Multimodal Technologies and Interaction

MDPI

Article

Improving Children's E-Safety Skills through an Interactive Learning Environment: A Quasi-Experimental Study

Iolie Nicolaidou [1,*] and Agnes Venizelou [2]

[1] Department of Communication and Internet Studies, Cyprus University of Technology, 30 Arch. Kyprianos Str., Limassol 3036, Cyprus
[2] Datatech Information Technology (I.T.) Solutions Ltd. 2 Sotira Street, Strovolos, Nicosia 2035, Cyprus; agnesv@datatech.com.cy
* Correspondence: iolie.nicolaidou@cut.ac.cy; Tel.: +357-(25)-002105

Received: 12 March 2020; Accepted: 7 April 2020; Published: 9 April 2020

Abstract: There is a worldwide concern for young children's online safety and a growing necessity for e-safety skills to be taught to children from a young age as part of formal schooling. The purpose of this study was to design and evaluate the effectiveness and motivational capacity of an interactive web-based learning environment for improving children's e-safety skills. A quasi-experimental pre-test post-test control group design was used with an experimental group of 48 sixth-grade primary school students, who used the web-based learning environment over two 80-min lessons, and a control group of 25 students who did not. Findings revealed a statistically significant difference ($t(47) = -14.06$, $p < 0.01$) in the experimental group students' e-safety performance, when students' pre-test scores (mean (M) = 41.13, SD = 10.47) were compared to their post-test scores (M = 56.69, SD = 9.38). The analysis of an attitudes questionnaire and of student interviews documented the experimental group students' positive attitudes toward the learning environment. Findings provide evidence of the effectiveness and motivational capacity of the web-based learning environment, which can be used in either formal education or informal learning settings, for improving children's e-safety skills.

Keywords: e-safety skills; children; personal data protection; avoiding hackers; cyberbullying; protection from malware; multimedia; interactive; web-based learning environment

1. Introduction

Children are spending increasing amounts of time online prompting practitioners and parents to raise concerns about their online safety [1]. E-safety, a person's skill to effectively respond to the challenges and opportunities offered by the internet [2], is an important skill that needs to be taught to children from a young age in formal schooling. Cyberethics, cybersafety, and cybersecurity, also known as C3, are three overlapping domains of knowledge [3] that can be seen as components of e-safety. According to Pusey and Sadera (2011), cyberethics are the moral choices individuals make when using the internet and digital media. Cyberethics issues include the protection of copyright, online etiquette, hacking, and online addiction. Cybersafety, according to the same authors, consists of the actions individuals take to minimize the dangers they could encounter when using the internet. Cybersafety issues include online predators and unwanted communications, as well as avoiding viruses, spyware, malware, and their spreading to other users. The last one of the three Cs, cybersecurity, involves the technical interventions that protect data, identity information, and hardware from unauthorized access or harm. Cybersecurity includes antivirus software, filters to avoid specific internet content, firewalls, and password protection [3].

E-safety is an area of interest for both academics and social policymakers [4]. The recognition of e-safety as an important skill for citizens to have from an early age, resulted in attempts to inform children, parents, and educators on online safety issues. This was done through several initiatives in schools worldwide [5] while the topic also received the attention of mass media worldwide. Moreover, since 2004, the "Safer Internet Day", a day dedicated to raise awareness of emerging online safety issues, which is celebrated in approximately 160 countries worldwide, is a landmark yearly event with respect to online safety. Events and activities such as the "Safer Internet Day" aim to promote the safer and more responsible use of online technologies, especially among children and young people across the world.

Three major risks children face online are associated with (a) personal data, (b) cyberbullying, and (c) malware. These three risks fall under the three overlapping domains of knowledge, cyberethics, cybersafety, and cybersecurity [3] that can be seen as components of e-safety. With respect to the first major risk, the vulnerability of personal data, young children often lack knowledge on privacy issues, which results in posting a large volume of personal data online [6]. Young children often voluntarily release personal data in public profiles of online social networks. The European Union (EU) kids online survey, conducted with children aged 9–15 in 25 European countries, showed that 25% of children aged 9–12 who use social networks have their profile as "public" and 20% of them have their address and/or phone number listed on their profile [7]. Children who are not aware of privacy protection on the internet often post inappropriate messages, images, and video, ignoring the permanency of online posts.

