applied sciences

MDPI

Article

An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context

Mário Antunes [1,2,*], Carina Silva [3,4] and Frederico Marques [5]

[1] Computer Science and Communication Research Centre (CIIC), School of Technology and Management, Polytechnic of Leiria, 2411-901 Leiria, Portugal
[2] INESC TEC-CRACS, 4200-465 Porto, Portugal
[3] Lisbon School of Health Technology, Polytechnic of Lisbon, 1990-096 Lisbon, Portugal; carina.silva@estesl.ipl.pt
[4] Centro de Estatística e Aplicações, University of Lisbon, 1749-016 Lisbon, Portugal
[5] School of Technology and Management, Polytechnic of Leiria, 2411-901 Leiria, Portugal; 2190377@my.ipleiria.pt
* Correspondence: mario.antunes@ipleiria.pt

Abstract: Digital exposure to the Internet among the younger generations, notwithstanding their digital abilities, has increased and raised the alarm regarding the need to intensify the education on cybersecurity in schools. Understanding of the human factor and its influence on children, namely their attitudes and behaviors online, is pivotal to reinforce their awareness towards cyberattacks, and to promote their digital citizenship. This paper aims to present an integrated cybersecurity and cyberawareness strategy composed of three major steps: (1) Cybersecurity attitude and behavior assessment, (2) self-diagnosis, and (3) teaching/learning activities. The following contributions are made: Two questionnaires to assess risky attitudes and behaviors regarding cybersecurity; a self-diagnosis to measure students' skills on cybersecurity; a lesson plan addressing cyberawareness to be applied on Information and Communications Technology (ICT) and citizenship education curricular units. Cybersecurity risky attitudes and behaviors were evaluated in a junior high school population of 164 students attending the sixth and ninth grades. The assessment focused on two main subjects: To identify the attitudes and behaviors that raise the risk on cybersecurity among the participating students; to characterize the acquired students' cybersecurity and cyberawareness skills. Global and individual scores and the histograms for attitudes and behaviors are presented. The items in which we have observed significant differences between sixth and ninth grades are depicted and quantified by their corresponding *p*-values obtained through the Mann–Whitney non-parametric test. Regarding the results obtained on the assessment of attitudes and behaviors, although positive, we observed that the attitudes and behaviors in ninth grade students are globally inferior compared to those attained by sixth grade students. The deployed strategy for cyberawareness was applied in a school context; however, the same approach is suitable to be applied in other types of organizations, namely enterprises, healthcare institutions and public sector.

Keywords: cybersecurity; cyberawareness; human factors; attitudes and behaviours; school context

check for updates

Citation: Antunes, M.; Silva, C.; Marques, F. An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Appl. Sci.* **2021**, *11*, 11269. https://doi.org/10.3390/app112311269

Academic Editors: Konstantinos Rantos, Konstantinos Demertzis and George Drosatos

Received: 30 October 2021
Accepted: 24 November 2021
Published: 28 November 2021

1. Introduction

Cyberspace has a plethora of interconnected entities, with the Internet being the paramount infrastructure that supports the services where the users conduct their digital life. Despite its global penetration and intrinsic benefits, the Internet and its services were not designed to be fully secure and are prone to human mistakes [1]. Despite the technological advances in information security and cybersecurity observed in the last decades to keep data, information, and services secured, the human factor plays a key role in information security and cybersecurity in organizations [1,2]. Human factors, namely users' attitudes and behaviors, are crucial to ensure an effective Information and Communications Technology (ICT) infrastructure protection in its major areas.

In the context of cybersecurity, attitudes refer to a person's perspective, which can influence the behavior online. Those attitudes are the result of a person's learned experiences, social factors, and observation, which may dictate the way a person decides about a particular event on its activity online [3,4]. Cyberpsychology is an emergent field that studies the effect of the Internet and cyberspace on the mind, behaviors, and attitudes of individuals [5]. Subjects like Internet addiction, depression, and social isolation are amongst the psychological behaviors studied. Intrinsically related to cyberpsychology is the study of the relationship between users' impulsivity, and risky behaviors, and attitudes towards cybersecurity and how they affect the overall level of cybersecurity [6].

Besides their digital lives, Internet users are humans, and their attitudes and behaviors condition their overall activity and outcomes that could be attained. Moreover, the digital being behind an Internet user has a physical presence and along their lifetime will produce a digital footprint with the data and information shared into the Internet services. It is thus critical that users adopt, from an early age, a cybersecurity culture on the Internet. The agreement to a set of cyber hygiene practices in their daily routine may prevent users from being threatened with cyberattacks, and private information leakage, which may bring physical, psychological, and monetary losses [7,8].

Generally, schools promote cultural, ethnic, and social diversity to fully accomplish the mission of preparing active citizens that may be able to work on worldwide enterprises supported by digital communications and services in cyberspace. Over the past decades, schools have undergone a digital transformation to better prepare the students for a digital world. Teaching–learning strategies have evolved to accommodate digital resources, management processes have been simplified, and more robust networking infrastructures have been installed in the schools. The digital revolution that occurred in schools implied an adjustment to the course curricula offered to the students. Generally, all the curricular units have adapted their contents to prepare the students for digital citizenship, not only by teaching technical subjects regarding the Internet but also by including transversal skills related to digital literacy, cybersecurity, and cyberawareness [9,10].

The school administration has to take part of the cybersecurity and cyberawareness processes. There are three major arguments that should be pointed out to enlighten the administration and ignite such a research project on the ground. First and foremost, the key role of the school is to qualify citizens in a myriad of skills, in which cybernetics and digital skills should be included. These skills should also include awareness about the risks of using technological devices connected to the Internet, the associated risky behaviors and attitudes, and which cyberawareness measures should be continuously adopted. Secondly, a cybersecurity assessment is a relevant tool to evaluate the cyberawareness level to further raise it, by including these subjects in curricular units and long live learning programs for teachers, staff, and students. Finally, cyberawareness in schools is a collective effort, involving all the school community players, namely students, parents, staff, teachers, and administration. A positive indication given by the administration to the whole community means a step forward for the success of the implementation of this strategy in a school context.

Having in mind the growing importance of cyberawareness and the key role of the school on digital citizens' education, this paper presents the results obtained with the implementation of an integrated cyberawareness program, by applying a methodology to evaluate the influence of risky behaviors and attitudes towards cybersecurity, as well as a self-diagnosis tool and a lesson plan.

The research aimed to evaluate the students' attitudes and behaviors in a junior high school. The students were all subjected to the evaluation and were attending the 6th or 9th grades. They had the opportunity to use a cybersecurity self-diagnosis application and to attend a cyberawareness class that was based on the ENISA Reference Incident

Classification Taxonomy report and several ENISA's cyberawareness multimedia material. The questionnaires and the overall research was conducted in a junior high school.

A general aim of this research was to elucidate and involve the whole school infrastructure, namely the administration, the students, the staff, and the teachers, in the subject of cybersecurity and cyberawareness. Despite the questionnaires having been directed towards the students, the first step was to elucidate the school administration about the need to integrate cybersecurity topics in curricula, and to assess students' risky behaviors and attitudes.

The questionnaires of attitudes and behaviors were applied to the students and further evaluated, while the self-diagnosis tool and the lesson plan was tested within the same population, although without a formal evaluation of their impact.

2. Literature Review

Information security and cybersecurity awareness and best practices in school environment have been reported by several authors [11–14]. In [11] Slusky and Partow-Navid reported the results obtained with the students at the College of Business and Economics, California State University, in 2011, and correlate cyberawareness with the ways the students apply their information security knowledge in real-world scenarios. The theory of motivation was applied by Hanus and Wu [12] at University of Texas to assess the impact of users' cyberawareness. The major authors' findings evidenced that consciousness towards cybersecurity significantly affects the perception of risk severity, the efficacy of the response, the self-efficacy, and the cost of response. More recently, in [13] the authors addressed the cybersecurity issues in the schools, identifying the major flaws, the risks, and the motivations behind cybercriminals' activities. The human factor is detailed, namely, the way students may influence cybersecurity. The authors conclude that a "one size fits all" approach is not adequate to promote cybersecurity in schools, the human factor is still low, and more work should be done.

