

Instruments/Methods for teaching cybersecurity	% of students' voted
Interactive presentations	**64%**
Videos	**57%**
Games/Platforms	**56%**
Websites	**40%**
Live chats	**28%**
Fiches (paper materials)	**15%**
Massive Open Online Courses (MOOCs)	**14%**

Comments:
The table above shows the students' responses to the instruments that must be used for teaching cybersecurity courses to high-school students in descending order. The most popular instrument with a percentage of 64% of students voted for is "Interactive presentations". At the second and third place, we can see 'Videos' and 'Games/Platforms' with a percentage of 57% and 56% accordingly. In the list of the top-five most popular instruments, we can also find "Websites" and "Live Chats" with the percentages of 40% and 28% accordingly.

Teachers' Responses:

Instruments/Methods for teaching cybersecurity	% of teachers' voted
Videos	**68%**
Interactive presentations	**63%**
Games/Platforms	**54%**
Live chats	**29%**
Massive Open Online Courses (MOOCs)	**27%**
Websites	**25%**
Fiches (paper materials)	**12%**

Comments:

The table above shows the teachers' responses to the instruments that must be used for teaching cybersecurity courses to high-school students in descending order. The most popular instrument with a percentage of 68% of teachers voted for is 'Videos'. At the second and third place, we can see 'Interactive Presentations' and 'Games/Platforms' with a percentage of 63% and 54% accordingly. In the list of the top-five most popular instruments, we can also find "Live Chats" and "Massive Open Online Courses" with the percentages of 29% and 27% accordingly.

Parents' Responses:

Instruments/Methods for teaching cybersecurity	% of parents' voted
Videos	**58%**
Interactive presentations	**56%**
Games/Platforms	**38%**
Live chats	**27%**
Fiches (paper materials)	**27%**
Websites	**21%**
Massive Open Online Courses (MOOCs)	**10%**

Comments:

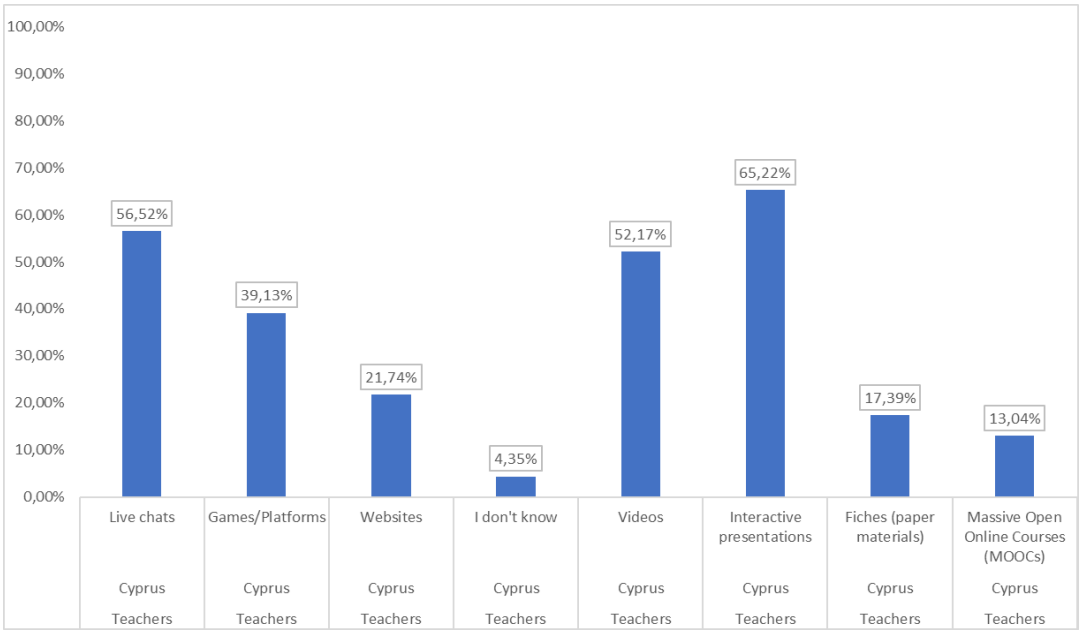
The table above shows the parents' responses to the instruments that must be used for teaching cybersecurity courses to high-school students in descending order. The most popular instrument with a percentage of 58% of parents voted for is 'Videos'. At the second and third place, we can see 'Interactive Presentations' and 'Games/Platforms' with a percentage of 56% and 38% accordingly. In the list of the top-five most popular instruments, we can also find "Live Chats" and "Fiches" with the percentage of 27% both.

In general, students, parents, and teachers seem to agree on more interactive or more gamified instruments to teach cybersecurity to high-school students. The three groups agreed on having the 'Videos', 'Interactive presentations', and 'Games/Platforms' in the top-three list of instruments that can be used. Only parents voted for 'Fiches' which is a more traditional method in teaching.