A second major risk typically faced by children when they are online refers to experiencing cyberbullying. Similar to bullying in face-to-face social interactions, two main characteristics indicative of cyberbullying behavior are the repetition intensity over time and the power imbalance between the victims and the bullies [8]. Cyberbullying is a danger that children have to be protected from as some of its negative consequences for the victim include feelings of depression, confusion, guilt, shame, self-harm, and avoiding peers and family members [9], while, in extreme cases, the victim may have suicidal thoughts or even commit suicide [6].

The third major risk that children face online refers to receiving malicious software threats. Children constitute easy targets for hacker attacks; therefore, they should know how to protect themselves from hackers [10], as well as know how to use antivirus software [11]. Malware software such as viruses, trojans, worms, and spyware [12] aims to destroy the operating system of a computer, allowing hackers to obtain access to the user's personal data [13], such as a user's password, to access a computer and data from a user's online account.

A literature review showed that there is a necessity for online safety to be taught [1,14]. For example, the study of Annansingh and Veli (2016) which focused on 271 children aged 7–11 years and investigated how they interact online, highlighted that e-safety policies and procedures are not kept up to date with technological advances and concluded that more resources are needed to educate children on safe practices on the internet [14]. Recognizing the importance of supporting children develop e-safety skills, several research studies conducted across the world used online gamified activities, multimedia, and stories to teach e-safety to students, focusing on different aspects of e-safety, such as the protection of personal data [15,16], cyberbullying [16,17], or protection from hackers [12]. Results from these studies were encouraging in general. The evaluation of Net-Detectives, a creative online role play activity aimed at 9–12-year-olds which focused on the protection of personal data, for example, showed that students learned about internet safety in a motivating and challenging environment [15]. Another example of an online game that focused on the protection of personal data is "Cybersmart Detectives", which was developed especially for primary school students to teach e-safety. The game was used by 292 students in nine schools, and it was evaluated by a sample of students using a brief questionnaire related to their habits online and their use of mobile devices, which was administered to students before and after their experience with the game. Results showed that the game was beneficial for both high-risk and low-risk students, as both groups reported significantly more positive actions at post-test

than pre-test [18]. Other studies that focused on personal data protection provided guidelines on what works in terms of improving and raising e-safety awareness in primary schools, as well as the barriers and challenges schools may face in trying to implement them [16]. With respect to computer security and protection from hackers, "Auction Hero" is an example of a simulation game which models life online to improve users' mental models of computer security and to help users make more secure decisions. The cognitive walkthrough evaluation of the first prototype of that game revealed general enthusiasm by its first users [12].

In the majority of the studies that were reviewed, there were no quantified results of students' performance with respect to the development of their e-safety skills, as most studies focused on users' self-reported measures and did not objectively evaluate students' performance in e-safety tests [16,19,20]. Another limitation of some of these studies refers to the fact that, even though they had adequate sample sizes, they did not include sufficient quantified results [16,17,20], but rather presented their findings using general terms or were qualitative in nature [21].

With respect to their focus, only one study was identified that specifically focused on familiarizing users with common online attacks and common computer security risks [12], such as phishing, viruses, attacks from hackers, etc., on helping them recognize the attacks, and on teaching them how to protect themselves, e.g., by using an antivirus system. This particular study focused on post-secondary education and not on children. The component of e-safety that relates to computer security risks and common online attacks seems to be understudied, compared to the components of protecting personal data and avoiding cyber bullying. There is, however, a need to teach students how to protect themselves from hackers from an early age.