Several authors analysed the correlation between the use of Internet and the adoption of cyberawareness measures in school context [14–16]. Tirumala et al. [14] analysed the impact in school context, with three groups of students between 8 and 21 years. The results reveal two important conclusions: A low level of cyberawareness; a global lack of knowledge regarding the fundamentals of cybersecurity and the software tools used to protect electronic equipment. The authors propose the creation of cyberawareness programs directed towards students. The dangers behind the use of Internet on higher education students are detailed in [15]. The authors measured the cyberawareness level by delivering a questionnaire to the students of the International School for Social and Business Studies in Slovenia with questions related to the respondents' familiarity with cybersecurity and cyberawareness. The research released a set of best practices for cybersecurity, which can be used by several groups of users, such as students at all stages, active professionals, and unemployed. The study also emphasized the need to enhance cyberawareness practices in the educational system in general.

A set of surveys and reports about cyberawareness in the school context were already available. In 2011, Livingstone et al. [17] applied a questionnaire directed to children and parents, to evaluate the online technologies and Internet experience in twenty-five European countries. The questionnaire was directed at children and parents and its main results can be summarized as follows: Most children access the Internet at home, which infers that parents are well-positioned to mediate that access; teenagers' access to the Internet is made from their bedrooms, which challenge the parents; despite the desktop being used as the most common Internet access, average children and teenagers use regularly two devices online; teenagers stay online longer periods, and children are beginning to stay online earlier. More recently, the EU Kids Online network report [18] presents the findings from a survey of $25,101$ children aged 9 to 16, from 19 European countries. The findings are based on a questionnaire developed by members of the EU

Kids Online network and are organized into the following four dimensions: Internet access, practices and skills, risks and opportunities, and social context [19].

Recently, the positive impact and the problems addressed by the Internet in the citizens' daily routine have been detailed in [16]. The authors' major findings point out that the level of cyberawareness is generally moderate or low in all age groups, emphasizing the need to adopt measures to improve cyberawareness on the school environment. The authors also maintain that cyberawareness challenges are global and should involve teachers, parents, students, and governmental entities. They also argue that media (e.g., television and radio) have a key role in awareness campaigns regarding cybersecurity, especially directed to students.

The measure of the level of understanding and awareness for cybersecurity was proposed by Mee et al. [20]. The authors measure the public motivation, government policy, educational system, labor market, and the digital divide. The authors assess and classify the literacy level into the following five key factors, considered as essential to the development of digital literacy in a wide set of countries: Governmental politics in terms of cybersecurity, the commitment of the schools to enhance the digital literacy of the population, and cyberawareness in the enterprises.

Enterprises also have general concerns regarding cyberawareness among their employees. Pfleeger and Caputo [21] conclude that enterprises which have adopted cybersecurity measures solely by implementing technological processes were not able to have a better level of security. According to the authors, the human factor in cybersecurity is not adequately considered in enterprises. In [22] the authors evaluate the relationship between individuals' consciousness and the Information Security Awareness (ISA) model. The authors used the Human Aspects of Information Security Questionnaire (HAIS-Q), which is based on a Knowledge, Attitudes, and Behaviors (KAB) model. Consciousness, sympathy, emotional stability, and propensity to take risks are identified by the authors as key factors to explain the variance in individuals. The findings obtained with the questionnaire in the enterprises were important to identify strengths and weaknesses regarding cyberawareness, as well as to define training actions.

The individuals' attitudes and behaviors towards the cybersecurity were studied by Hadlington [6]. The major findings try to explain the way individuals' attitudes and behaviors, as well as Internet addiction and impulsivity, are intrinsically related to the cybersecurity risks taken in the organizations. The author evaluated these issues with four online questionnaires, namely "ABbreviated Impulsiveness Scale" (ABIS), "Online Cognition Scale" (OCS), "Risky Cybersecurity Behaviors Scale" (RScB), and "Attitudes Towards Cybersecurity and Cybercrime in Business" (ATC-IB). The major findings are as follows: Attitudes towards cybersecurity were negatively correlated with the individuals' involvement in risky behaviors; Internet addiction and impulsiveness are directly related to risky behaviors.

Regarding the impact of cyberawareness in Small–Medium Enterprises (SME), Boletsis et al. [23] and Antunes et al. [24] have pointed out the key factors and the cyberawareness best practices that should be adopted in this type of organization. In healthcare institutions, Nunes et al. [25] evaluated the cybersecurity awareness level of health practitioners in hospitals and identified the associated risk. Two questionnaires derived from Hadlington's ATC-IB and RScB scales were used to evaluate the cybersecurity risk faced by these professionals, according to the measured attitudes and behaviors taken online. In a wide scope, which embraces enterprises, SME, public institutions and individuals, ENISA's cybersecurity culture guidelines report [26] details the human aspects of cybersecurity and the existing research behind "behavior science", which includes a wide range of multidisciplinary disciplines. According to the report, cybernetics threats exist in all organizations, but they are recurrently seen as a technical problem, underestimating the human factor.

Communication issues, regarding cybersecurity maintenance in organizations, are detailed by Furnell et al. [27]. The authors highlight that the user's role is emphasized by keeping cybersecurity but is barely recognized by IT teams. Some experiments with social engineering were carried on, involving employees in enterprises. In the same direction, Alshaikh [28] identifies five key initiatives to improve cybersecurity cultures, namely identifying key cybersecurity behaviors, establishing a "cybersecurity champion" network, developing a brand for the cyber team, building a cybersecurity hub, and aligning security awareness activities with internal and external campaigns promoted by the enterprises. The deployed framework was implemented in three enterprises in Australia and demonstrated the benefits to creating "functional cybersecurity cultures" in the organizations.

Cybersecurity learning platforms have been generally applied in the school system [29–31]. In [29] the authors propose a web application to manage cybersecurity learning content, together with a mobile application to raise young learners' awareness on basic cybersecurity and privacy issues. Quayyum [30] provides a comprehensive overview of the challenges in cybersecurity education for children. The same author [31] investigates and presents new knowledge and tool development that may be effective on teaching the children about cybersecurity. Gamification strategies are used to engage and motivate students to learn cybersecurity subjects.

Regarding cyberawareness self-diagnosis and learning platforms, a comprehensive set of tools were released to promote cyberhygiene practices and make users aware of the risky behaviors and attitudes when they are online. A list of security awareness training tools oriented to enterprises, provided by G2 crowd software review, is available in [32]. Regarding cyberawareness programs for schools, the list is vast and incorporates governmental and Non-Governmental Organization (NGO) initiatives, and commercial software platforms [33,34].

In the research presented in this paper two contributions evolve from previous works described in the literature. The behavior and attitude assessment scales derive respectively from Hadlington's RScB and ATC-IB scales, which were adapted to the school environment and are detailed below in this document. Regarding self-diagnosis web application development, its database of questions is aligned with the European Union Agency for Network and Information Security (ENISA) Reference Incident Classification Taxonomy report [35], elaborated by the ENISA's Incident Classification Taxonomy Task Force. It is a widely disseminated document, which has been adopted by the network of Computer Security Incident Response Teams (CSIRT).