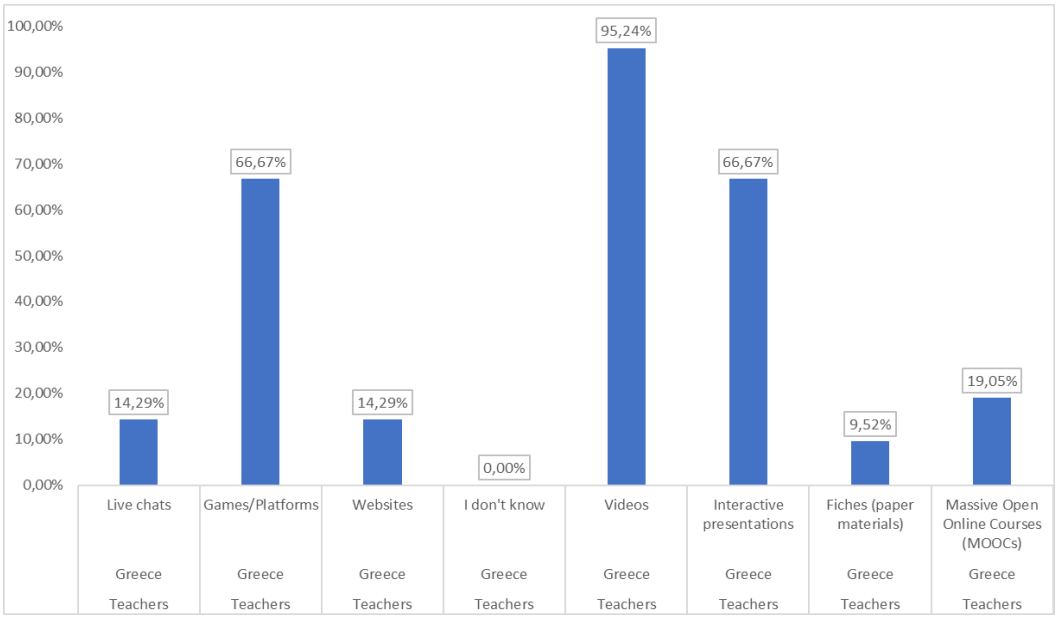
Q9. Country analysis

<u>Teacher's viewpoint:</u>

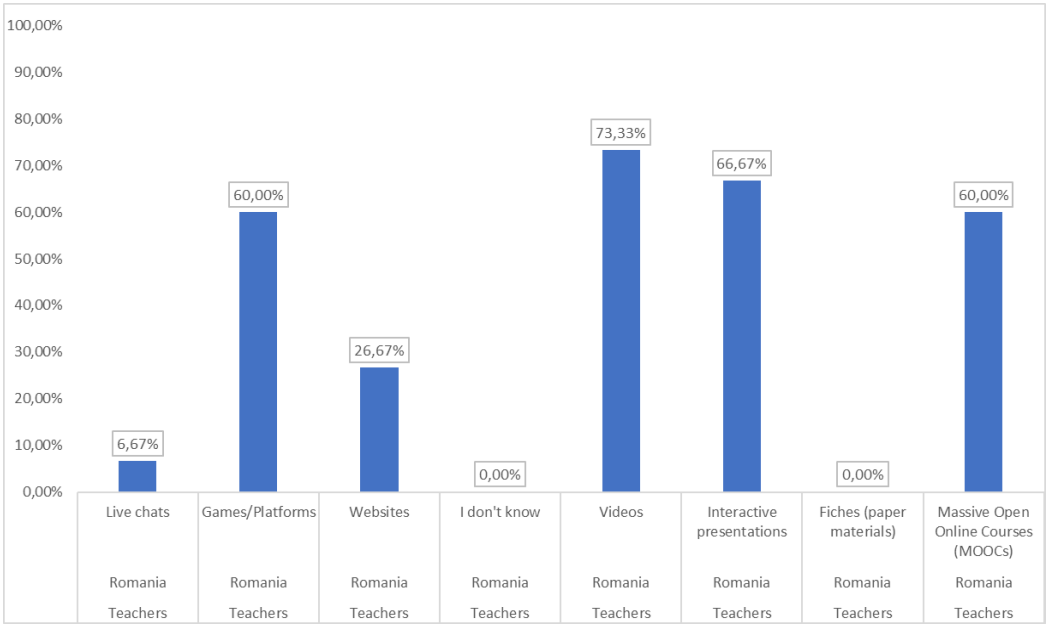
Cyprus



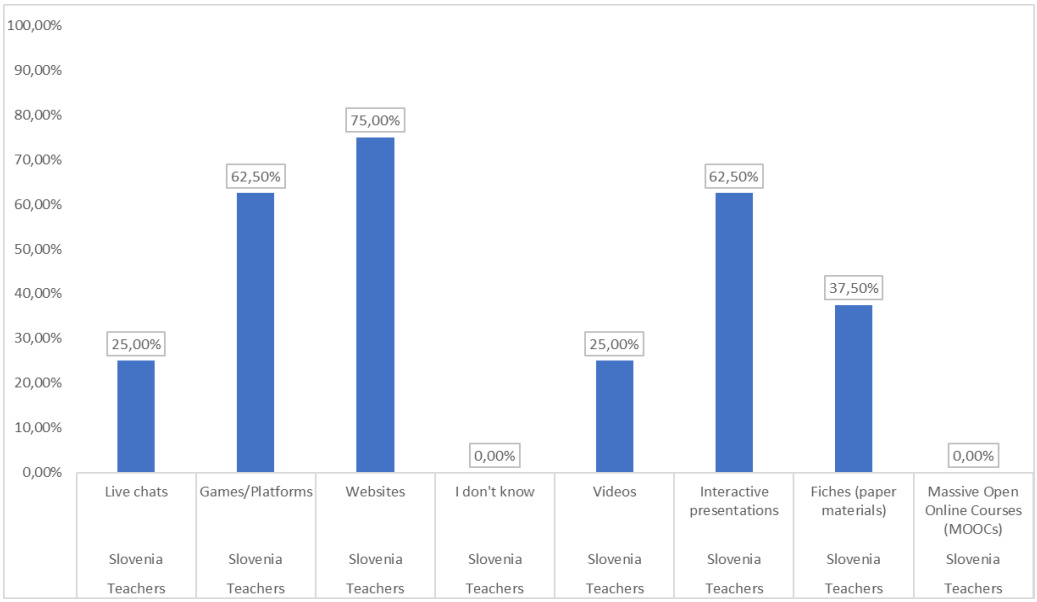
Greece



Romania



Slovenia



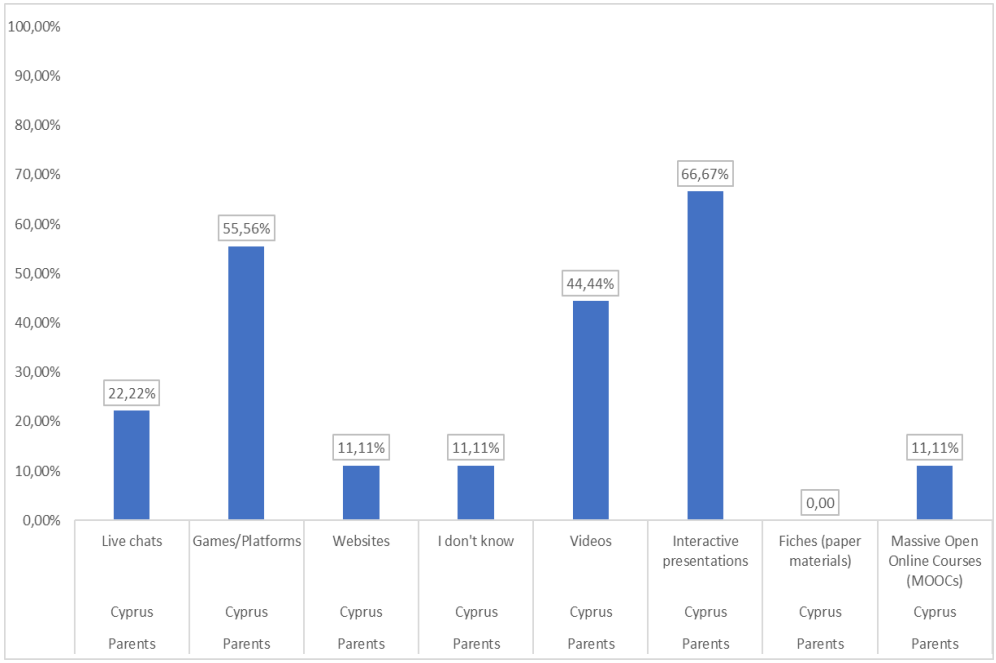
Comments:

As shown from the graphs above, the results per country differ. For example, in Cyprus the two most preferred methods / instruments that they believe would be more effective to while teaching cybersecurity to high school students are Interactive presentations and live chats, where as the preferred ones 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 more clear regarding the least preferred methods / instruments for teaching cybersecurity to high school students which are MOOCs (Cyprus and Slovenia), Fiches (paper materials) (Greece, Romania) and live chats (Greece, Romania and Slovenia).

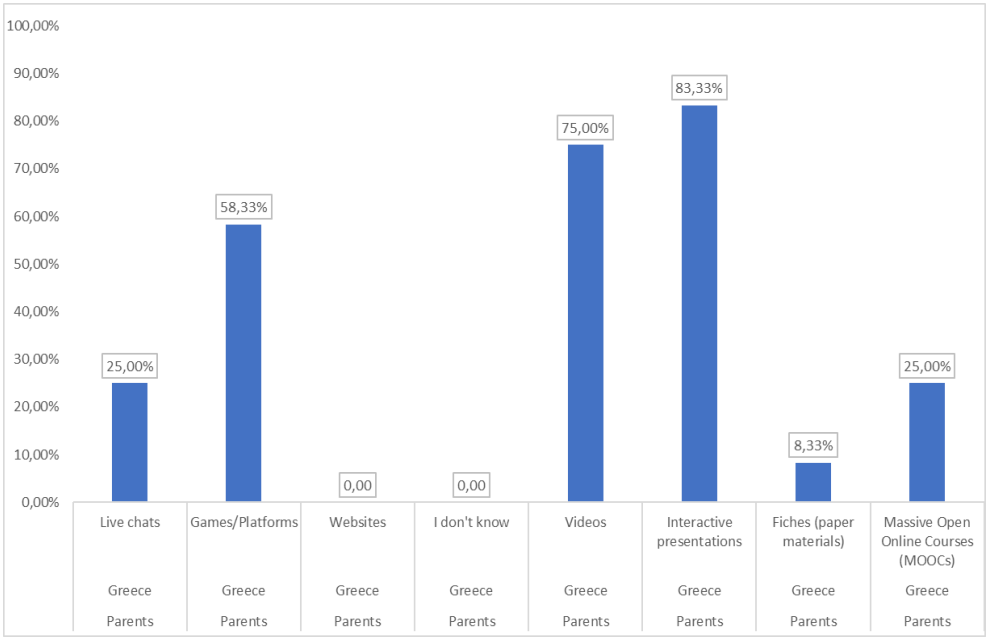
<u>Parents' viewpoint:</u>

The following graphs show the opinions of parents of high-school students when asked the same question.

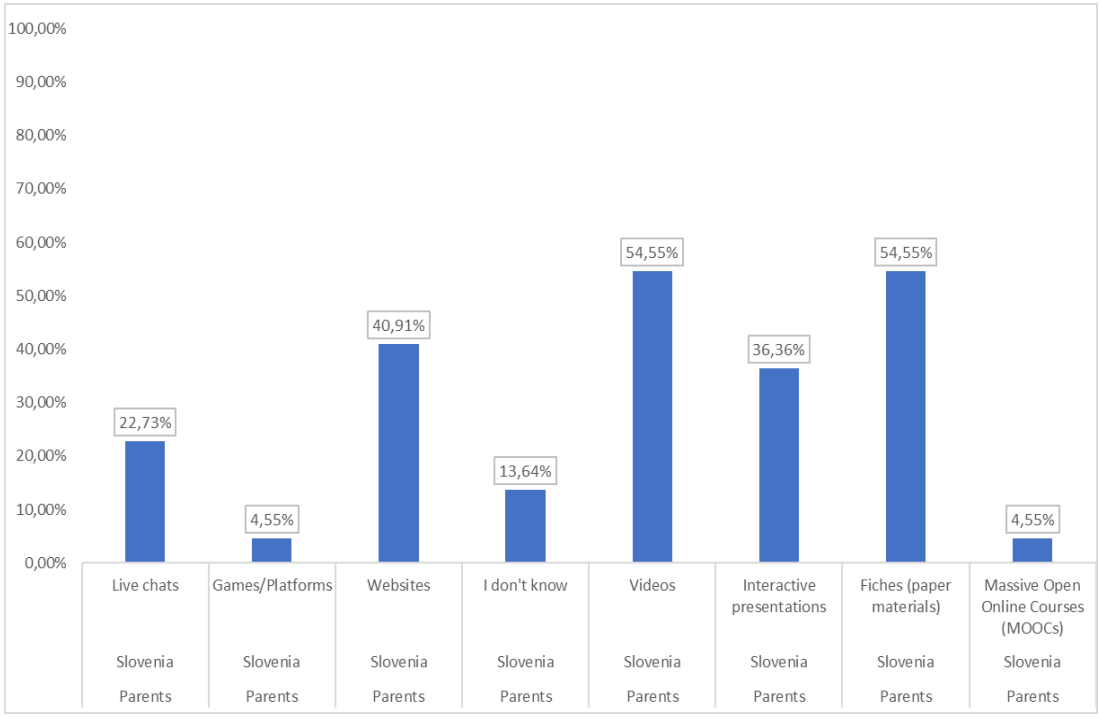
Cyprus



Greece



Slovenia



Comments:

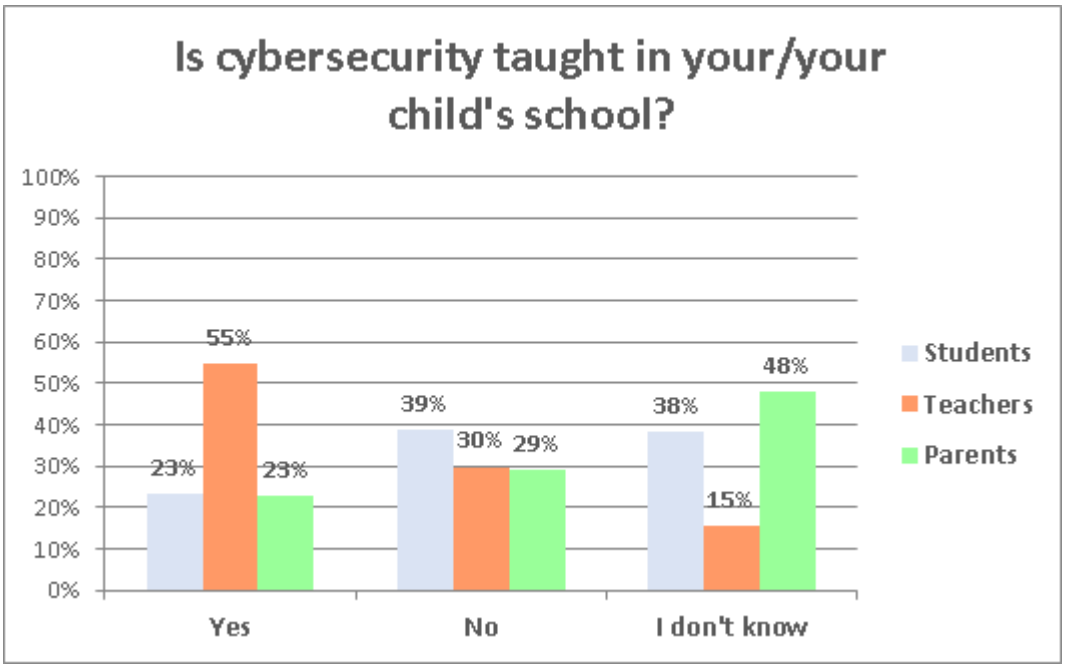
As shown from the graphs above, the results per country differ. For example, in Cyprus the two most preferred methods / instruments that they believe would be more effective while teaching cybersecurity to high school students are Interactive presentations and Games/platforms, whereas the preferred ones in Greece are Interactive presentations and videos, and in Slovenia videos and Fiches (paper materials). On the other hand, the least preferred methods / instruments for teaching cybersecurity to high school students are Fiches (paper materials) and Websites (Greece, Cyprus) and Massive Open Online Courses (MOOCs) and Games/Platforms (Slovenia).

Q10. Is cybersecurity taught in your/your child's school in any form?

Type of Question: multiple choice

Possible answers:

- *Yes*
- *No*
- *I don't know*



Comments:

From the plot above we can see that the majority of teachers (55%) replied positively in whether cybersecurity is taught in their school, while parents' majority replied with "I don't know" with percentages of 48% and students' percentage replied negatively with 38%. A very low percentage (23%) of students and parents replied positively. The results show that even if cybersecurity courses are part of the curriculum or taught in high schools in other forms students, and parents are unaware of it.