The Need for This Study

Studies that focused on teaching e-safety skills to children through technology-based interventions were reviewed. In the majority of research studies that focused on teaching protection of personal data and avoiding cyberbullying, there were no quantified results of students' performance with respect to the development of their e-safety skills, through diagnostic tests. Most of the previous studies were based on self-reported data. However, the findings of the study conducted by Macaulay et al. (2019) with 329 children, aged 8–11 years, suggest that "some children may think that they know how to stay safe online but lack objective knowledge that could actually keep them safe. Consequently, there is a need to assess children's objective knowledge of online safety (and online) dangers and to provide appropriate education for children who currently lack it" [1] (p. 1).

Moreover, no research focused on teaching malware risks to primary school children, which seems to be an understudied area. Additionally, according to Laouris et al. (2011), most strategies for teaching internet safety that target children focused more on providing information and less on children's active engagement [19].

To address these gaps, the present study aimed to design, develop and evaluate an interactive web-based learning environment called "Be smart when online!", which engages students on every step through interactive games, quizzes, activities, and discussion forums. The purpose of this study was to evaluate the interactive web-based learning environment "Be smart when online!" with respect to (a) its effect on improving children's e-safety skills and (b) its motivational capacity.

As there were no quantified results of students' performance with respect to the development of their e-safety skills in the majority of studies that were reviewed, in the present study, the learning environment "Be smart when online!" was evaluated through quantified results of student tests, administered prior to and after the intervention. The analysis of these tests revealed a statistically significant difference ($t(47) = -14.06$, $p < 0.01$) in the experimental group students' e-safety performance, when students' pre-test scores (mean (M) = 41.13, SD = 10.47) were compared to their post-test scores (M = 56.69, SD = 9.38). Control group students did not experience a statistically significant difference in their e-safety skills. The analysis of an attitudes questionnaire and the analysis of student interviews documented the experimental group students' positive attitudes toward the learning environment.

This provides an indication that the designed learning environment seems to be an effective and motivational way for students to develop their e-safety skills with respect to protecting personal data, avoiding hackers, and combating cyberbullying.

2. Materials and Methods

2.1. Research Questions

The study attempted to answer the following two research questions:

Research question 1: Is the learning environment "Be smart when online!" effective for the development of sixth-grade students' e-safety skills?

Research question 2: What are students' attitudes toward the learning environment "Be smart when online!"?

2.2. Research Design and Participants

The study followed a quasi-experimental, pre-test, post-test control group design. Three primary schools with access to a computer lab were chosen using convenience sampling to participate in the study. There was a total of 48 (26 boys, 22 girls) sixth-grade primary school students who acted as participants in the experimental group and used the web-based learning environment over two 80-min lessons. There were 25 sixth-grade primary school students (14 boys, 11 girls) who acted as participants in the control group and did not receive formal instruction of e-safety skills.

The research protocol of the study was approved by the Center for Educational Research and Evaluation (Proposal submission number 7.15.06.15.1/2) prior to conducting the study and followed American Psychological Association (APA) ethical standards and General Data Protection Regulation (GDPR) guidelines. All participants were informed in writing about the objective of the study, and students' parents signed consent forms for their children to voluntarily participate in it.

2.3. Learning Environment "Be Smart When Online!"

The learning environment "Be smart when online!" targets 11- to 12-year-old children and consists of three main parts. The first part attempts to help students identify their prior knowledge on the topic of e-safety through an embedded pre-test of 20 multiple-choice questions, in the form of scenarios, to which they receive instant feedback. The second part is the instructional part, which covers three areas: (a) protection of personal data, (b) avoiding cyberbullying, and (c) protection from hackers. The instructional part includes multimedia, such as videos, images, presentations, interactive activities, and discussion forums. In this part, children are engaged in learning and can practice their skills through interactive quizzes and games with instant feedback, and they can reflect on their learning by posting comments in discussion forums. The third and last part consists of an embedded post-test, which is identical to the pre-test, encouraging students to achieve a higher score. The estimated duration of an intervention that follows the structure of the learning environment in a formal education setting is two 80-min lessons.