3. Research Methodology

The research methodology comprises three integrated and complementary actions to leverage cyberawareness in a school environment, namely: Two questionnaires delivered to the students to assess the risky attitudes and behaviors; a self-diagnosis questionnaire to evaluate the students' knowledge level regarding cybersecurity; a lesson plan to be integrated into ICT and/or citizenship education curricular units to alert students to cybersecurity attitudes and behaviors. Cyberawareness in school environment is a continuous process and it is meant to intersect three fundamental dimensions: Assessment, self-diagnosis of skills, and teaching–learning strategies. Figure 1 depicts the overall methodology designed to apply a fully integrated cyberawareness in the school environment. Continuous assessment is achieved by evaluating attitudes, behaviors, and technical skills, while continuous learning is the result of incorporating learning activities in classroom regarding cyberawareness and cybersecurity attitudes and behaviors.

Two distinct methodologies were applied to produce the assessment scales and to delineate the self-diagnosis web application, respectively. Both methodologies are described below.

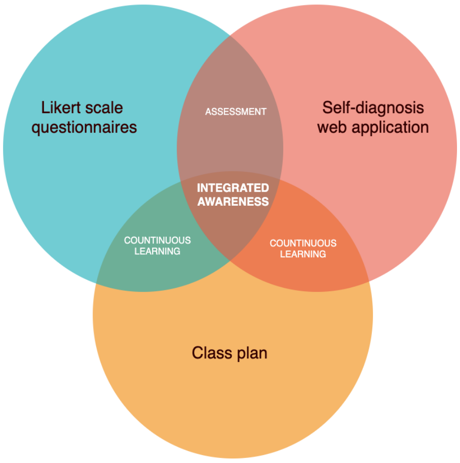


Figure 1. Overall integrated methodology for a cyberawareness in schools.

3.1. Risky Attitude and Behaviour Assessment Scales

The methodology delineated to define and adjust the questionnaires is depicted in Figure 2. Two questionnaires were deployed and applied, namely, Cybersecurity Behaviors in Schools (CsB-S), and Cybersecurity Attitudes in Schools (CsA-S). The starting point to delineate these questionnaires was the identification of state-of-the-art questionnaires adopted for similar research. Hadlington's RScB and ATC-IB [6] were selected, as they were already applied in similar contexts. The findings attained with recent work developed by the authors [25], in which similar questionnaires were applied in health institutions to evaluate health practitioners' cybersecurity attitudes and behaviors, were also considered in the decision.

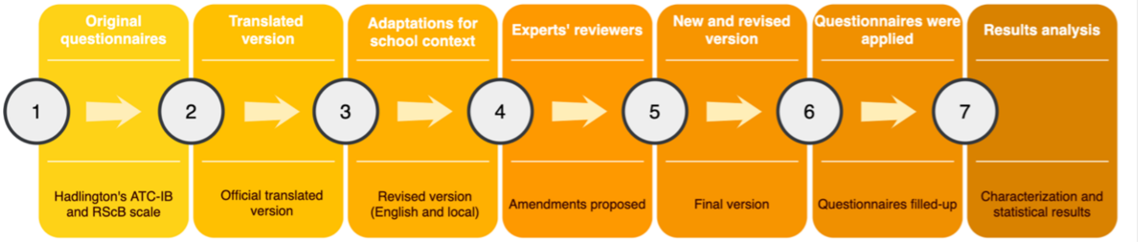

Original questionnaires
Translated version
Adaptations for school context
Experts' reviewers
New and revised version
Questionnaires were applied
Results analysis
1
2
3
4
5
6
7
Hadlington's ATC-IB and RScB scale
Official translated version
Revised version (English and local)
Amendments proposed
Final version
Questionnaires filled-up
Characterization and statistical results

Figure 2. Overall methodology applied on questionnaire development.

The school environment is different from enterprises or health institutions in that sense a list of adaptations to the questionnaires was made to accommodate them to be applied to school context. The rewritten version of the questionnaires was subjected to the evaluation of a group of experts in cybersecurity and cyberawareness. The suggestions, amendments, and proposals collected in this stage were then incorporated in the final version of the questionnaires. The questionnaires were made available online in the Lime Survey platform, that is, the results analysis concerning the last step of the methodology, where the characterization of the study and the corresponding results were summarized.

In this research two new questionnaires were developed, namely to evaluate students' risky attitudes (CsA-S) and behaviors (CsB-S) when they are online, both in entertainment and in a school environment. Students have responded to both questionnaires in a 90-min class.

Regarding attitude assessment, Table 1 summarizes the twenty-five questions that are part of the CsA-S questionnaire, where the answers were scored from 1 to 4 points (1 = Totally Agree; 2 = Agree; 3 = Disagree and 4 = Totally Disagree). The high levels of the scale correspond to positive attitudes and questions marked with '*' have an inverted score that corresponds to bad attitudes.

Table 1. Cybersecurity Attitudes in Schools (CsA-S).

ID	Question
A1 *	I believe that it is safe to ignore update warnings from computer software.
A2	I am aware of my role in keeping the school protected from potential cybercriminals.
A3	I believe everyone in the school has a role to play in protecting against threats from cybercriminals.
A4 *	It is hard to know how I can help protect the school from cybercrime.
A5 *	I don't have the right skills to be able to protect the school from cybercrime.
A6	I believe that personal information should not be revealed online, namely who I am, where I live or which school I attend.
A7 *	Computer systems provide all the protection a school need.
A8 *	I think that reporting cybercrime is a waste of time.
A9 *	The Police lack the capacity to deal with cybercrime effectively.
A10 *	I believe that cybercriminals are more advanced than the people who are supposed to be protecting us.
A11 *	I would download copyright material (images, documents, videos).
A12	I believe when I view violence related content in a school, I may have been promoting its sharing and comments.
A13 *	I worry that if I report a cyberattack to the Police it might damage the reputation of the school.
A14 *	I think more could be done to communicate/disseminate/sensitize the risks from cybercrime to individuals in the school.
A15	I am aware of the schools IT use policy and attempt to follow it.
A16 *	I would not know how to report a cyberattack if one happened.
A17 *	I don't think that reporting a cyberattack launched from the school is my responsibility.
A18 *	I don't pay attention to school material about the threats from cybercrime.
A19	I am confident that I would be able to spot the signs of a cyberattack.
A20	I believe that, when inappropriate content appears online, I should ask for help from an adult.
A21	I feel that any individual within the school is at risk of manipulation from confidence tricksters.
A22 *	I think that cybercriminals only target a school when there is a substantial financial gain.
A23 *	I believe only companies are targeted by hackers and cybercriminals.
A24 *	I feel that only companies that take payments using online systems are at risk of being victims of cybercrime.
A25 *	I think that I have the right to be always online, with access to all Internet services.

* Items negatively worded were reverse-scored for further analysis.

Similarly, in the CsA-S scale, some questions were removed or adapted, as in the CsB-S scale. The questions related to the management issues were not relevant for the respondents and were removed or adapted.

The released version of CsB-S scale is detailed in Table 2. It is composed of twenty questions related to risky behaviors that users may take online. Questions are composed of a seven-point Likert scale, scored from 1 to 7 (1 = Never to 7 = Daily). The high values of the scale correspond to negative behaviour, with however the questions marked with '*' having an inverted score, which corresponds to good behaviors.

Table 2. Cybersecurity Behaviors in Schools (CsB-S).