Combined Q. Verification of the knowledge / or implementation of secure online practices by high school students

This section contains the overview and results of a group of questions contained in the Survey which aimed at the verification of the knowledge / or implementation of secure online practices by high school students by providing simple scenarios and questions.

The questions contained in this Group are:

1. When it comes to create a password for an online account you choose

2. When you receive an email from an unknown sender, most of the times

3. Which of the following describes your activities in social media platforms?

4. A Web page asks you to enter your credentials (username/email and password). What is your action?

5. When you share files online (e.g. Dropbox, GoogleDrive, WeTransfer)

6. Imagine the situation that you meet a stranger online and that person asks you to meet also "in person"

1. When it comes to create a password for an online account you choose

Type of Question: single choice

Possible answers:

- *Something easy to remember (e.g. Birthdate, address, phone,12345678)*
- *A long and complex password (e.g. Ja32!!errTY*sAe)*
- *A combination of the above*
- *I use an application that creates passwords for me*
- *I don't have an online account*
- *No answer*

The above answers can be classified in relation to the achieved level of security as follows:

Password practice	***Security classification****
Something easy to remember (e.g. Birthdate, address, phone,12345678)	⊖⊖⊖
*A long and complex password (e.g. Ja32!!errTY*sAe)*	⊕⊕⊕
A combination of the above	⊕
I use an application that creates passwords for me	⊕⊕
I don't have an online account	
No answer	

** The minus (-) and plus (+) signs denote if the practice contributes negatively and positively to security respectively. The number of signs shows the measure of contribution (towards the negative or the positive) in every case.*

The following table contains the results of classification of the answers to the questions per country.

To calculate the values included in the table below, the number of times each answer was selected with the security classification of the relevant question.

*For example, for Cyprus, there are 9 participants answering this question. Of these 7 selected the answer "A combination of the above", providing (7*1)=7 positive points. The same process is followed in the case of negatively contributing answers. The values in column Total contain the results of the addition of positive and negative. Finally, the percentage of participants that selected the most negative and most positive answers are displayed.*

Country	Total	Negative Only	Positive Only	% of max negative answer	% of max positive answer
Cyprus	12	0	12	0,00%	11,11%
Greece	13	-6	19	16,67%	41,67%
Romania	97	-63	160	16,28%	20,93%
Slovenia	18	-42	60	25,45%	18,18%

2. When you receive an email from an unknown sender, most of the times

Type of Question: single choice

Possible answers:

- *You open the email right away*
- *You check the sender's address, the theme, if there is an attachment and if it looks secure. Then you open the email*
- *You delete the email*
- *You delete the email and block this address*
- *You don't use email applications*
- *No answer*

The above answers can be classified in relation to the achieved level of security as follows:

Email practice	Security classification*
You open the email right away	⊖⊖⊖
You check the sender's address, the theme, if there is an attachment and if it looks secure. Then you open the email	⊕⊕
You delete the email	⊕
You delete the email and block this address	⊕⊕⊕
You don't use email applications	
No answer	

** The minus (-) and plus (+) signs denote if the practice contributes negatively and positively to security respectively. The number of signs shows the measure of contribution (towards the negative or the positive) in every case.*

The following table contains the results of classification of the answers to the questions per country.

To calculate the values included in the table below, the number of times each answer was selected with the security classification of the relevant question.

*For example, for Cyprus, there are 9 participants answering this question. Of these 4 selected the answer "You check the sender's address, the theme, if there is an attachment and if it looks secure. Then you open the email", providing (4*2) =8 positive points. The same process is followed in the case of negatively contributing answers. The values in column Total contain the results of the addition of positive and negative. Finally, the percentage of participants that selected the most negative and most positive answers are displayed.*

Country	***Total***	***Negative Only***	***Positive Only***	***% of max negative answer***	***% of max positive answer***
Cyprus	*7*	*-3*	*10*	*-30,0%*	*11,11%*
Greece	*26*	*0*	*26*	*0,0%*	*0,00%*
Romania	*161*	*-30*	*191*	*-15,7%*	*7,75%*
Slovenia	*63*	*-27*	*90*	*-30,0%*	*16,36%*

3. Which of the following describes your activities in social media platforms?

Type of Question: multiple choice

Possible answers:

- *Only "followers"/ "friends" can see your posts*
- *Your email address, phone number, are shown in your profile*
- *Everyone can see your posts (i.e. public posts)*
- *You accept requests only from people you know in person*
- *No answer*
- *You accept requests from people you don't know in person but are friends of your friends.*
- *You accept requests from people you don't know in person*

The above answers can be classified in relation to the achieved level of security while using social media platform as follows:

Social media practice	***Security classification***
Only "followers"/"friends" can see your posts	⊕⊕⊕
Your email address, phone number, are shown in your profile	⊖⊖⊖
Everyone can see your posts (i.e. public posts)	⊖⊖⊖
You accept requests only from people you know in person	⊕⊕⊕
No answer	⊖

You accept requests from people you don't know in person but are friends of your friends.	⊕
You accept requests from people you don't know in person	⊖⊖⊖

** The minus (-) and plus (+) signs denote if the practice contributes negatively and positively to security respectively. The number of signs shows the measure of contribution (towards the negative or the positive) in every case.*

The following table contains the results of classification of the answers to the questions per country.

To calculate the values included in the table below, the number of times each answer was selected with the security classification of the relevant question. (The answers were only evaluated for those participants that declared use of Social media in a previous question).

*For example, for Cyprus, there are 8 participants answering this question. Of these 7 selected the answer "Only "followers"/"friends" can see your posts", providing (7*3)=21 positive points. The same process is followed in the case of negatively contributing answers. The values in column Total contain the results of the addition of positive and negative. Finally, the percentage of participants that selected the most negative and most positive answers are displayed.*

Country	***Total***	***Positive Only***	***Negative Only***	***% of max negative answer***	***% of max positive answer***
Cyprus	*36*	*-3*	*39*	*-7,7%*	*4,17%*
Greece	*36*	*-12*	*48*	*-25,0%*	*12,12%*
Romania	*170*	*-244*	*414*	*-58,9%*	*22,60%*
Slovenia	*116*	*-110*	*226*	*-48,7%*	*22,22%*

4. A Web page asks you to enter your credentials (username/email and password). What is your action?

Type of Question: single choice

Possible answers:

- *You enter your credentials*
- *You first check the URL/link(www.example.com) of the webpage and then you give your credentials*
- *I do not enter credentials, and leave / close that web page*
- *No answer*

The above answers can be classified in relation to the achieved level of security as follows:

Web practice	***Security classification***
You enter your credentials	⊖⊖⊖
You first check the URL/link (www.example.com) of the webpage and then you give your credentials	⊕⊕
I do not enter credentials, and leave / close that web page	⊕⊕⊕
No answer	

** The minus (-) and plus (+) signs denote if the practice contributes negatively and positively to security respectively. The number of signs shows the measure of contribution (towards the negative or the positive) in every case.*

The following table contains the results of classification of the answers to the questions per country.

To calculate the values included in the table below, the number of times each answer was selected with the security classification of the relevant question.

For example, for Cyprus, there are 9 participants answering this question. Of these 1 selected the answer "You enter your credentials", providing (1-3)=-3 negative points. The same process is followed in the case of positively contributing answers. The values in column Total contain the results of the addition of positive and negative. Finally, the percentage of participants that selected the most negative and most positive answers are displayed.*

Country	***Total***	***Positive Only***	***Negative Only***	***% of max negative answer***	***% of max positive answer***
Cyprus	*17*	*-3*	*20*	*-15,0%*	*11,11%*
Greece	*25*	*0*	*25*	*0,0%*	*0,00%*
Romania	*201*	*-45*	*246*	*-18,3%*	*11,63%*
Slovenia	*96*	*-15*	*111*	*-13,5%*	*9,09%*

5. When you share files online (e.g. Dropbox, GoogleDrive, WeTransfer)

Type of Question: single choice

Possible answers:

- *First you create a shared link and then you send the link to the people you want to have access to the files*
- *First you create an email-list with the people you want to share the files. In this way, they have to log in with their accounts and have access to the files*
- *I have no experience with file sharing*
- *No answer*

The above answers can be classified in relation to the achieved level of security as follows:

Email practice	***Security classification***
First you create a shared link and then you send the link to the people you want to have access to the files	⊕⊕
First you create an email-list with the people you want to share the files. In this way, they have to log in with their accounts and have access to the files	⊕⊕⊕
I have no experience with file sharing	
No answer	

** The plus (+) signs denote that the practice contributes positively to security respectively. The number of signs shows the measure of contribution in every case.*

The following table contains the results of classification of the answers to the questions per country.

To calculate the values included in the table below, the number of times each answer was selected with the security classification of the relevant question.

Since no answer contributes negatively, the relevant fields and their derivatives remain empty.

Country	***Total***	***Positive Only***	***Negative Only***	***% of max negative answer***	***% of max positive answer***
Cyprus		*12*			*22,22%*
Greece		*14*			*16,67%*
Romania		*165*			*19,38%*
Slovenia		*38*			*3,64%*

6. Imagine the situation that you meet a stranger online and that person asks you to meet also "in person"

Type of Question: single choice

Possible answers:

- *You say "yes"*
- *You say "no"*
- *You say "yes" and then you let a friend know the time and the place of the meeting*
- *You say "yes" and then you let a family member know the time and the place of the meeting*
- *You don't meet strangers*
- *You say "Yes", if he/she is a friend of a friend*
- *You say "no" and you inform your guardians*
- *No answer*

The above answers can be classified in relation to the achieved level of security as follows:

Email practice	***Security classification***
You say "yes"	⊖⊖⊖
You say "no"	⊕⊕
You say "yes" and then you let a friend know the time and the place of the meeting	⊖⊖
You say "yes" and then you let a family member know the time and the place of the meeting	⊖
You don't meet strangers	⊕⊕
You say "Yes", if he/she is a friend of a friend	⊖⊖
You say "no" and you inform your guardians	⊕⊕⊕
No answer	

** The minus (-) and plus (+) signs denote if the practice contributes negatively and positively to security respectively. The number of signs shows the measure of contribution (towards the negative or the positive) in every case.*

The following table contains the results of classification of the answers to the questions per country.

To calculate the values included in the table below, the number of times each answer was selected with the security classification of the relevant question.