Prior to this study, the learning environment was pilot-tested with a group of 25 children attending summer school in university premises [22]. Twenty-one of those students attended the fourth to sixth grade of primary school and four children attended the seventh to ninth grade. Instruments were also pilot-tested to verify that they were understandable and that they could be completed by students independently. A paired-samples *t*-test revealed a statistically significant difference ($t(18) = -3.96$, $p < 0.01$) when students' pre-test scores (M = 84.74, SD = 8.74) were compared to their post-test scores (M = 92.36, SD = 9.33), providing preliminary results indicating its effectiveness. A few changes were made as a result of this pilot test to improve the learning environment prior to enacting it in classrooms in formal education [22].

2.4. Experimental Setting

In this study, the learning environment was used by experimental group students who were working individually or were interacting in dyads in computer labs at public primary schools over two 80-min sessions. The second researcher was present during all sessions, but she did not provide any pedagogical support or guidance to the children. Technical support was provided in a few instances. Control group students did not receive formal instruction with respect to e-safety. They took the same online pre-tests and post-tests and the same written tests as the experimental group students, during the same timeframe. Control group students received immediate feedback on their online pre-test, as experimental group students did.

2.5. Data Sources

Four data sources were used in this study: (a) an online test assessing e-safety skills with 20 multiple choice scenarios, (b) a written test assessing e-safety skills with six open-ended questions, (c) a questionnaire with 18 Likert-scale questions assessing students' attitudes toward the learning environment, and (d) a student interview protocol assessing students' knowledge and attitudes.

The effectiveness of the learning environment is operationalized as the statistically significant increase between students' e-safety pre-test and post-test scores. Students' e-safety skills were assessed using two tests. The first test was based on 20 scenarios that students had to reflect on before answering multiple choice questions consisting of four plausible answers. The test included seven scenarios on the protection of personal data, six scenarios on the protection from hackers, six scenarios on avoiding cyberbullying, and one scenario which combined all three areas. The test was embedded in the learning environment. The maximum possible score of the test was 100. An example of a scenario on the protection of personal data was the following:

"David has been chatting over the last two weeks with someone with whom he shares a hobby. They're thinking of meeting in person on Saturday and they're looking for a meeting place. What would you advise David to do?

Option 1: Go to the cinema, there's a premiere of a movie.

Option 2: Meet in a crowded place.

Option 3: Go for bowling.

Option 4: Inform his parents first."

The correct answer for a student who is a minor, such as the children of the target group of this study, is Option 4, to inform his parents or guardians first, before meeting in person with a stranger.

The second test that was used for the assessment of students' e-safety skills included six open-ended questions; two of these tested skills on protecting personal data, another two tested skills related to avoiding hackers, and the last two tested skills related to avoiding cyberbullying. Example questions were the following: "What are some rules that you know for protecting personal data? How can you protect yourself from malware? What would you advise someone who has been a victim of cyberbullying?". The maximum possible score of the test was 100.

The instrument that was used to assess students' attitudes toward the learning environment consisted of two demographic questions that included gender and frequency of use of the internet and 18 questions on a five-point Likert scale ranging from completely disagree (1) to completely agree (5). The questionnaire assessing students' attitudes toward the learning environment focused on the learning environment's affordances, interface, activities, pedagogical approach, and educational value, and students' motivation and active participation. Example statements assessing students' attitudes toward the learning environment referred to the following: "The learning environment was easy to use", "I liked instant feedback on my performance in the quizzes", and "I liked using this learning environment to learn about e-safety".

The student interview protocol included 15 open-ended questions, nine of which assessed knowledge and six of which assessed attitudes toward the learning environment. Example questions assessing knowledge were the following: "What do you know about personal data on the internet?"

and "What do you know about cyber bullying?". Example questions assessing attitudes toward the learning environment were the following: "What did you think of the learning environment?" and "Did you face any difficulties when using the learning environment?". Six students from the experimental group participated in individual semi-structured interviews that made use of this interview protocol.