ID	Question
B1	Sharing passwords with friends and colleagues.
B2	Using or creating passwords that are not very complicated (e.g., family name and date of birth, letter strings).
B3	Using the same password for multiple websites.
B4	Using online storage systems to exchange and keep personal or sensitive information.
B5	Entering payment information on websites that have no clear security information/certification.
B6	Using free-to-access public Wi-Fi.
B7	Relying on a trusted friend or colleague to advise you on aspects regarding online security.
B8	Downloading free anti-virus software/apps from an unknown source.
B9	Disabling the anti-virus on my computer so that I can download information from websites.
B10	Bringing in my own USB to school in order to transfer data onto it.
B11 *	Checking that software in your smartphone/tablet/laptop/PC is up to date.
B12	Downloading digital media (music, films, games) from unlicensed sources.
B13	Sharing my current location on social media.
B14	Accepting friend requests on social media because you recognize the photo.
B15	Clicking on links contained in unsolicited emails from an unknown source.
B16	Sending personal information to unknown people over the Internet.
B17	Clicking on links in an e-mail message that come from a trusted friend or colleague.
B18 *	Checking for updates for any anti-virus software you have installed.
B19	Downloading data and material from websites on your computer without checking its authenticity.
B20	Storing personal, family and friend's information on your personal electronic device (e.g., smartphone/tablet/laptop).

* Items negatively worded were reverse-scored for further analysis.

The rationale behind CsB-S scale adaptations was the socio-cultural and organizational context of the schools, comparing with the enterprises. Hadlington's scales included questions about management issues and their intrinsic relationship with the perception of risk and cyberawareness. As students do not have enough skills about the institutions responsible for cybersecurity and information security management, those questions were removed in the final versions of the questionnaire.

3.2. Self-Diagnosis Application

Regarding the self-diagnosis web application development, the following presumptions were initially defined:

- The web application should be user-friendly and easy to use.
- The database of questions should include a vast number of items, and on each interaction, a new randomly generated set of questions should be used.
- The text of each question and its possible answer options should use an understanding, unambiguous, and easy-to-read language.
- The database of questions should follow a predefined layout that meets the published cybersecurity and information security taxonomies and standards.
- There should be provided feedback to the user, according to the answer given for each question. The feedback should include a score, a list of further readings, and a set of tips and hints that should be followed to mitigate some kind of bad behavior that has been observed in the answers.

Figure 3 depicts the overall methodology adopted to build the self-diagnosis web application. the areas identified in the first step meet the CSIRT taxonomy [26]. For each of the ten areas that were identified, a list of ten multiple-choice questions was then set up. For each option chosen in the answer, a score was defined regarding its level of assertiveness. For each less appropriate or even wrong answer, a feedback report was prepared, giving indications about mitigation practices that should be adopted. Finally, before designing and releasing the auto-diagnosis questionnaire to the students, the number of questions to include and the layout were defined.

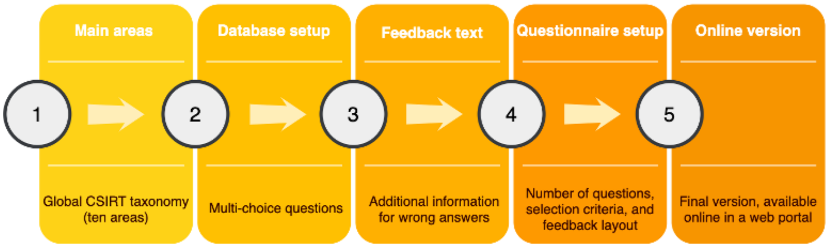
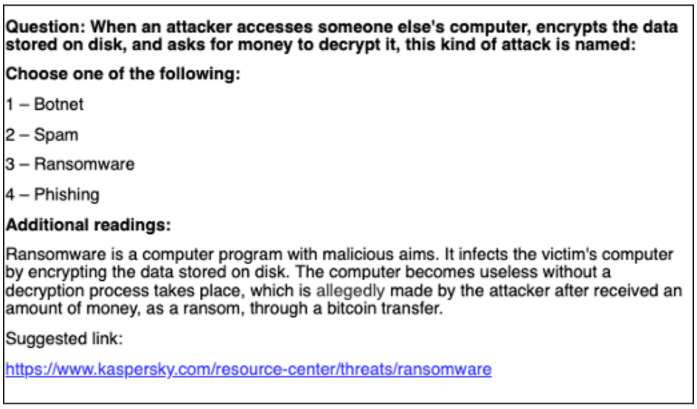

Main areas
Database setup
Feedback text
Questionnaire setup
Online version
1
2
3
4
5
Global CSIRT taxonomy (ten areas)
Multi-choice questions
Additional information for wrong answers
Number of questions, selection criteria, and feedback layout
Final version, available online in a web portal

Figure 3. Methodology adopted to develop the web application for self-diagnosis.

An example of a question and its layout is depicted in Figure 4. For each question, a list of four options for answers is presented to the user, one being correct and the remaining ones incorrect. A feedback text is presented when the wrong answer is selected.



Question: When an attacker accesses someone else's computer, encrypts the data stored on disk, and asks for money to decrypt it, this kind of attack is named:

Choose one of the following:

1 – Botnet

2 – Spam

3 – Ransomware

4 – Phishing

Additional readings:

Ransomware is a computer program with malicious aims. It infects the victim's computer by encrypting the data stored on disk. The computer becomes useless without a decryption process takes place, which is allegedly made by the attacker after received an amount of money, as a ransom, through a bitcoin transfer.

Suggested link:

https://www.kaspersky.com/resource-center/threats/ransomware

Figure 4. Example of the question layout for self-diagnosis web application.

3.3. Lesson Plan

Continuous learning is achieved by applying teaching–learning strategies to approach cyberawareness and cybersecurity topics in the classroom. The following presumptions were initially identified to mold the lesson plan defined in this research:

- A 90-minutes slot was available to apply a lesson plan to briefly accommodate the cyberawareness topics. Further developments should include a deeper lesson plan which should be included in a longer duration slot.

- Two different curricular units were eligible to accommodate these subjects, namely Information and Communication Technologies (ICTs), and Education for Citizenship, being both part of the 6th and 9th grade curricula.

The lesson plan was designed to include international guidelines, namely the ENISA Reference Incident Classification Taxonomy report [35] and ENISA information security awareness material [36].

Figure 5 depicts the overall alignment of the defined lesson plan. The lesson starts with a briefing to the subject, followed by the presentation of a list of topics, classified into three main groups: Common issues, technical solutions, and other topics. After the lecture, a debate follows for discussion of topics learned.

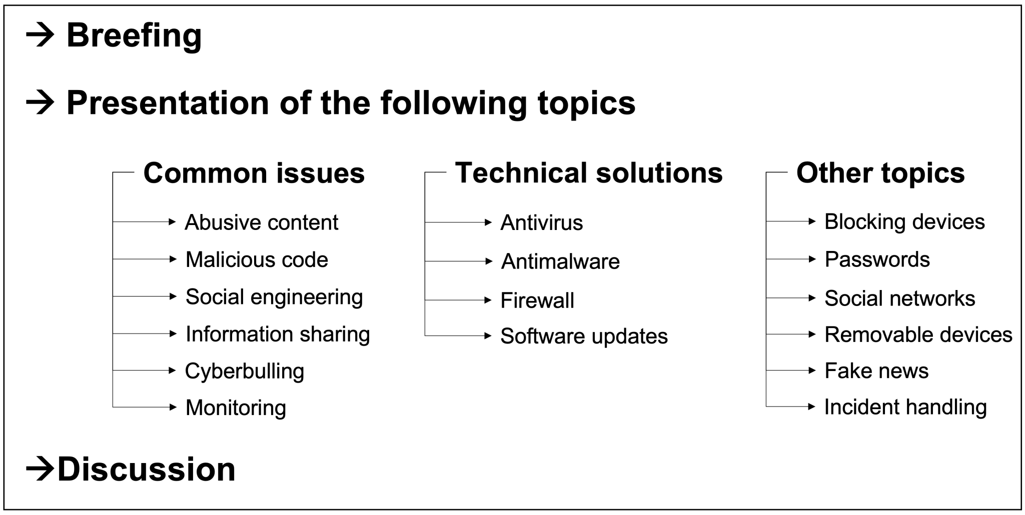


Figure 5. Overall design of the lesson plan.