*For example, for Cyprus, there are 9 participants answering this question. Of these 2 selected the answer "You say "no"", providing (2*2)=4 positive points. The same process is followed in the case of positively contributing answers. The values in column Total contain the results of the addition of positive and negative. Finally, the percentage of participants that selected the most negative and most positive answers are displayed.*

Country	***Total***	***Positive Only***	***Negative Only***	***% of max negative answer***	***% of max positive answer***
Cyprus	*16*	*-3*	*19*	*-15,8%*	*0,00%*
Greece	*-12*	*-37*	*25*	*-148,0%*	*0,00%*
Romania	*67*	*-86*	*153*	*-56,2%*	*2,33%*
Slovenia	*31*	*-28*	*59*	*-47,5%*	*3,64%*

3.4. Main findings of the survey

- *In general, there is a similarity among the types of online applications high-school students based in different EU countries use in their everyday life. In the cases of online games applications and online sharing files applications (which are listed as the third and first less popular applications in our results) we can observe differences in the responses between countries. E.g., a very small percentage of ~16% voted for online games in Greece while in Cyprus we have a higher a percentage of ~41%. Similar results were observed on the per country analysis on the question for the type of devices used by students. Based on these results we should be concerned whether some countries have special needs compared to others, a factor to be considered when developing the teaching materials and the methodology.*
- *Students feel more confident in most online activities, but their parents and teachers are more concerned about their level of confidence. In the per country analysis we can observe that Romanian and Cypriot students have slightly higher level of confidence on average, in the online activities we asked for, than Greek and Slovenian students, although the difference is not significant.*
- *We needed to measure if students do not only feel confident but also are confident in taking online actions in a secure and safe way. To do so we asked the students a number of questions to assess their cybersecurity skills and practices (See Combined Q.). By looking into the students' responses in these questions we can observe that students in general but also in a per country level failed to select the correct/best practice in all the questions. We obtain very low percentages of students selecting the best practices with no significant difference among the countries. These results show that the aforementioned confidence level of the students in the several online activities does not correspond to the reality since students do not follow the correct practices to ensure their safety.*
- *Students seem to be more confident in being aware of, being able to detect, avoid and handle the risks than their parents and teachers believe they are. Teachers look to be more concerned on the topic than the parents in general. But handling the risks seems to be the statement that also students mention they feel less confident about. These results show cybersecurity courses need to focus also on risk coping techniques to teach students not only to be aware of the risks but also to be prepared to respond to those risks properly. It is important to note that in the per country analysis in the responses received by teachers and parents from Greece and Cyprus, the teachers look to be more concerned than the parents, but Slovenian parents' perception matches the teachers one. This result might need further investigation since it might show a better collaboration practice between parents and teachers in Slovenia that can be adopted in other EU countries.*
- *The results of our study show that the majority of high-school students have experienced an online risk, proving that actions need to be taken to educate and support students in topics related to cybersecurity. Additionally, it seems that students do not share their risks' experiences with their parents and teachers, a sign that they do not trust them or talk about such topics with them but maybe with their friends or other adults. By including cybersecurity topics in the high-school courses or topics to be discussed, a collaboration between students, teachers and parents might be built in handling the online risks.*

- *Even if cybersecurity is covered in some high schools (based on teachers' responses), students and parents seem to be unaware of it. More effort is needed to promote these options and to establish cybersecurity courses in high schools.*
- *In identifying the 'hot' cybersecurity topics that are more important to discuss during a course with high-school students, the three groups of participants agreed on the topics of 'Being safe in online social media', 'Recognizing Fake Accounts', 'Ensuring Privacy'. The selection of these topics is in line with the very high percentage (93%) of participants mentioning that they use social media applications, but it is opposed to the level of confidence students mention they feel in those activities. More specifically the students replied to be 'confident' (on average) in being safe on online social media platforms and recognizing fake online content and 'neutral confident' in ensuring their privacy.*
- *In our per country analysis, we found differences in the responses given by the parents and teachers for the preferred methods/instruments to teach cybersecurity, which might reflect the different methods that are already used/preferred or feasible in each country. In general though there is an agreement that the cybersecurity courses need to be built with more interactive and gamified instruments that will engage the students to participate to, be more interested in and pay attention to learn.*
- *The conclusions drawn following the interpretation of the answers per questions are not heavily influenced by the country of residence of the participants in the process. Nevertheless, there are some points where customization of the teaching material could be applied, based on the country of residence which might serves better the special needs identified for a country.*

4. The Interviews

To complement and further understand the results obtained from the survey, we implemented a follow-up interview. The target audience of the interviews were high-school teachers, parents, and school management representatives. We reached our interviewees through the survey since at the end of it we were asking adult participants to give their contact details if they were willing to further contribute to this effort.

We collected all the contact information the participants shared with us and we sent an invitation email to ask them for their availability to participate in the interviews phase. ***Four*** *parents and* ***five*** *teachers replied positively to the interviews and then we scheduled the interviews. The nine interviews took place using online meeting platforms in June 2021. All the interviewers had sent the results of the survey and the list of the interviewer's questions to the interviewees beforehand in order to provide them material for discussion. The interviews were recorded with the consent of the participants and later were transcript-ed anonymously.*

The interview was structured in three main sections as follows:

- *Few words about the participants (5 questions)*
- *Existing Practices (7 questions)*
- *Questions on Future needs (2 questions)*

An in-depth analysis of the parents' and teachers' interviews follows on a per-question notion, after that we present the general comments on the interviews' results.

4.1. Parents' Interviews - Analysis

Few words about you

Q1: 'What is your level of knowledge in cybersecurity & cybersafety topics?'

Two of the participants replied with "basic" and two with "advanced"

Q2: 'How/ When/ From where have you gained knowledge in cybersecurity & cybersafety topics?' (e.g. during studies/ seminars/ special training/ other)

The two participants with advanced skills replied with "studies/special training/non-formal training/books and other relevant sources" and the two parents with basic skills replied with "none/other".

Q3: 'Are you confident in using/applying cybersecurity & cybersafety tools?
Which tools do you use?'
(Parental controls/ parental settings in TV/ Browser/ Application level)

The participants with advanced skills mentioned tools on mobile phones to limit the time of mobile phone usage, to limit the applications downloads, to limit the use of YouTube and other applications, and virus checkers.
A participant with basic skills in cybersecurity mentioned "parental settings on TV".

Q4: 'What is your children's age'? In what type of school do they go?'
14-17 years old -Lyceum

Q5: 'Were you or your child already a victim of a cybersecurity attack, identity, cyber-harassment, or similar?'

The participants mention experience with malware, spam with viruses. One mentioned that he/she is aware of any harassment and bullying in the child's school.

Existing Practices:

Q1: 'Is cybersecurity & cybersafety part of the curriculum in your child's school?'

Summary:

Parents awareness of the cybersecurity & cybersafety courses their children attend		
	Responses - Existing practices	***Comments and Suggestions***
Awareness level	*low-medium* *from what they heard from their child and teacher*	*parents didn't provide a lot of information* ***Reasons for not teaching cybersecurity in high-schools:*** *-no time* *-not a priority,* *-lack of knowledge (older teachers)* *- lack of adequate materials"*
Time spent	*2-3h per week (as part of the curriculum)* *throughout the year, no fixed schedule (as taught by the teacher outside the curriculum)*	*only one parent mentioned for the courses in the curriculum* *a parent suggests to have a week to raise awareness, ideally: 1 hour per month regularly*

	special courses or seminars are offered by organizations (e.g. police) outside the school's curriculum or time occasionally	
Cybersecurity & Cybersafety Topics taught	*cyberbullying, sexual grooming, privacy (as part of the curriculum)* *-safety harassment, bullying how to react in the case of harassment and bullying or any other attacks, privacy* *-Passwords, Spam mails, Downloads of applications and files, risks on using the mobile phones, software viruses*	*"social engineering" as a topic to discuss*
Instruments & Methods to teach	*presentation slides, execution of scenarios, giving real facts, over the discussion, paper materials*	****more efficient:** giving real facts, tailored campaigns in social media, led by influencers or other guests. Serious games with children's active participation to recognize in real situations potential danger, hands on tasks or sessions- interactive*

One participant mentioned 'I don't know if it is part of the curriculum', the other two participants replied with a 'no' and only one replied with a 'yes'.

We asked the participant that replied with a 'yes' the following questions to get further information on the cybersecurity courses that are part of the school curriculum:

- "How do you learn about it?

"my child told me"

- "How much time/teaching periods in a school year do they spend on these topics as part of the curriculum?"

“2-3 hours/week”

-"What topics do they cover in the courses?"

“cyberbullying, sexual grooming, privacy”

-"In which form the courses are taking place"

“presentation slides, execution of scenarios, giving real facts”

-"Which one is more effective in your opinion?"

“giving real facts”

To further investigate if cybersecurity is taught even if it is not part of the curriculum we asked the interviewees the following questions:

Q1A:‘Do their teachers teach these topics even if it is not part of the school curriculum?’

Two parents replied with a ‘yes’. And we asked them the following questions to get more information:

- "How do you learn about it?

1.“my child and told me” This participant didn’t provide further information for the questions below.

2.“my child and the teacher told me”

- "How much time/teaching periods in a school year do they spend on these topics as part of the curriculum?"

“It is spread throughout the whole year, but there is no fixed schedule. It is necessary to present those topics to children many, many, times. 1 hour per month regularly would be a good option.”

-"What topics do they cover in the courses?"

“Topics are mostly safety harassment and bullying but also cybersecurity. How to react in the case of harassment and bullying or any other attacks Passwords. Spam mails. Downloads of applications and files. Work with the mobile phone. Examples and cases.”

-"In which form the courses are taking place"

“Courses are taken in very different forms, from presentation slides over the discussion, paper materials.”

-"Which one is more effective in your opinion?"

“For kids would be the most effective tailored campaigns in social media, lead by influencers or other guests. Serious games with children's active participation to recognize in real situations potential danger.”

-"Complementary notes"

"We also had a seminar for parents. More of them would need additional knowledge as well. A good source for materials for parents, teachers, for everyone is https://safe.si/ (English - https://safe.si/english)"

For the parent replied with a 'no' for teachers teaching cybersecurity apart from the school curriculum, we asked the following questions to obtain further information and their views:

-"Why not? What is your view?"

"no time thus not a priority, lack of knowledge (older teachers), lack of adequate materials"

-"In your opinion, how much time is needed to be spent for cybersecurity & cybersafety courses?"

"for beginning as a block (like a week to raise awareness)"

-"What topics should they cover in the courses?"

"cyberbullying, privacy, spam emails, social engineering"

-"In which form the courses would be better to take place?"

"hands on tasks/sessions, be confronted and learn on examples, scenarios, based on real situations (confronted without knowing), interactive"

-"Which one is more effective in your opinion?"

N/A

Q2:"Are there any special 'seminars/workshops/presentations' for students outside the curriculum?"

"Yes, they are some outside school hours"

"Munich police offer some presentations at some local schools; children are more aware of cybersecurity than teachers."

We asked parents replied with a 'yes' further questions to get more information:

-"How much time/teaching periods in a school year does it spend on it? How much time is needed?"

"They are organised occasionally for children (students) and parents. Not so many in the last year because of Covid-19."

"the special workshops, seminars are outside school hours"

-"What topics are covered in the courses?"

"Safety, passwords, sexual grooming, cyber harassment, cyber bullying, danger on Internet in general"

"software viruses, fake accounts, strength of password, privacy, spam emails"

-"In which form are the courses taking place?"

"Classical lectures with presentations and slides"

"presentation-slides, paper material, discussion"

-"Which one is more effective in your opinion?"

"Giving real facts, execution of scenarios"

"presentation slides"

-"Complementary notes"

"Those courses, seminars are also aimed at parents."