2.6. Data Analysis

All quantitative data were input to a statistical package (IBM SPSS Statistics 25) for analysis. Students' e-safety skills were calculated as the composite score of the first and second tests assessing e-safety skills, which had an equal weight of 50%, resulting in a performance score on a scale of 1–100. Pre-test and post-test scores were compared for both groups, using paired samples *t*-tests.

Students' answers in the attitudes' questionnaire were calculated as a composite score consisting of their answers in 18 Likert-scale questions. There were two questions that were negatively phrased in the instrument in order to verify that students carefully read the statements before completing them and did not simply agree with the statements. An example of such a statement was the following: "I would prefer to learn about online safety using a book (instead of through a web-based learning environment)". Students' answers in the two statements that were negatively phrased were reversed before the calculation of the composite score. Descriptive statistics were used in reporting students' attitudes toward the learning environment.

An alpha level of 0.01 was set a priori for all statistical analyses.

Qualitative data from student interviews were transcribed verbatim and analyzed using content analysis.

3. Results

3.1. Establishing Group Equivalence

Participants were pre-tested with respect to their e-safety skills. Group equivalence was firstly established. There were no statistically significant differences among the two groups when an independent-samples *t*-test was performed ($t(71) = -0.14$, $p > 0.01$) to compare the pre-test of students' e-safety performance for the experimental group (M = 41.13, SD = 10.47) and for the control group (M = 41.49, SD = 10.68).

3.2. Is the Learning Environment "Be Smart When Online!" Effective for the Development of Sixth-Grade Students' E-Safety Skills?

The learners' e-safety performance score was compared pre- and post-intervention for the experimental and control group. Table 1 shows students' e-safety performance, pre and post, for the experimental group, whose members used the web-based learning environment, and for the control group, whose members did not use the web-based learning environment. The results showed that students' performance increased from 41.13 (SD = 10.47) to 56.69 (SD = 9.38) for the experimental group and from 41.49 (SD = 10.68) to 44.61 (SD = 12.73) for the control group. A paired samples *t*-test showed an overall statistically significant improvement in the experimental group when pre-test and post-test performance was compared ($t(47) = -9.01$, $p < 0.01$). The control group did not show a statistically significant improvement when pre- and post-test performance was compared ($t(24) = -2.19$, $p > 0.01$).

Table 1. Pre–post e-safety performance for experimental and control group. M—mean.

	Pre-Intervention M	SD	Post-Intervention M	SD
Experimental	41.13	10.47	56.69 **	9.38
Control group	41.49	10.68	44.61	12.73

** Statistically significant result ($p < 0.01$).

The next analysis focused on comparing students' progress in the two groups post intervention (Table 1). The experimental group (M = 56.69, SD = 9.38) outperformed the control group (M = 44.61, SD = 12.73) and an independent samples *t*-test revealed that this difference was statistically significant ($t(71) = 4.61$, $p < 0.01$). Cohen's *d* had a value of 1.08 in this study [23]. Following Cohen's (1992) suggestion that enables us to compare an experiment's effect-size results to known benchmarks, effect sizes of 0.20 are small, effect sizes of 0.50 are medium, and effect sizes of 0.80 are large [24]. Based on Cohen's suggestion, the effect size of the study qualifies as a large effect.

Findings from the quantitative analysis were triangulated with qualitative data from the analysis of student interviews. All six children who were interviewed were able to describe what is considered as personal data on the internet and provided several examples, while four out of six children referred to the importance of personal data. With respect to protecting personal data, four out of six children learned that they should not reveal their personal data or post their location online and that they should use strong passwords. Two out of six children learned that they should use a pseudonym in online discussion forums. Two children understood the concept of privacy of personal data of third parties, even if third parties are their friends. This is evident from the fact that they explicitly stated that they should not post photographs of their friends online unless they first obtain their permission.