3.4. Statistical Analysis of the Scales

Descriptive statistics were used to examine response variability and missing data in the assessments. An individual descriptive item analysis was performed to identify and eliminate those items with missing data. A sample size of 88 students was obtained in the 6th and 76 in the 9th.

Data were analyzed considering positive behaviors (scores equal to or less than 3 points on the Likert scale were considered positive behavior) and positive attitudes (scores equal to or greater than 4 points of the Likert scale were considered positive attitude). A global score for both scales was obtained. Regarding CsB-S scale, the score ranges between 20 and 140, where low values indicate low riskier behavior in cybersecurity. Global score of CsA-S scale ranges between 25 and 100, where high values are indicative of low riskier attitudes.

The data were analysed according to gender and grade group stratification and were presented as mean (standard deviation) and proportions as appropriate. To compare global score means between gender and grades a *t*-test for independent samples was used. To compare the differences of item questionnaires between the 6th and 9th grades the non-parametric test of Mann–Whitney was used. There was a 5% significant level.

Cronbach's alpha was used to analyze the internal consistency of both scales. Reliability values equal to or greater than 0.6 are considered adequate for a survey instrument [37]. Statistical data analysis was conducted using the software IBM SPSS (Statistical Package for the Social Sciences, version 26).

4. Results and Discussion

This Section details the results obtained with the CsA-S and CsB-S questionnaires. The sample is composed of 164 respondents, being equally distributed between males and females. From the total of respondents, 88 belong to the 6th grade, while the remaining

76 are at 9th grade. A Cronbach's alfa of 0.8 for CsA-S scale and 0.63 for CsB-S scale were obtained.

Table 3 describes the identified findings to which the questionnaires should respond. For each finding, the corresponding list of questions present in the CsA-S and CsB-S questionnaires are pointed out.

Table 3. List of findings and the corresponding questions of CsA-S and CsB-S.

ID	Finding	ID
01	The students express some level of awareness regarding their privacy online and the consequences of exposing their personal data?	A6 B5, B13, B14, B16, B20
02	Students' online attitudes and behaviors are tendentiously positive or negative?	A11, A12, A17, A25 B8, B9, B12, B19, A8
03	What is the students' perception about the cybersecurity information provided by the school?	A14, A15, A16, A17, A18
04	When contacting with strangers online, are the students' aware about the concerns involved?	B2, B4, B5, B14, B15, B17
05	Are students aware about their attitudes and behaviors towards cybersecurity in school?	A1, A2, A3, A4, A5, A7 B2, B9, B11
06	Do students understand the cybercriminals' motivations?	A19, A22, A23, A24
07	Do students reckon on law enforcement and ICT technicians?	A8, A9, A10, A13
08	Do students aware about protecting their equipment and data?	B1, B2, B3, B6, B8, B9, B10, B11, B18, B20
09	Do students aware about the consequences of using unofficial and copy-write protected software?	B8, B12, B19

Considering students' awareness of their online privacy (Finding 01) it was observed that both behaviors and attitudes (Figure 6a)) are positive, where item B20, related to storing information, showed the lowest positive behavior (64%). Students have tendentiously positive behaviors and attitudes (Figure 6b)), where the item A25, related to the access to all Internet services, achieved the lowest positive value (52%) in Finding 02.

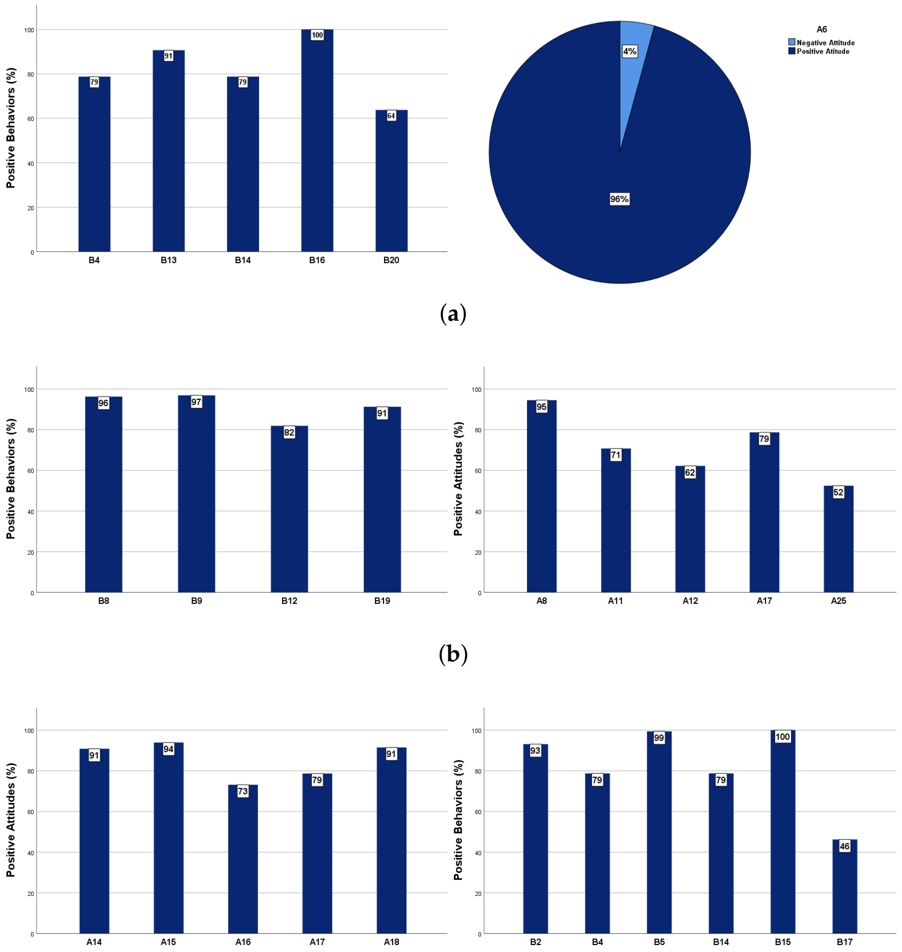
As depicted in Figure 6c, students showed to have a positive perception about cybersecurity provided by the school (Finding 03). Regarding the awareness when they are contacted by strangers, students have shown to have a positive behavior (item B17) by only clicking on links coming from trusted people. This item had the lowest positive value (46%) in Finding 04.

Students showed also to be aware of their attitudes and behaviors (Figure 7a) towards cybersecurity in school, where items A7 (*Computer systems provide all the protection a school need*) and B11 (*Checking update software*) on Finding 05 attained the lowest positive values, 51% and 58% respectively.

The attitudes related to understanding cybercriminals' motivations (Figure 7b) were positive, where item A22 (*Cybercriminals only target a school when there is a substantial financial gain*) presented the lowest value for positive attitude (52%) on Finding 06. Attitudes related to law enforcement and ICT technicians are positive (Figure 7b), where item A10 (*Cybercriminals are more advanced than the people who are supposed to be protecting us*) achieved a very low positive value (31%) on Finding 07.

Students are aware about protecting their equipment and data (Figure 7c) however, concerning checking for updates for anti-virus programs (item B18). Students also showed to have a very low positive behavior (38%) on Finding 08, and to have a positive behavior about using unofficial and copyright protected software (Figure 7c), on Finding 09 (item B12).

The distribution of the global score of attitudes and behaviors is depicted in Figure 8, where the values range between 20 and 140 for the behaviors and between 25 and 100 for the attitudes. Low values represent positive behaviours, while high values represent good attitudes. It is possible to observe a positive skewed distribution on the behavior scale, where 75% of the students obtained a global score up to 50, which shows a globally positive behavior attained. Regarding attitudes, a mean (standard deviation) global value of 76 (7.7) was obtained, showing that globally students presented positive attitudes.