Q3: 'Is your child interested in the cybersafety & cybersecurity topics?How do they share their interest on these topics?'

Summary:

Cybersecurity Interest of students	***Ways they Share this interest***
interest in how to be protected and act in risks cases	*-talk about these topics with their friends -sharing their experiences* **less possible to share that with their parents and teachers*

"Yes, as a user, to know how to act and protect himself, is well informed. Children share a lot of that info with friends and schoolmates especially if they are confronted with issues, they inform each other when they find out about spams or any other attacks.Discuss also with parents, but not so much with teachers."

"Yes. They discuss with parents and friends (in breaks as they might be confronted with issues), less with teachers."

Q4: 'Has your child shared with you any risk he/she faced online or how do you motivate them to share their experiences?'

Summary:

Sharing risks experiences with parents	*-a child shares with the parent their own or their friends experiences*

	-motivate the child by having discussions on how to be protected against online risks
Communicate the experiences with the schools	*-only in cases that the risks is related to school* *-school's social services are involved more in cybersafety issues rather than cyber security*

"He told me what he experienced and what he got as info from his friends"

"no big issue yet; hope child will share with parent"

-"If yes, what did you do?

"I am teaching him how to protect himself, so he is coming to me when he needs help.

-"Did you share this info with the school/teacher/any other official authority?

"There were no cases that it would be needed to give the info from my side to the school. Other parents are even less interested according my experiences

"Depending on the issue (if related to school) yes share."

-"Complementary notes"

"The school's social service takes care of security cases that relate mainly to cyber harassment and cyberbullying"

Q5: 'From the results of our survey it seems like students and parents are not well aware of the cybersafety & cybersecurity courses in school, while the majority of teachers stated that there are such courses in the school curriculum.'

Summary:

Reasoning the awareness gap between parents, students and teachers	*-not enough time spent on these topics to raise the awareness of parents and students* *-students don't pay attention* *-if it is embedded in other courses then parents/students don't recognize it*
Ways to eliminate that gap	*-explicitly inform the parents* *-cybersecurity courses must be obligatory part of the curriculum* *-spend more time on these topics* *-involve both parents and students in the courses*

-"Why is that happening, in your opinion?

"Parents are not aware of all the lectures that children have. Children are neither aware that they have cybersecurity lessens if they are a part of other lectures, while teachers are aware of all this, so the discrepancy appears

"formulation of cybersecurity at school can be interpreted very broadly, teachers even addressing a small part (e.g. privacy) of the topic would reply yes; lot of students do not even pay attention"

"3h/week are not enough for learning this"

-"How can this change?

"Parents must be explicitly informed about cybersecurity lessons or they must become obligatory part of curricula."

"has to become part of compulsory curriculum ; as long as mandatory will be dropped due to lack of time "

"the schools need to spend more hours on these topics learning / practice"

-"Complementary notes"

"Involvement of parents in cybersecurity teaching together with children. Children believe that they know everything, because they are digital natives."

Q6: 'Was the cybersecurity ever discussed in your child's school at meetings between teachers and parents? '

Summary:

Are cybersecurity topics discussed during teachers and parents meetings?	*No*
Will cybersecurity events be useful for parents?	*Yes, there is lack of parents' knowledge and skills regarding the digital world in comparison with their children, it is important to educate them.*

"Actually not . If there is any problem, the discussion is done between the child, parents and social worker at the school. This info is not spread further to other parents."

"the only issue privacy when revealing data / forms outside the school"

"NO"

-"Would discussions/info events for parents be useful/preferable?

"Yes, it would be very much needed. Most parents do not have this knowledge and most children know more about computers than their parents. Better to say they believe that they know."

"information would be useful to make parents aware; parents are not enough interested to take care of the issue themselves"

"yes, it would be useful"

-"Complementary notes":

"Parents' education in cybersecurity and cybersafety is very important."

Q7: "Students seem to feel more confident in detecting, avoiding and handling online risks than their parents and teachers think they are.What do you think about that? "

Summary:

Reasoning the difference in the parents'/teachers' perception of the level of confidence students have	*-students believe they are confident but they are not - why?* *- they haven't experienced any real risk* *- they spend a lot of time online and discuss about risks only with their friends* *-teachers do not trust the students, they teach them but don't get feedback*
Reasoning the fact that students feel less confident in detecting and handling the risks?	*-students may did not experience any risks so they can't measure how confident they are in this*
Is avoiding risks covered more?	*-Yes, campaigns provide more material in how to avoid the risks*
How to teach handling the risks better?	*-training exercises on the basis of real examples in a controlled environment* *-short videos to explain the risks with examples* *-real hand-on session, real exercised* *-game like "escape rooms" - find way out of problematic situation"*

"Children believe that they are confident, because they probably did not experience any real attacks, so their judgment is not real."

"teachers do not trust students; students think they know more than teachers; they do not speak about the topic; usual flow of information from teachers to students - there is no feedback loop at school "

"Because they are using internet many hours per day and they talk with each other about any problem"

-"Students also stated that they feel less confident in detecting and handling the online risks."

"Mostly they do not have real experiences so their judgment is probably in this case real."

-"Do you believe that avoiding the risks is more covered in the existing courses / workshops/campaigns?"

"No so much in courses maybe in some existing campaigns but outside schools "

"yes"

"campaigns covered this topic more than others"

-"How to teach detecting and handling online risks to be more effective?"

"Training exercises on the basis of real examples in a controlled environment would bring children the feeling of a real attack. Another possibility would be short videos to explain the same.

"idea of the real hand-on session, real exercised; game like "escape rooms" - youth like to play such games; you have to find way out of problematic situation"

-"Complementary notes"

"Children do not like to read so other media must be used."

"kind of vaccination in cybersecurity" - "cybersecurity antibodies in a mind of people" - students get them when practicing cybersecurity relevant situation and later know how to react; e.g. sending email similar to school one but opening might cause a small problem - but thus students can get aware not to open each email and know how to recognise fakes "

Questions on Future Needs

Q1:"Do you believe that cybersafety and cybersecurity topics must be discussed

only during the Computer Science classes or also in special seminars/workshops (during the school time or not) are also required?"

Summary:

Cybersecurity as part of the curriculum or as special seminars/workshops outside school curriculum?	*Both are needed,* *-Add these topics in ICT classes but also in other courses where it is applicable,* *-Seminars and workshops must complement the courses*

"They must be discussed during the Computer Science Classes, but also during all other classes in which the connection to cybersecurity and cybersafety can appear - for example a class about sociology should also discuss cybersafety and cybersecurity in social networks. If it is possible to connect the class with the cyber topics, it should be connected. Also other seminars and workshops would be welcome."

"On the long run cybersecurity must be part of standard curriculum (address ministries, politics, at national and EU level), computer science classes; teachers must be forced to teach cybersecurity; teachers must be provided with respective teaching / exercise materials

"Also in special seminars/workshops (during the school time or not) are also required"

-"Complementary notes"

"It is important to address cybersecurity and cybersafety interdisciplinary along with the areas that emerge as an example. ICT is used everywhere but it is not safe. We have to work on awareness and knowledge of all involved stakeholders (children, teachers, parents) and

Q2:"What would you change in the existing practices on teaching cybersafety & cybersecurity in your school?"

"all of these to be improved"

-topics *"introduce social engineering (not high awareness on this issue)"*

-methodology/form of teaching material

-awareness

-motivation *"YES"*

-time-wise *"YES"*

4.2. Teachers' Interviews - Analysis

Few words about you

Q1:"Are you a generic teacher/teacher of informatics/other?"

Three of the interviewees were computer science teachers, one was the school's director of Foreign Languages, and the other was a teacher in business administration.

Q2:"What is your level of knowledge in cybersecurity & cybersafety topics?"

One teacher mentioned basic to advanced level, three teachers mentioned advanced level and only one teacher mentioned basic.

Q3: "How/ When/ From where have you gained knowledge in cybersecurity & cybersafety topics?"

Summary:

Teachers interviewees' source of knowledge in cybersecurity & cybersafety topics
-Personal interest (seminars, trainings, talking with other professionals) *-Mandatory Trainings* *-During studies* *-Experience in IT industry*

Participants responses:

"No formal training, individual extensive research on the topics by reading and talking with other Cybersecurity professionals - also because she is a parent"

"Seminars and training(Microsoft Show Case School) provided from the school, and also on her own interest for professional development"

"a little bit during studies, most during preparations for own lectures; own time personal interest"

"Public Seminars about internet-safety such as https://blogs.sch.gr/internet-safety/archives/1196. Individual research and interest in cybersafety. Master-thesis related to the effect of the internet-use on high-school students"

"Seminars. 20 years of experience in the IT industry. Recently, he is working as a Professor in a public high school. He also provides online courses about cybersecurity."

Q4: "Are you confident in using/applying cybersecurity & cybersafety tools? Which tools do you use?"

Summary:

Parental controls used by teachers interviewees		
at home	***at school***	***generally***
-basic parental control through the browser *-filters/ time control/ MAC address control*	*-block inappropriate sites* *-banned mobile phones for students* *-WIFI only for school stuff students are only allowed to access the Web -through school computer devices* *-(private school) students use ipads - restriction in areas out of school purposes*	*-antivirus* *-VPNs* *-prefer other methods and not parental controls or tools*

Participants responses:

"very basic - parental controls at home/ through the browser/ not very confident - her husband uses filters/time control/ MAC address control / in school blocking websites that are not appropriate, banned mobile phones/ there is WIFI to the stuff of school but not for the students, Students are not allowed to use their mobiles or WIFI during school time, they access the Web through school's computer devices"

"Yes, parental controls for her kids, restriction in the areas out of school purposes for the ipads used by students during school time, IT department of school is responsible of this, other teachers and parents are informed about that practises"

"confident in using antivirus programs"

"He feels very confident to use cybersafety tools but he is mainly using interactive seminars and games in order to teach cybersafety to his students and to their parents. Peer tutoring. Also, volunteering work/seminars in Elementary schools."

"Yes. Parental control tools and Add-ons for Firefox (home network). VPNs."

Q5: "What is your students' age? In what type of school do you teach?

The students ages the interviewees teach are in the range from 12 to 19 in public Gymnasium or Lyceum schools, and Private high-schools

Existing Practices:

Q1: "Is cybersecurity & cybersafety part of the curriculum in your school?"