From the interviews, it was evident that five out of six children learned what cyberbullying is, while four out of six children could provide examples of that constitutes cyberbullying. A boy for example said "(an example of a cyberbullying incident is) if a person finds a photo and edits it and changes his face, and then he posts it, and then everybody at school makes fun of him". When children were asked to think about actions against cyberbullying in cases where they are victims, all six of them reported that they should immediately inform an adult, such as a parent or their teacher. Three out of six children mentioned that they should never chat with strangers online, and four out of six children emphasized that they should not meet strangers in person. Three children said that they would ignore online messages that attempt to bully them, one child mentioned that he would block the perpetrator, and two children said that they would not delete incriminating messages so that they could report the incident to the police.

However, it should be noted that, as interviews were only conducted with experimental group students after the intervention, only post-test interview data were available. This weakness in the design of the study did not allow for a comparison between students' pre-test and post-test interviews. As a result, it cannot be claimed that students' documented knowledge with respect to e-safety through interviews was necessarily a result of their interaction with the learning environment.

3.3. What Are Students' Attitudes toward the Learning Environment "Be Smart When Online!"?

The composite score of the 18 (phrased as five-point Likert scale) statements that examined students' attitudes toward the learning environment was M = 4.44 (SD = 0.26) out of a maximum possible score of five, indicating that students had positive attitudes toward the learning environment, in general.

Table 2 shows the mean scores of each dimension of the questionnaire assessing students' attitudes toward the learning environment. The first five dimensions (affordances, interface, activities, pedagogy, and educational value) focused on the learning environment. The last two dimensions (motivation, active participation) focused on the students. All seven dimensions received high scores, indicating that students evaluated the aspects that were examined positively.

Table 2. Experimental group students' attitudes toward the learning environment "Be smart when online!".

Dimension	M	SD
Affordances	4.39	0.52
Interface	4.39	0.50
Activities	4.66	0.33
Pedagogy	4.49	0.44
Educational value	4.89	0.26
Motivation	4.54	0.39
Active participation	4.00	0.8
Composite score	4.44	0.26

Student responses in specific questions are presented next using net percent agreement (NPA), which is the composite score of frequencies and percentages of students who either agreed or strongly agreed with a statement, as suggested by Dunn et al. (2013) [25]. All students agreed or strongly agreed with the following statements: "Everything I learned about e-safety in the learning environment is important" (100%, 48/48) and "I learned a lot about e-safety through the learning environment" (100%, 48/48), which indicates that students saw the educational value of the environment. A very high percentage of 93.7% (45/48) of the students found the learning environment interesting. Almost all students (97.9%, 47/48) liked the interactivity that was provided by the quizzes that provided instant feedback. Students also liked the fact that they could repeat those quizzes to achieve a higher score for practicing purposes (91.7%, 44/48). They found the content understandable (87.6%, 42/48) and liked the images (83.4%, 40/48) and videos that were used (93.8%, 45/48).

Another finding that is worth mentioning refers to the fact that a relatively high percentage of students (77.1%, 37/48) agreed or strongly agreed with the statement that they worked in the learning environment independently without feeling the need to ask for help, which is a positive finding that shows that the learning environment could also be used at home for informal learning.

4. Discussion

This study was designed in response to calls in the literature for the need to create learning resources to teach e-safety skills to children of a young age. The evaluation of the learning environment "Be smart when online!" using a quasi-experimental pre–post control group design showed that the experimental group outperformed the control group when pre-test and post-test performance with respect to e-safety skills was compared, and this difference was statistically significant. The effect size of the study (Cohen's d = 1.08), which was higher than 0.8, qualified as a large effect size [24]. Qualitative data from student interviews confirmed this finding. This provides an indication that the designed learning environment "Be smart when online!" was effective in supporting children's e-safety skills with respect to three areas, the protection of their personal data, avoiding cyberbullying, and avoiding hackers, despite the short time of its class enactment. However, it should be noted that, as student interviews were not conducted prior to the beginning of the study, baseline data with respect to children's knowledge on e-safety were not available as qualitative data. Therefore, it is possible that students' reported knowledge on e-safety through interviews was not necessarily a direct result of their interaction with the learning environment. This is a methodological weakness, which was also observed in previous research studies in this area [16,17,19–21].