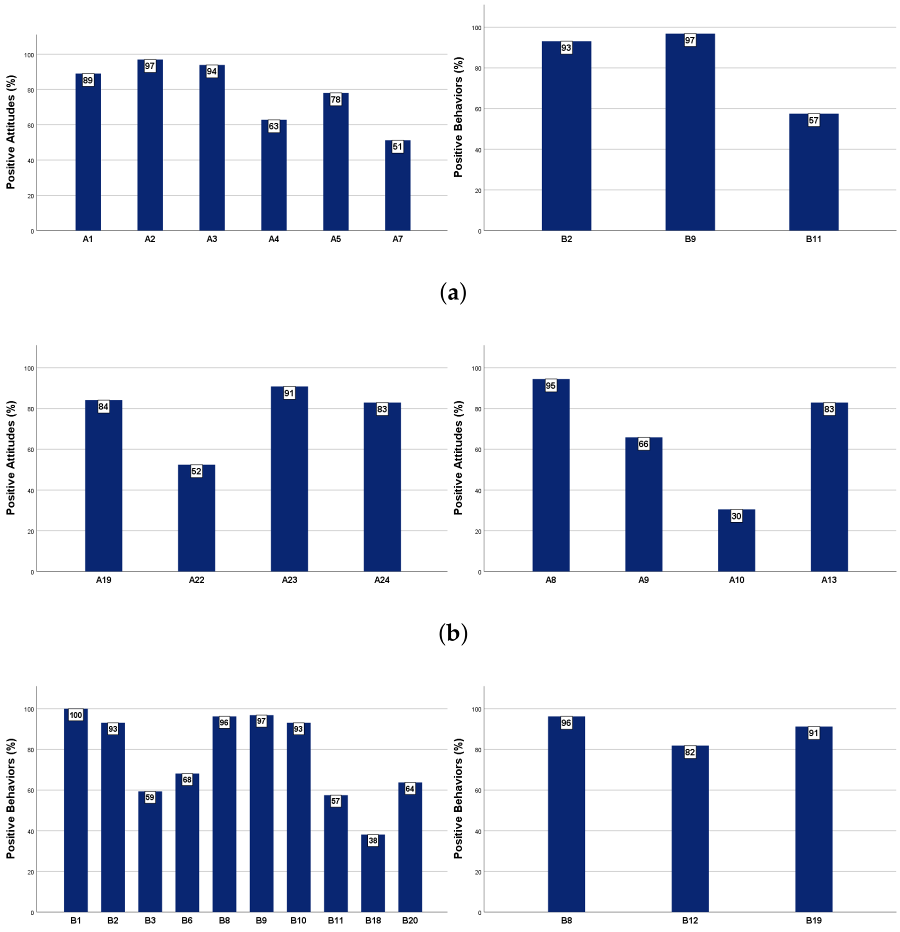


(**a**)

(**b**)

(**c**)

Figure 6. Findings: Attitudes and behaviors. (**a**) Finding 01—attitudes and behaviors. (**b**) Finding 02—attitudes and behaviors. (**c**) Findings 03 and 04—attitudes and behaviors.



(**a**)

(**b**)

(**c**)

Figure 7. Findings: attitudes and behaviors. (**a**) Finding 05—attitudes and behaviors. (**b**) Findings 06 and 07—attitudes. (**c**) Findings 08 and 09—behaviors.

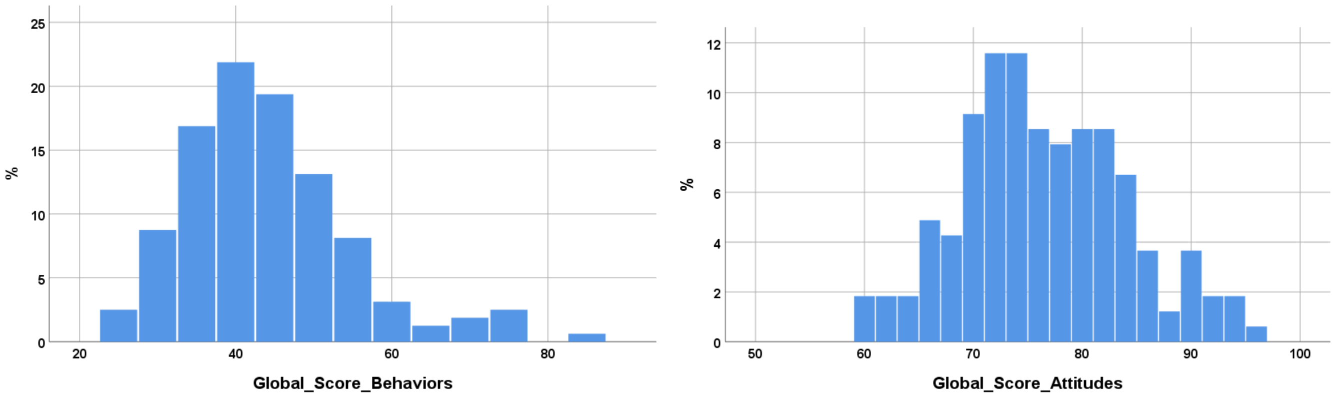
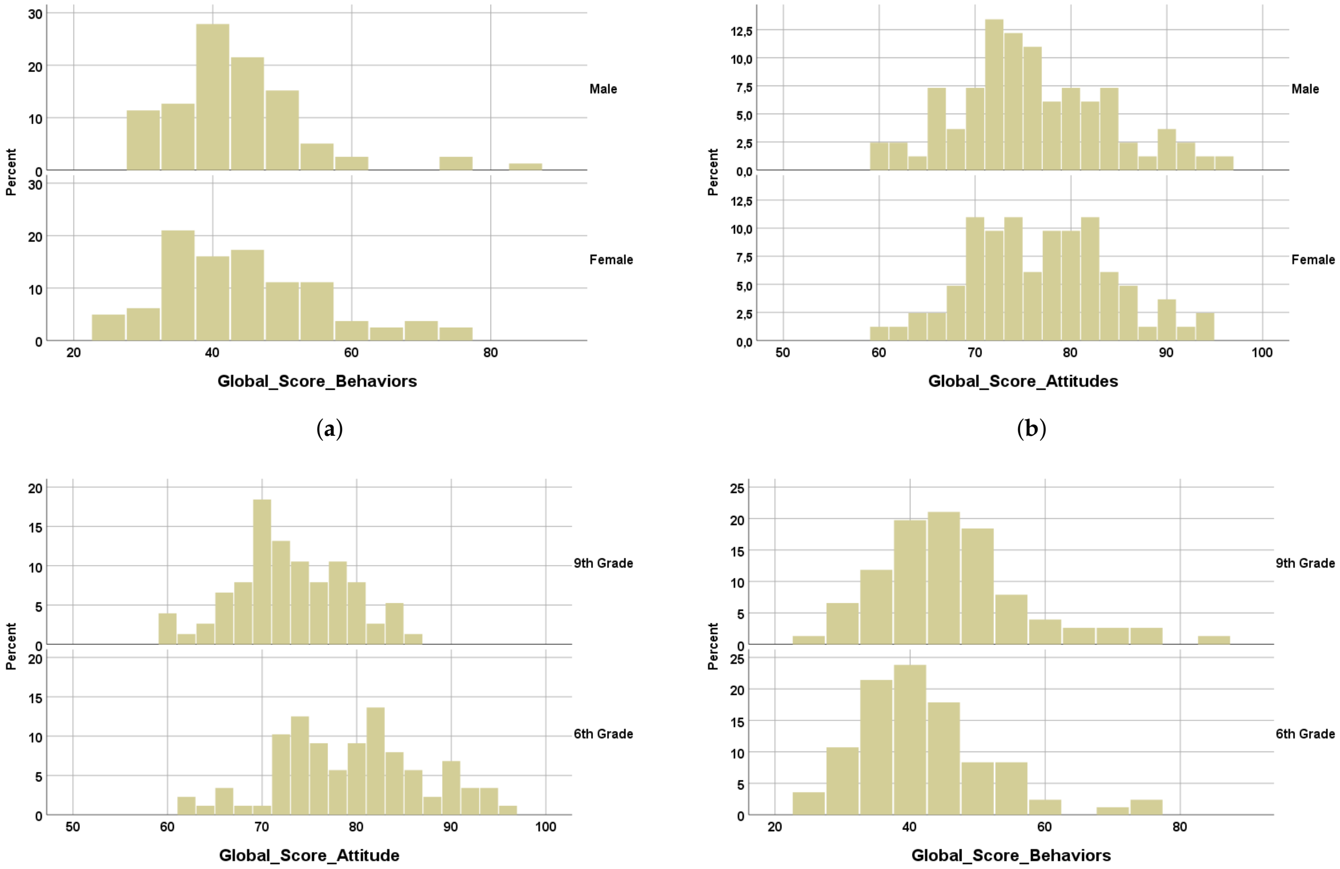