Summary:

Cybersecurity courses as part of the curriculum	
Time spent	*-few hours per year in specific classes* *-some teachers use more time on teaching these topics outside the curriculum* *- a private school teacher said that it is taught in many semesters*
Topics	*The topics vary regarding the type of school, the school year of the students, the direction the student chose in their studies, the interest of the teacher.* *Some of the topics mentioned:* ❖ *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*
Instrument and methods	❖ *videos for cyberbullying* ❖ *discussion* ❖ *show them examples of risks* ❖ *topics are covered in school books* ❖ *work in teams on specific topics, learn and explore themselves and make presentations afterwards* ❖ *Peer tutoring* ❖ *Interactive seminars* ❖ *slides* ***more effective:*** ❖ *videos* ❖ *discussion* ❖ *do a research all together* ❖ *sharing personal or friend's experiences/stories* ❖ *learning by doing* ❖ *Peer tutoring* ❖ *Interactive seminars where older students teach younger students.* ❖ *Documentaries about sexual grooming* ❖ *Theater games for students - role playing.*
Comments	*"use extra time (e.g. end of the day when students are tired) to discuss this topics as they are more interesting and light for discussions"*

All the teachers replied with a yes, one teacher mentioned that only cybersafety is taught in school curriculum, one mentioned that it is well included within other subjects in many semesters, and one mentioned that it is only taught for first high school class students.

We asked the following questions to obtain more information:

-"How much time/teaching periods in a school year do you spend on these topics as part of the curriculum?"

"first class of secondary - 2 periods, other classes 0 based on the syllabus / she is also taking more periods "

"in many semesters (e.g. in 1st year 3 weeks), but mainly 4th and 5th year;"

"Officially, 4-5 hours per year. Plus, Volunteering work/ seminars for students and parents Officially, 2-3 courses/ first year (A class) of Gymnasium. He voluntarily teaches his students some topics related to cybersafety and cybersecurity (2 courses, first and last week of the school year)."

-"What topics do you cover in the courses? "

"syllabus: cyberbullying, spam,phishing/ viruses were before some years part of the syllabus but now no "

"strong passwords in 1st year, 3rd year antivirus programs, 5th year data encryption and data safety, safe data transfer; those students choosing e-business and telecommunication (from 3rd to 5th year) learn more on cybersecurity e.g. protection of personal data

All these topics even if some of them are not part of the curriculum. Volunteering work. strong passwords, sexual grooming, cyberbullying, phishing, fake accounts in social networks

-"In which form the courses are taking place?"

e.g. presentation-slides, paper material, discussion, hands on tasks, videos, execution of scenarios, giving real facts

"videos for cyberbullying - teens committing suicides after being bullied, discussion, show them the malicious software she receives by sharing screen and looking at the mail and explain how to avoid:

"classical teaching setup, topics are covered in school books, but students are asked to work in teams on specific topics, learn and explore themselves and make presentations afterwards, Videos, Peer tutoring, Interactive seminars"

"Short YouTube Videos, discussion, slides"

-"Which one is more effective in your opinion?"

"videos, discussion, do a research all together, sharing personal or friend's experiences/stories, no presentations, no handouts because students need to actually see the facts, they won't read a book or paper material "

"discussions, learning by doing "

"He believes that the most effective approach is Peer tutoring and Interactive seminars where older students teach younger students. Documentaries about sexual grooming (effective for students and parents)."

"Discussion"

-"Complementary Notes"

"when students are tired with the syllabus topics, she uses this time to show them these interesting topics"

"teachers would like teaching software (no books or paper material) for practical exercises Theater games for students (max 25). First, the students watch a video about cybersafety, for instance the story of a young girl who has been harassed online (sexual grooming or cyber-bullying). Then, the students are playing the girl's role trying to alter the end of the story."

Q2:"Are there any special 'seminars/workshops/presentations' for students outside the curriculum? "

Summary

Cybersecurity courses outside the curriculum	
Time spent	*-on a yearly basis* *-many times throughout the year (private school teacher, the school has cybersecurity&safety integrated in its mission)*
Type of seminars	*outside specialized organizations visit schools* *-police officers* *-psychologists* *-telecommunication companies* *-safe-internet day -campaigns* *school IT specialists presentations* *thematic weeks with relevant topics competitions on*
Topics	*-how to be safe online* *-cyberbullying* *-fake accounts* *-cyberprivacy* *-viruses* *-sexual grooming*

	-spam mails **mostly cybersafety topics and not cybersecurity*
Instruments and Methods used	*presentation* *videos (with authentic stories)* *statistics, real facts* *discussion (for real events and facts)* *Q&A* *digital & paper material* *online surveys* *participate in competitions* *webinars* *student projects (AQA)* ****most effective:*** *presentation, showing the real videos, videos, and ask students for personal stories to share*
Comments	*'how active a school is' also depends on the principal of the school* *teach different topics in different ages of students* *parents, teachers must be taught too*

"YES, once a year Cytanet organizes seminar on how to be safe online (only two students can participate except this year because of covid 20 students online)"

"Yes, School IT specialists at the beginning of the year and throughout the year police officers, psychologists give talks, thematic weeks with relevant topics (cyberbullying, fake accounts, cyberprivacy,viruses), competitions on cyberbullying (sexual grooming))

"no, don't know that there are any"

"NO"

"No. Only once a year seminar, safe-internet day."

-"How much time/teaching periods in a school year does it spend on it? How much time is needed?"

“once a year Cytanet organizes seminars on how to be safe online, police officer or a specialist give talks once a year one-two period for the whole school”

-"What topics are covered in the courses?”

“how to be safe online, cybersafety not cybersecurity”

“spam mails, sexual grooming, viruses (especially to high school students), in general cyberbullying, cyber privacy”

-"In which form the courses are taking place?”

“presentation, videos, statistics, discussion, Q&A”

“presentations,paper material (not during pandemic)-> online surveys, digital material, videos with authentic stories, real facts, participate in competitions(students won with creating a site related to sexual grooming), discussions for real events and facts (e.g. incidence of students sending naked pictures of their teammates -> discussion for cyber privacy), webinars, student projects (AQA) - research and answering questions on specific areas- a student worked on cybersecurity”

-"Which one is more effective in your opinion?"

“presentation, showing the real videos and it is effective because there is a person coming to the school (not just your teacher), the students "get scared"/being more aware but the discussion there is not that effective (too many students) videos (the power of the image) and ask students for personal stories to share”

-”Complementary notes”:

“it depends on the principal of the school, they sometimes invite people (specialist, police officers) / cybersecurity must be simplified and also be taught / because the whole school is there is difficult for them to participate and ask questions/ enrich the curicullum and also have the extra seminars”

“teach different topics to different age students, give more data, facts, general they pay attention to these topics since their school use the technology in their everyday activities, they need to train students, parents and teachers in order to be able to say they succeed in implementing the vision and mission of the school, there are teacher trainers who teach other teachers - how to avoid problems with their school accounts”

Q3:"How do you ensure that the students understood cybersecurity and safety topics? Please provide details."

Summary

Assessment of the student's understanding on cybersecurity and cybersafety topics
-when students talk about it after the discussions in the class/seminars/etc. *-just by looking at their eyes* *-when quiet students participate in these discussions* *-Games* *-Quizzes as digital forms* *-Assignments* *- Discussion* ****Comments:*** *-standard quizzes,tests, and assignments will add more pressure on them - undesired*

"when having the same students the next years the students express their experience during the courses given before, no testing on these topics by a quiz, no assignments (too much pressure/no time because of the other topics in the syllabus), you can see in their eyes if they understood or not, quiet students also participate so you can see the impact one them"

"Games / Quizzes as digital forms/ Assignments / Discussion"

"at school presentations and discussions but no classical examination if they have understood or not "

"Discussion, assignments, peer tutoring

"Mainly by discussing with students"

-"Complementary notes":

"They don't' have related problems that other schools have"

Q4: "Based on your experience in the classroom, are students interested in the cybersafety & cybersecurity topics?"

Summary

Are students interested in cybersecurity and cybersafety topics?	*yes*
How they show that?	*-by asking questions* *-by sharing experiences* *-by discussing* *-by bringing back the topic to the class* *-by showing more interest than in other courses* *-by paying attention* ****Comments:*** *if these topics become part of the curriculum, it might affect the students' interest negatively*

"Yes"

"Yes, topics are interesting for pupils, enjoy learning about cybersecurity as they can be personally affected (some faced loss of data, passwords, phishing, spam, cybermobbing)

"Yes".

"Yes, are very interested in Cybersecurity/Cybersafety topics"

"Yes"

-"How do they show their interest?"

"Absolutely, they pay attention, ask questions, sharing experiences, discussing, most interesting class of the year, bring back the topic to the class"

"A lot, you can see it after watching related videos also they share experiences with the teachers and in the class"

"Actively participate in discussions"

"Generally, the students worry about their safety online even if they do not openly admit it."

-"Complementary notes":

"if you give the topics as lessons (with homework, tasks) then they might less interested"

Q5:"Have any of your students shared with you any risk he/she faced online?"

Summary

Do students share their online risks experiences with their teachers?	*-rarely* *-simple stuff-small problems* *-they most likely report their friends' experiences but not theirs*
How to motivate them to do so?	*-during discussion* *-ensuring the confidentiality* *-build trust with the students*
What is the protocol if a student shares an experience?	*-strict law from the ministry of education->you need to report it immediately* *-talk to the principal,then to the school counselor, notify the authorities* *-a private's school protocol: student's mentor(a teacher) -> psychologist -> director of studies->parents* *-suggest reporting the incidence to specialized organizations* *-handles the problem and advice the student if the student is not in danger* **two of the teachers didn't know about any protocol*

"Rarely, if it is something simple they might admit it otherwise they are embarrassed, share experience of their friends(not themselves) personally to the teacher in break time"

"Yes, they share experiences"

"generally these problems not well discussed with teachers, this teacher has good relationship with own class to discuss"

"Rarely share their experiences. For instance, a 12 years old girl had been harassed online by her boyfriend (one year older than her). The teacher was not informed about this incident directly by the student but by the non-governmental organization to which the parents reported the incident."

"Yes, two of his students. One student reported online harassment and the second one that his account (of an online game) has been hacked"

-How do you motivate them to share with you their experiences?

"during the discussions in the class"

"they know it's confidential, there is a mentor for each student where they can go and share any problem, they can go to the school psychologist"

"With discussion. He tries to build a relationship of trust with the students so that they can talk openly about these incidents."

"Discussion"

-"What is the protocol if a student shares with you a bad experience he/she had online?"

"strict law from the ministry of education, there was a seminar, if you are aware of a student in danger you need to report it immediately, talk to the principal,then to the school counselor, notify the authorities, try to get the students and convinced them to tell their parents/the school need to tell to the parents"

"protocol= mentor -> psychologist -> director of studies and parents. if it's something not disturbing and dangerous that she can handle she can give advice (teachers got specific training in cybersecurity), if not the student should go to the psychologist of the school, if it is a really important issue they go to the director of studies, parents are also notified if it is something outside the capacity of the school"

"not really"

"There is an official protocol in some schools (schools that have an Educational Counselor). In Practice, mainly via https://saferinternet4kids.gr/nea/hotlines/ (Non-governmental organization) where the parents or the students can submit their complaint"

"No. From what he knows there is no protocol"

-"If there is no protocol, what are you doing with this info? "

"Discussion. Handle the problem discreetly. Advises the student to consult a psychologist or make a complaint to the police cyber-crime division."