Students assumed an independent role in this study and used the learning environment without the need for support or guidance by a schoolteacher. The majority of students (77.1%, 37/48) stated that they could work in the learning environment independently and did not feel the need to ask for help. This indicates that the learning environment is not only appropriate for a classroom setting in formal education, but it can also be valuable as a resource for informal learning at home using mobile devices, without the need of parental support or guidance. This is partly made possible through the

use of gamified interactive activities in the learning environment that provide instant feedback and replayability to allow for increased performance scores over practice.

The analysis of attitudes data showed that students were enthusiastic, they thought that they learned a lot from the learning environment, and they enjoyed several of its features, such as quizzes with instant feedback, multimedia elements, and interactive activities. However, it should be acknowledged that the vast majority of statements in the attitudes questionnaire (16 out of 18 statements) were positively phrased statements, and this might have had an impact on the results. Positive student attitudes findings agree with what we know about effective learning environments on e-safety from the literature, from studies that followed a similar pedagogical approach, such as Net-Detectives [15], Cybersmart Detectives [18], SimSafety [19], and the Cybersmart program [17].

Previous studies did not measure learning benefits using standardized tests. The contribution of this study lies in that students' e-safety skills were measured pre and post using two tests which combined closed-ended questions based on realistic scenarios that children may face in their everyday life, and open-ended questions, whose inclusion helped to alleviate problems of random answers by students. Another contribution refers to the fact that, to the best of the authors' knowledge, the area of learning how to protect devices from malware, viruses, and hackers is an understudied area that did not receive adequate attention in research studies that included young children. This area was included as one of the three areas that the learning environment targeted, receiving equal attention as the protection of personal data and avoiding cyberbullying.

The study had several limitations, including a small sample size, the lack of a randomized sampling procedure, the lack of instruction on e-safety for the control group, and the lack of baseline interview data, which prohibit the generalizability of results. Moreover, the evaluation did not involve children's parents to understand if children were already exposed to e-safety learning or strategies.

5. Conclusions

In conclusion, this study described an interactive learning environment that can be used in formal education or in informal learning settings to increase young children's e-safety skills. The effectiveness of the learning environment for the development of children's e-safety skills was shown through a statistically significant increase of children's post-test performance as compared to their pre-test performance, and through the experimental group students' higher post-test performance as compared to control group students. The evaluation of the learning environment resulted in a large effect size. The motivational capacity of the web-based learning environment was shown through experimental group students' positive attitudes results. This study comes in response to calls to assess children's objective knowledge of online safety and to provide appropriate education for children who currently lack it [1], and it adds to the database of empirically validated, web-based learning resources to support the development of e-safety skills.

With respect to future work, the involvement of teachers and parents is considered crucial as they are both stakeholders who play an important role with respect to young children's e-safety strategies. Data collection in the form of interviews from children's teachers, parents, and close family members, such as older siblings, would be an invaluable addition that would strengthen the study's findings.

Author Contributions: Conceptualization, I.N. and A.V.; methodology, I.N. and A.V.; software, A.V.; validation, I.N. and A.V.; formal analysis, I.N. and A.V.; investigation, A.V.; resources, A.V.; data curation, A.V.; writing—original draft preparation, I.N.; writing—review and editing, A.V. and I.N.; visualization, A.V.; supervision, I.N.; project administration, A.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors would like to thank all the primary school students who voluntarily participated in this study.