Figure 8. Distribution of global behaviors and attitudes.

The mean value of the global score of behavior (t = 0.38 , p = 0.704) and attitudes (t = 0.789 , p = 0.431) between gender were compared and no significant differences were found (Figure 9a,b).

In Figure 9a,c the distribution of the global scores attained for attitudes by grade are represented, and concerning both significant differences were observed (global behavior: $t = -2.731$, $p = 0.007$; global attitude: $t = 6.035$, $p < 0.001$), and it can be observed that students of 6th grade showed to have higher positive attitudes and behaviors. This fact may infer the need to invest more in cyberawareness in the 9th grade students. The fact that these students have more information and apparently have more experience with the electronic devices and digital applications may give them a more relaxing attitude regarding cyberawareness.

Since significant differences were observed between the global scores of behaviors and attitudes, all the items of both questionnaires between 6th and 9th grades were compared. Table 4 presents the questions where significant differences were found and the corresponding *p*-value obtained using the Mann–Whitney non-parametric test.



(**a**)

(**b**)

(**c**)

(**d**)

Figure 9. Distribution of global behaviors and attitudes. (**a**) Distribution of global score of behaviors by gender. (**b**) Distribution of global score of attitudes by gender. (**c**) Distribution of global score of attitudes by grade. (**d**) Distribution of global score of behaviors by grade.

Table 4. Cybersecurity Attitudes and Behavior questions where significant differences were found between grades.

ID	Question	*p*-Value [a]
A1 *	I believe that it is safe to ignore update warnings from computer software	0.010
A2	I am aware of my role in keeping the school protected from potential cybercriminals	<0.001
A5 *	I don't have the right skills to be able to protect the school from cybercrime	0.016
A6	I believe that personal information should not be revealed online, namely who I am, where I live or which school I attend	0.002
A8 *	I think that reporting cybercrime is a waste of time	0.002
A9 *	The Police lack the capacity to deal with cybercrime effectively	<0.001
A10 *	I believe that cybercriminals are more advanced than the people who are supposed to be protecting us	0.008
A11 *	I would download copyright material (images, documents, videos)	<0.001
A13 *	I worry that if I report a cyberattack to the Police it might damage the reputation of the school	<0.001
A15	I am aware of the schools IT use policy and attempt to follow it	<0.001
A16 *	I would not know how to report a cyberattack if one happened	0.008
A17 *	I don't think that reporting a cyberattack launched from the school is my responsibility	0.004
A18 *	I don't pay attention to school material about the threats from cybercrime	<0.001
A19	I am confident that I would be able to spot the signs of a cyber-attack	0.023
A20	I believe that, when inappropriate content appears online, I should ask for help from an adult	<0.001
A25 *	I think that I have the right to be always online, with access to all Internet services	0.008
B3	Using the same password for multiple websites	0.001
B4	Using online storage systems to exchange and keep personal or sensitive information	0.029
B5	Entering payment information on websites that have no clear security information/certification	0.003
B9	Disabling the anti-virus on my computer so that I can download information from websites	0.005
B12	Downloading digital media (music, films, games) from unlicensed sources	0.017
B13	Sharing my current location on social media	<0.001
B19	Downloading data and material from websites on your computer without checking its authenticity	0.034

* Items negatively worded were reverse-scored for further analysis; [a] Mann–Whitney non-parametric test.

5. Conclusions and Future Work

This paper has described a three-fold integrated cybersecurity and cyberawareness strategy, composed of risky attitudes and behaviors assessment, a self-diagnosis questionnaire, and a lesson plan. The integrated strategy was implemented and tested in a junior high school, with 6th and 9th grade students. CsA-S and CsB-S questionnaires evaluated the risky behaviors and attitudes towards cybersecurity and were filled by 164 respondents. The self-diagnosis questionnaire was made available for the same students who also benefited from the implementation of a lesson plan designed for digital citizenship classes.

Globally, the cybersecurity consciousness of the school administration, students, and parents was a major challenge, as these players were not initially too aware of the importance of the subject and the positive impact of an assessment to enhance students' cybersecurity skills. The implementation of this research study and the dissemination of the results in the school brought additional consciousness regarding the need to implement integrated cyberawareness in the school.

The global results obtained with the cybersecurity assessment questionnaires reveal that 6th grade students are globally more aware than those attending 9th grade. Despite the latter being older, and thus they should be globally more aware, this result suggests they are also more relaxed in applying cybersecurity best practices. It also suggests the need to intensify additional cyberawareness measures in this age group.

The following possible further developments were identified along with the research. It is possible to improve what can be measured; we should promote the dissemination of the attitude and behavior assessment questionnaires to other schools in the community. Besides the data enrichment, it should give an important additional management instrument for the educational authorities to promote cybersecurity and cyberhygiene habits in the schools.

Regarding the self-diagnosis application, gamification has to be seen as the next stage. The development of a gamified mobile version with "reward" mechanisms would disseminate the continuous and wide use of the cybersecurity self-diagnosis application.

The impact of the teaching/learning strategies in the students' cyberawareness perception should also be measured. Further developments include the application of the questionnaires to the students after the implementation of the lesson plan. The cyberawareness strategy is being adopted concerning other groups, namely parents, teachers, staff, and administration.

The proposed strategy and methodology is also suitable to be applied in distinct contexts, namely SMEs and public sector institutions in order to raise the cybersecurity level among the employees. Despite the need to eventually adjust the questionnaires to a specific context, the global strategy can be applied to a wide range of institutions and businesses, aiming to raise the cybersecurity and cyberawareness level.

Author Contributions: Conceptualization, M.A., C.S. and F.M.; Data curation, C.S. and F.M.; Formal analysis, M.A., C.S. and F.M.; Funding acquisition, M.A.; Investigation, M.A., C.S. and F.M.; Methodology, M.A. and C.S.; Software, F.M.; Supervision, M.A. and C.S.; Validation, M.A. and C.S.; Visualization, C.S. and F.M.; Writing—original draft: M.A., C.S. and F.M.; Writing—Review &; Editing: M.A., C.S. and F.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy concerns and the need to be made anonymous on request.