-"Complementary notes"

"encourage the students to talk to an adult/relative/teacher/parent and not to their friends to find help/ it is very difficult to get the student who is involved to the risk because their friends are sharing that with the teacher/ there are no school psychologists"

"there are not serious issues until now because of the effort given by the school to fight these topics"

"in some topics (e.g. cybermobbing, cyberbullying) professional organisation to help would be useful"

Q6: "From the results of our survey it seems like students and parents are not well aware of the cybersafety & cybersecurity courses in school, while the majority of teachers stated that there are such courses in the school curriculum.Why is that happening, in your opinion? "

Summary

Explaining the gap	*-parents know the topics taught in their children' school only if it is labeled in their curriculum* *-non-CS teachers have no idea of what is actually taught in Computer Science course* *-students mentioned no even if they attend some courses* *-teachers wanted to support their schools*
How to change that?	*-increase awareness to the parents and teachers* *-teach the teachers* *-involve parents in the discussion* *-parents must show more interest in what their children do in school*

"the parents are the problem, if cybersafety and security is labeled as a lesson in the school curriculum or their kids are taking part in a project then they say yes, it is a part of the school curriculum"

"teachers are not well informed, especially non-CS teachers have no idea about what is being taught in the CS lessons, the same happens with the parents"

"cybersecurity and safety are very new issues, older teachers are not aware of relevance and do not feel confident to teach that"

"He believes that these diagrams do not reflect reality. Students may have answered "no" while they may have done seminars. He believes that 80% of parents do not know if seminars are held. Teachers want to support their school and they answer "yes" He believes that the lessons are so few and the students practically did not realize that they were doing seminars in cybersafety/cybersecurity. He believes that in the end cybersafety/cybersecurity is not really taught in highschools."

-"How can this change?"

"increase awareness to the parents and teachers, seminars, "teacher education days" there are seminars there that are related to different topics -> inform them what is going on"

"we need to involve parents in the discussion actively, it is a general problem- parents must ask their kids what they are doing at school, ask more specific questions on these problems e.g. instead of asking if these topics are part of the school curriculum ask them if they have ever discussed about cybersecurity topics with their kids and the related activities in school"

-"Complementary notes" - "other teachers might talk about the internet/technology but do not give solutions because they re might not being confident in this topics"

Q7: "Students seem to feel more confident in detecting, avoiding and handling online risks than their parents and teachers think they are. What do you think about that?"

Summary

Explaining the difference in confidence in detecting,avoiding and handling online risks students have VS their teachers and parents' opinion	*students think they are confident while they are not, they can't handle the risks, they have no experiences*
Is avoiding risks more covered in existing courses?	*- yes, no much time is spent so other topics might not be covered* *-handling the risks is more difficult for the students to assess their confidence in, since it has to do with 'external powers' too*
How to teach detecting and handling the risks in a more effective way?	*-increase teaching periods* *-increase awareness of parents and teachers* *-school system must support these topics* *- give parents instructions to set the safety settings at home* *-with showing online risks examples* *-educate the teachers in regular basis*

"disagree, they think they are confident, they are teenagers and feel that they know everything, it is dangerous that they think they are confident in this. this is a characteristic of the youth, younger people are more optimistic, (they believe that they know, they can detect, they can handle), parents are always more concerned, but teachers they should not have this response, they should be confident that they can teach these topics and be more engaged to develop themselves and help their students to be more confident"

"as teachers observed that students often overestimate own skills"

"While students believe that they can handle the risks, in practice they are not so experienced."

"Students, while they think they can handle the risks, in practice they can not."

-"Students also stated that they feel less confident in detecting and handling the online risks. Do you believe that avoiding the risks is more covered in the existing courses/workshops/campaigns?" "yes, it might be the case. Too few periods are spent to teach the topics so there is not enough time to give/absorb all the information"

"to be cautious and avoid the risks it has to do with yourself so they can say they are more confident but to detect and handle is also depend on others, when you are expose you might don't know to whom talk to. schools that do not provide mentors and psychologists or the experience to deal with these -> so students don't know to whom they can talk to. Detecting - a child cannot be so sure on how to detect the risk, even grown ups might not detect "

“partly”

-How to teach detecting and handling online risks to be more effective?

“increase the teaching periods in each class to teach the topics, increase awareness for the parents and teachers, the school system is not supporting these topics, parents need to be more involved - give them instructions to set the safety settings at home / actual material with instructions how to apply the settings/ or to actually be protected/ phone numbers to get helped - here give handouts”

“with examples, show videos and say this is an online risk”

“first to properly educate/train teachers; include more cybersecurity topics in regular curriculum (in Austria there is an update every 10 years), because if it is part of curriculum will boost more training offers for teachers”

“ See the aforementioned teaching methods”

"YouTube videos together with discussion and some slides. Real world use-cases regarding phishing. To learn how to install Firefox add-ons. Extra courses in the curriculum"

-”Complementary notes”:

“good example, training platform funded by EU: https://europa.eu/taxedu/home_en”

Questions on Future Needs

Q1: "Do you believe that cybersafety and cybersecurity topics must be discussed only during the Computer Science classes or also in special seminars/workshops (during the school time or not) are also required?”

Summary

Teaching Cybersecurity & safety topics must only take place in CS classes or also in special seminars/etc?	*-Both, as a combination.* *-Not necessary to be part of the curriculum.* *-Throughout all the years a student is in school* *-Only CS teachers must give those courses since other teachers are not trained*

“both, taught in CS classes and workshops/seminars a combination it is a society thing so it must be everywhere No it does not needed to be discussed during the class time in the curriculum but special workshops and seminars not only for the teachers, but also for the students and the parents”

“combination of both ; there must be a general frame, seminars workshops good to emphasise special topics”

"Both. Mainly with seminars and actions outside the curriculum"

"Only during the Computer Science classes, because the teachers of other specialties themselves do not have the knowledge (and the technical training)"

-"Complementary notes:"

"all related activities must happen throughout the years that a student is in school, not only once, build the confidence, the culture of the student. Schools should have that as a mission and not just part of the curriculum"

"example of new commercial secondary school with focus on "management in cybersecurity" (it is new pilot in austria starting september 2021, new special curriculum is tested): https://www.haktamsweg.at/management-cyber-security.html (contact can be established for discussions)"

Q2: "What would you change in the existing practices on teaching cybersafety & cybersecurity in your school?

Summary

Topics	*-strong passwords* *-spam* *-malicious software* *-how to detect dangers* *-cyberbullying* *-online shopping* *-hacked accounts* *-sexual grooming* *-data transfer* *-encryption* *-data loss* *-the problem of time students spend playing online games - chat-rooms of online-games* *-emphasis on TikTok*
Instruments methods used	*-project in each cybersafety topic* *-a full day with workshops on cybersecurity and cyber safety* *-bring people specialist to train the teachers* *-interactive* *-ask students to work in groups, do research on these topics and make a presentation*
Awareness	*-make it stronger*

Motivation	*-government should include the topics in the curriculum* *-teachers must be motivated to improve their professional skills*
Time-wise	*-more time is needed*
****Comments***	*-school/teachers must be close to their students* *-create different material for educating:* *-students,* *-teachers* *-parents*

"everything, nothing is there"

"For her school nothing, it is incorporated in the school mission. All the schools should show to the students how to protect themselves within the year (cyberbullying) to make them aware of potential dangers/threats. Cybersecurity and cybersafety is now very related with the way we give education (pandemic) so we should make sure that we protect the students."

"Everything, more or less. Interactive actions outside the curriculum"

-"topics"

"strong passwords, spam, malicious software, how to detect the dangers"

"cybersafety, cyberbullying, other threats that they might face - especially for high school students:online shopping, hacked accounts,sexual grooming"

"all topics mentioned in survey are important, also data transfer, encryption, data loss, virus on smartphone"

"Students do not create strong passwords and they download files while you should not. All the top-5 (based on teachers' replies) should be taught. Also, they should emphasize the problem of time students spend playing online games. Emphasis on TikTok. TikTok is the most popular platform among young people. Also, the chat-rooms of online-games (danger of sexual grooming)."

-methodology/form of teaching material

"project in each cybersafety topic, a full day with workshops on cybersecurity and cyber safety, bring people specialist to train the teachers"

"interactive (learning by doing, training platform for students to make and test, experience in safe environment, experiment with given theoretical part) and give students possibility to discuss"

"Powerpoint presentations by the teacher are not effective. It might be effective if the students work in groups, prepare the slides and make their own presentation. In other words interactive presentations/seminars/work"

-awareness

"make it stronger"

-motivation

"government should try to implement topics like these in the curriculum teachers must be motivated to improve their professional skills by taking cybersecurity&cybersafety"

-time-wise

"more time - new curriculum must be redesign within all years, government should try to implement topics like these in the curriculum"

"within the year give seminars, etc."

"in own school there are already time frames to discuss the topic"

-"Complementary notes"

"different material on educating the teachers, and the material that will be used to teach the students, also material for parents must be created"

"school should make sure that they are close to students, they can listen to them, teachers must understand what is happening to them"

4.3. General comments linked to the interviews

Sample size: *The first thing to note about CONCORDIA's campaign for teachers, parents and students is the small sample size of collected answers and even smaller one of arranged interviews. This is an indication that this target group cannot be easily reached through the usual means of communication. Even though there is a concern for cybersecurity / cyber safety among parents and teachers, they do not seem to preemptively search for relevant content. Thus, we would argue that online campaigns (which almost always follow personalized preferences) is not the optimal way to reach this audience. More coordinated actions with campaigns and emails through school networks might be a better solution, however these campaigns usually need the approval of a government agency (e.g., ministry of education). Also, the number of people that accepted to give an interview is considerably low, showing the participants' reluctance to further engage with an online survey. Due to the small sample size and to be able to do this, this analysis provides general observations on the existing status of cybersecurity in schools and does not try to explain any personal opinions.*

Diversities: *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. For the latter, the reasons are the lack of knowledge/experts/materials to teach such courses, giving the impression that there is also a lack of interest by the school to deal with the matter. External courses (outside school hours) can be found in some cases, but these are independent efforts (e.g., Munich police) and not a common practice across the EU. Another aspect has to do with handling incidents (e.g., online harassment). Answers indicate that there is not always a protocol to follow and for institutes that have one, there are many differences about the actions to be followed. Finally, participants gave different answers when asked about their opinion on what should be changed in existing schools, courses, or curriculum. There were answers stating that considerable changes are needed, as well as an answer that strongly supports their school's current curriculum.

Common views: *Despite the many differences on the current status as well as suggested actions to promote cybersecurity / cyber safety in education, there are various topics that given answers seem to converge. All participants agree on the importance of cybersecurity in education and the need to form a long-term mission instead of 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 is that all parents and/or teachers believe that students overestimate their skills / 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 what their parents/teachers think. This can be attributed to the generation gap; however we argue that in many cases younger people are more familiar with technology and can in fact be capable of better understanding these risks.*

Conclusions: *Concluding this analysis, we should highlight the following points. There is a high interest in cybersecurity among teachers, parents and students, however, there seems to be a gap between the education and the cybersecurity experts' community. 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 large diversities between cybersecurity education across institutes (current state of play), but they all seem to agree on the necessary steps that must be done onwards (future strategy). Indicative example is that all participants agree on the need for interactive courses on cybersecurity. Another aspect that has been identified in this analysis, has to do with the lack of coordinated actions and initiatives across the EU to support schools and students. Currently, cybersecurity education is either provided as an additional topic inside computer science courses or through independent activities organized by external providers and agencies (e.g., Munich police). Furthermore, the lack of central coordination and well-defined protocols and strategies also affects the ability to identify and respond to incidents.*

5. Additional research

CyberSecurity and gamification of cybersecurity training: summary of the report[2]

The field of cyber security is undergoing many dramatic changes, demanding the organizations to embrace new practices and skill sets by their employees. With the recent high-profile attacks, training in cyber security became necessary in most institutions, including educational, commercial or other types of organizations. New studies in this field have shown that cybersecurity education requires more innovative educational approaches like use of cyber ranges and serious games that have proven the cyber skills training to be more effective. The cyber security education seems especially well-suited for use of serious/educational games as they enable interactivity in the training process and lead the learner to take decisions about preventing attacks or protecting the site or themselves in an environment similar to real life. It is very indicative that the Concordia survey among the high school students, mentioned along with videos, mentioned the games as a desired vehicle for learning and training cyber security skills. Many cybersecurity games developed to be used in education are currently available on the market, however not all are designed with very clear educational goals and target audience. This summary is based on the report that analyses a selection of cybersecurity games available on the internet dedicated to training and education, classify them according to the TULIP classification and present the results of the evaluation of 12 selected games in a search for games that are suitable to be used in high school student education. The set of games was selected according to their properties and popularity. The technical and learnability properties found based on the game playing are collected in the enclosed table below.

The following CyberSecurity games were played and evaluated, all of them are available on the web:

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

The study found that the games differ in their purpose, educational goal and as well in the technical properties. Some of them are dedicated to single player and some of them involve

[2] JERMAN-BLAŽIČ, Borka. Changing the landscape of cybersecurity education in the EU : will the new approach produce the required cybersecurity skills?. *Education and information technologies*, ISSN 1360-2357, [in press] 2021, 26 str., doi: 10.1007/s10639-021-10704-y

multiplayer strategy where the player teams compete against each other, head-to-head in order to take control or maintain control of a computer network. Most of the selected games for evaluation are dedicated to players from the industrial environment but some of them are applicable for training learners from the wide public interested to learn more in order to become more aware about the cyber security threats. Special attention within the set of the studied games was paid to the learnability of the game and suitability for training or education of high school students and their teachers. The evaluation process identified five games that are applicable for educating this group of learners and they could be recommended to this audience. Among the card-based games the Cyber Threat game was found to be applicable, other identified games for high school student education were Target attack, Cybersecurity Lab, Permission impossible, Data Centre attack and Keep tradition secure.

The summary of the results of the evaluation report are presented in a table in ***Annex 1****. The table provides the main information that characterize the game properties and its value for the education process. More information about the studied games can be found in the report.*

The technical properties considered in the evaluation:

- ***Platform:*** *Web Based/Stand Alone (OS: PC/Linux/macOS)*
- ***Distribution:*** *Weather the game is free for use, or needs licence for playing, or is on cd-rom, or is run only by downloaded application/client, the year of publishing: when the game become available for public use*
- ***Label:*** *The name of the team that has developed the game.*
- ***Single/Multi user:*** *Weather game has to be played by one or many players*
- ***Dimension:*** *Weather game is present in 2D/3D environment*
- ***Group:*** *To which main group the game belongs (according to TULIP classification) : Table Top, Networking, Firewall, CTF, General.*
- ***Genre:*** *Whether the »game-flow« has been played in a form of Roleplay-Character, as an Adventure, as team Competition or as a Playing cards game.*

The e-learning properties and the game learnability used in evaluation:

- ***Competitive or Non Competitive:*** *If 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).*
- ***Degree of complexity:*** *the computer model complexity that is underlying in the game scenario.*
- ***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 presented as the upgrade level in the game summary reports prepared for the learner.*
- ***Deterministic or stochastic:*** *If the game is stochastic by nature or is prepared as a deterministic game that has a fixed rule scenario.*
- ***Background knowledge****: The kind of background knowledge requested for playing the game (basic knowledge of ICT, intermedia, advanced or a pure beginner knowledge (general public).*

- ***Learnability and the Learning Outcome: C****ybersecurity game does show a clear learning goal in order to be classified as educational or 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 positive outcome/scores.*
- ***Clear Goal:*** *The game has to show clearly the purpose of the cybersecurity gaming. It should be clear if the game is dedicated to training skills, just learning a single cybersecurity topic or is only building awareness about cybersecurity.*
- ***Target Audience:*** *The game target audience 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) and their usage depends on the level of background knowledge each audience should have.*

The selection of the cybersecurity games was installed and tested by academic staff teaching cybersecurity at Jožef Stefan Institute, Slovenia. The results are presented as items in Annex 1.

By making the classification and evaluation of the selected games, we concluded that some games would be appropriate to be studied further as a possible learning tool for the high-school Students. These games can be a useful approach for training or teaching some of the fundamental topics of the cybersecurity field of education. We have selected three games for further inspiration:

A. TARGET ATTACK

Targeted Attack: The Game is an immersive simulation game created by Trend Micro ltd (www.trendmicro.com) for student training to test system cybersecurity abilities and to make the right decisions for avoiding the devastating consequences of a major data breach.

Targeted attack in the game is built on the principles of adventure game, which means, it is a type of video game in which the participant plays a fantasy role in an episodic adventure story. More than any other genre, the adventure games depend heavily upon their story and setting in creating a compelling single-player experience. This game offers the player the unique chance to step into someone else's shoes and to find out if the player is good enough to come and face critical challenges of data breach.

The game transfers the player into the role of the CIO person who works for a global organization called The Fugle, responsible for making the first release of a biometrically authenticated mobile payment application. The player in his/her role of CIO has to steer the project through its final stages, dealing with the internal security team, such as the player's colleagues in Marketing and PR and the player's CEO.

To play a game visit: http://targetedattacks.trendmicro.com/

B. PERMISSION IMPOSSIBLE

Permission Impossible, an online game designed to teach people both with and without a computer science background about firewalls. The aim of the game is to introduce the novices

about basic firewall terminology and concepts as well as how to build a firewall rule set to enable incoming and outgoing packet traffic.

Permission Impossible provides scaffolded learning through increasingly complex levels. Initial levels provides detailed instruction, with later levels progressively providingless details, less intuitive missions, and finally removing the color hints from the interface completely. Once The user start to play a game, there is the avatar called Roboto, who is guiding the user through the game. The Roboto provide the user different tasks and hints how to complete the different tasks in order to complete the current level.

To play a game visit: https://groups.inf.ed.ac.uk/tulips/projects/1617/PermissionImpossible/

C. KEEP TRADITION SECURE

Keep tradition secure game (keeptraditionsecure.tamu.edu.) is an on-line game that can be played anywhere using a laptop, desktop, tablet or mobile device. The game was developed by a Texas research group in a A&M Texas University (Agricultural and Mechanical College of Texas). In the game, players help the hero known as "Good_Bull'' to track a hacker, "Bad_Bull," across the campus. Good_Bull needs your help. A notorious hacker with the screen name "Bad_Bull" hates Texas A&M tradition and is causing trouble around campus.

The principle of the game is more or less based on quiz questions. Various questions about cyber security are presented and, when answered correctly, the players get a clue intentionally left by the hacker in the form of riddles regarding Texas A&M traditions. The game is actually a good learning tool for basic cybersecurity knowledge. It actually helps users to be aware of the everyday threats when browsing the internet. It is an asset that anyone can use, from young kids to older students or average internet users.

To play a game visit: https://keeptraditionsecure.tamu.edu/

6. Conclusions and next steps

The analysis performed on the survey and interviews answers could be concluded as follows:

***(1) the most in need topics to be covered in the materials** are "Being safe in online social platforms"," Recognizing fake accounts", "Ensuring their privacy in online activities", "Creating strong passwords", "Using email applications in a secure way" based on the topics-to-be-discussed ranking we obtain from parents, teachers, and students through the survey. Moreover, the lower confidence level mentioned by the students in "Secure online shopping", "Sharing files online", and "Securely Downloading" adds those topics in the list of the most in need topics to be covered.*

***(2) the most appropriate format for the materials** to be developed would be the videos, interactive presentations, games/platforms. The teachers and the parents interviewed strongly suggested on having interactive instruments where real facts are presented to the students followed by discussions between the students and the teachers on the topics covered by exchanging prior related experiences. Paper material was mentioned marginally, for the use of disseminating contact information of special organizations offering support for students experiencing an online risk.*

***(3) the areas not (enough) covered by existing programs** are how to detect and handle the 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 detecting and handling the online risks and make the students feel confident in such tasks. Increasing the time and the frequency of such courses and presenting the threats in a more practical than theoretical way can help in improving the effectiveness of existing programs. Additionally, during the interviews, we drew the conclusion that cybersafety topics (e.g. cyberbullying, sexual grooming, privacy, etc.) are more discussed than cybersecurity topics (e.g cyber-attacks, spams, viruses). This can be an indicator that the existing programs focus more on spreading awareness on cybersafety topics and less on cybersecurity topics.*

The conclusions are not significantly influenced by the country of residence of the participants in the process.

The additional research performed on the latest studies in the education field have shown that cybersecurity education requires innovative approaches like the use of cyber ranges and serious games that have proven to be more effective in developing cyber related skills. Indeed, these approaches enable interactivity in the training process and lead the learner to take decisions in a safe but similar to the real-life environment thus helping accelerate the learning process.

These findings will be further validated in live event before moving to the next step in the process, the design of the materials. When designing the materials we will first assess the

feasibility on build on the existing solutions within the consortium such as Cybersafety Family Advice Suite (CFAS)[1] developed by Cyprus University of Technology and the Privacy calculator[2] developed by University of Zagreb, Faculty of Electrical Engineering and Computing.

---

[1] CFAS is a collection of cybersafety tools that uses machine learning classifiers and other filters to protect children when using online social media. The child is always aware of any information the parent or the tool can have over his/her activities in online social media. The parent can set the settings for the child's cybersafety, the parental and backend visibility, but the child should give his/her consent in order to set the settings in operation. CFAS uses its architecture to spread awareness to the parents and the children about the various threats they face online. Also, it utilizes the Guardian Avatar approach that provides a more interactive method to advise the children in a direct and user-friendly manner.

[2] The Privacy Calculator tool (https://privatnost.hakom.hr/index_en.php) aims at educating and encouraging people to think about problems linked to the security and privacy of the personal data on the Internet. The system assesses the risk for the privacy of the owner of such data and provides real-world scenarios which correspond to the selected parameters. Along with the estimated risk, we encourage users to study the offered scenarios because they are the key to understanding the frauds and the problems they can bring.

Annex 1: ***Evaluation table of cybersecurity game properties***

	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, rolepla	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 Competitive	Competitive	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