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

Abbreviations

The following abbreviations are used in this manuscript:

ABIS	ABbreviated Impulsiveness Scale
ATC-IB	Attitudes Towards Cybersecurity and Cybercrime in Business
CsA-S	Cybersecurity Attitudes in Schools
CsB-S	Cybersecurity Behaviors in Schools
CSIRT	Computer Security Incident Response Teams
ENISA	European Union Agency for Network and Information Security
HAIS-Q	Human Aspects of Information Security Questionnaire
ICT	Information and Communication Technology
KAB	Knowledge, Attitudes, and Behaviors
NGO	Non-Governmental Organizations
OCS	Online Cognition Scale
RScB	Risky Cybersecurity Behaviors Scale
SME	Small–Medium Enterprises

References

1. Bellovin, S.M. Layered Insecurity. *IEEE Secur. Priv.* **2019**, *17*, 96–95. [CrossRef]
2. Craig, T. Net of Insecurity: A Flaw in the Design. The Internets Founders Saw Its Promise But Didnt Foresee Users Attacking One Another. USA, 2015. https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/ (accessed on 22 October 2021).
3. Dawson, J.; Thomson, R. The future cybersecurity workforce: going beyond technical skills for successful cyber performance. *Front. Psychol.* **2018**, *9*, 744. [CrossRef] [PubMed]
4. Goel, S.; Williams, K.; Dincelli, E. Got phished? Internet security and human vulnerability. *J. Assoc. Inf. Syst.* **2017**, *18*, 2. [CrossRef]
5. Ancis, J.R. The Age of Cyberpsychology: An Overview. *Technol. Mind Behav.* **2020**, *1*. [CrossRef]
6. Hadlington, L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* **2017**, *3*, e00346. [CrossRef] [PubMed]
7. Vervier, L.; Zeissig, E.M.; Lidynia, C.; Ziefle, M. Perceptions of Digital Footprints and the Value of Privacy. In Proceedings of the IoTBDS, Prague, Czech Republic, 7–9 May 2017; pp. 80–91.
8. Levy, Y.; Gafni, R. Introducing the concept of cybersecurity footprint. *Inf. Comput. Secur.* **2021**, *29*, 724–736. [CrossRef]
9. Navaridas-Nalda, F.; Clavel-San Emeterio, M.; Fernández-Ortiz, R.; Arias-Oliva, M. The strategic influence of school principal leadership in the digital transformation of schools. *Comput. Hum. Behav.* **2020**, *112*, 106481. [CrossRef]
10. Demartini, C.G.; Benussi, L.; Gatteschi, V.; Renga, F. Education and digital transformation: The âĂIJriconnessioniâĂİ project. *IEEE Access* **2020**, *8*, 186233–186256. [CrossRef]
11. Slusky, L.; Partow-Navid, P. Students information security practices and awareness. *J. Inf. Priv. Secur.* **2012**, *8*, 3–26. [CrossRef]
12. Hanus, B.; Wu, Y.A. Impact of usersâĂŹ security awareness on desktop security behavior: A protection motivation theory perspective. *Inf. Syst. Manag.* **2016**, *33*, 2–16. [CrossRef]
13. Richardson, M.D.; Lemoine, P.A.; Stephens, W.E.; Waller, R.E. Planning for Cyber Security in Schools: The Human Factor. *Educ. Plan.* **2020**, *27*, 23–39.
14. Tirumala, S.S.; Sarrafzadeh, A.; Pang, P. A survey on Internet usage and cybersecurity awareness in students. In Proceedings of the 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016; pp. 223–228.
15. Zwilling, M.; Lesjak, D.; Natek, S.; Phusavat, K.; Anussornnitisarn, P. How to deal with the awareness of cyber hazards and security in (Higher) education. In Proceedings of the Thriving on Future Education, Industry, Business and Society. Proceedings of the Makelearn and TIIM International Conference, Piran, Slovenia, 15–17 May 2019; pp. 433–439.
16. Rahman, N.; Sairi, I.; Zizi, N.; Khalid, F. The importance of cybersecurity education in school. *Int. J. Inf. Educ. Technol.* **2020**, *10*, 378–382. [CrossRef]
17. Livingstone, S.; Haddon, L.; Görzig, A.; Ólafsson, K. Risks and Safety on the Internet: The Perspective of European Children: Full Findings and Policy Implications from the EU Kids Online Survey of 9–16 Year Olds and Their Parents in 25 Countries. Online Report 06.3, 2011. Available online: http://eprints.lse.ac.uk/33731/ (accessed on 22 October 2021).
18. Smahel, D.; Machackova, H.; Mascheroni, G.; Dedkova, L.; Staksrud, E.; Ólafsson, K.; Livingstone, S.; Hasebrink, U. EU Kids Online 2020: Survey Results from 19 Countries. Online Report. Available online: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf (accessed on 24 october 2021).
19. eukidsonline.net. Available online: http://www.eukidsonline.net/ (accessed on 19 October 2021).

20. Mee, P.; Brandenburg, R.; Lin, W. Oliver Wyman Forum Global Cyber Risk Literacy and Education Index. Oliver Wyman Forum, Octubre, 2020. Available online: https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index.html (accessed on 26 November 2021).
21. Pfleeger, S.L.; Caputo, D.D. Leveraging behavioral science to mitigate cyber security risk. *Comput. Secur.* **2012**, *31*, 597–611. [CrossRef]
22. McCormac, A.; Zwaans, T.; Parsons, K.; Calic, D.; Butavicius, M.; Pattinson, M. Individual differences and information security awareness. *Comput. Hum. Behav.* **2017**, *69*, 151–156. [CrossRef]
23. Boletsis, C.; Halvorsrud, R.; Pickering, J.B.; Phillips, S.C.; Surridge, M. Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. In *VISIGRAPP (3: IVAPP)*; Scitepress: SetÃžbal, Portugal, 2021; pp. 266–274.
24. Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *J. Cybersecur. Priv.* **2021**, *1*, 219–238. [CrossRef]
25. Nunes, P.; Antunes, M.; Silva, C. Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. *Procedia Comput. Sci.* **2021**, *181*, 173–181. [CrossRef]
26. ENISA. *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*; European Union Agency for Network and Information Security: Athens, Greece, 2018.
27. Furnell, S.; Esmael, R.; Yang, W.; Li, N. Enhancing security behaviour by supporting the user. *Comput. Secur.* **2018**, *75*, 1–9. [CrossRef]
28. Alshaikh, M. Developing cybersecurity culture to influence employee behavior: A practice perspective. *Comput. Secur.* **2020**, *98*, 102003. [CrossRef]
29. Giannakas, F.; Papasalouros, A.; Kambourakis, G.; Gritzalis, S. A comprehensive cybersecurity learning platform for elementary education. *Inf. Secur. J. A Glob. Perspect.* **2019**, *28*, 81–106. [CrossRef]
30. Quayyum, F. Cyber security education for children through gamification: Challenges and research perspectives. In *International Conference in Methodologies and intelligent Systems for Techhnology Enhanced Learning*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 258–263.
31. Quayyum, F. Cyber security education for children through gamification: Research plan and perspectives. In Proceedings of the 2020 ACM Interaction Design and Children Conference: Extended Abstracts, London, UK, 21–24 June 2020; pp. 9–13.
32. Best Security Awareness Training Software in 2021 | G2. Available online: https://www.g2.com/categories/security-awareness-training/ (accessed on 19 October 2021).
33. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A comparative study. *J. Comput. Inf. Syst.* **2020**, 1–16. [CrossRef]
34. Aldawood, H.; Skinner, G. Educating and raising awareness on cyber security social engineering: A literature review. In Proceedings of the 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, NSW, Australia, 4–7 December 2018; pp. 62–68.
35. ENISA. *Reference Incident Classification Taxonomy-Task Force Status and Way Forward*; European Union Agency for Network and Information Security: Athens, Greece, 2018.
36. ENISA. Material. Available online: https://www.enisa.europa.eu/media/multimedia/material/ (accessed on 20 October 2021).
37. Field, A. *Discovering Statistics Using SPSS*; Sage Publications: Washington, DC, USA, 2009.