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

References

1. Macaulay, P.J.; Boulton, M.J.; Betts, L.R.; Boulton, L.; Camerone, E.; Down, J.; Kirkham, R. Subjective versus objective knowledge of online safety/dangers as predictors of children's perceived online safety and attitudes towards e-safety education in the United Kingdom. *J. Child. Media* **2019**, 1–20. [CrossRef]
2. Litt, E. Measuring users' internet skills: A review of past assessments and a look toward the future. *New Media Soc.* **2013**, *15*, 612–630. [CrossRef]
3. Pusey, P.; Sadera, W.A. Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *J. Digit. Learn. Teach. Educ.* **2011**, *28*, 82–85. [CrossRef]
4. Lobe, B.; Livingstone, S.; Haddon, L. Researching Children' s Experiences Online Across Countries: Issues and Problems in Methodology. *Eu Kids Online* **2007**, 1–64. Available online: https://lirias.kuleuven.be/bitstream/123456789/200390/1/ReportD4.1MethodologicalIssuesCover.pdf (accessed on 21 February 2020).
5. Valcke, M.; De Wever, B.; Van Keer, H.; Schellens, T. Long-term study of safe Internet use of young children. *Comput. Educ.* **2011**, *57*, 1292–1305. [CrossRef]
6. O'Keeffe, G.S.; Clarke-Pearson, K. The impact of social media on children, adolescents, and families. *Pediatrics* **2011**, *127*, 800–804. [CrossRef] [PubMed]
7. Livingstone, S.; Ólafsson, K.; Staksrud, E. Social networking, age and privacy. *Eu Kids Online* **2011**, 1–13. Available online: http://eprints.lse.ac.uk/35849/ (accessed on 8 April 2020).
8. Chatzakou, D.; Leontiadis, I.; Blackburn, J.; Cristofaro, E.D.; Stringhini, G.; Vakali, A.; Kourtellis, N. Detecting Cyberbullying and Cyberaggression in Social Media. *ACM Tran. Web (TWEB)* **2019**, *13*, 1–51. [CrossRef]
9. Mishna, F.; Mcluckie, A.; Saini, M. Real-World Dangers in an Online Reality: A Qualitative Study Examining Online Relationships and Cyber Abuse. *Soc. Work Res.* **2009**, *33*, 107–118. [CrossRef]
10. Monteith, B. Hacking for Good and Bad, and How to Protect Yourself against Hacks ! *Knowl. Quest* **2016**, *44*, 60–64.
11. Nagarajan, A.; Allbeck, J.M.; Sood, A.; Janssen, T.L. Exploring game design for cybersecurity training. In Proceedings of the IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems, Bangkok, Thailand, 27–31 May 2012; pp. 256–262. [CrossRef]
12. Chiasson, S.; Modi, M.; Biddle, R. Auction Hero: The Design of a Game to Learn and Teach about Computer Security. *World Conf. E-Learn. Corp. Gov. Healthc. High. Educ.* **2011**, 2201–2206.
13. Fire, M.; Goldschmidt, R.; Elovici, Y. Online Social Networks: Threats and Solutions Survey. *IEEE Commun. Surv. Tutor. Online* **2014**, *16*, 1–18. [CrossRef]
14. Annansingh, F.; Veli, T. An investigation into risks awareness and e-safety needs of children on the internet: A study of Devon, UK. *Interact. Technol. Smart Educ.* **2016**, *13*, 147–165. [CrossRef]
15. Wishart, J.M.; Oades, C.E.; Morris, M. Using online role play to teach internet safety awareness. *Comput. Educ.* **2007**, *48*, 460–473. [CrossRef]
16. Shipton, L. Improving e-safety in primary schools: A guidance document. *Final Rep.* **2011**. Available online: https://www.researchgate.net/publication/275654352 (accessed on 24 February 2020).
17. Chadwick, R.; Knight, P. Cybersmart: Learning online safety. *J. Christ. Educ.* **2012**, *4*, 26–29.
18. Dooley, J.; Thomas, L.; Falconer, S.; Cross, D.; Waters, S. Educational Evaluation of Cybersmart Detectives. *Final Rep* **2011**. Available online: https://ro.ecu.edu.au/ecuworks2011/862/ (accessed on 7 March 2020).
19. Laouris, Y.; Aristodemou, E.; Fountana, M. Teaching Internet safety in virtual environments. *Int. J. Media Cult. Politics* **2011**, *7*, 67–76. [CrossRef]
20. Xenos, M.; Papaloucas, S.; Kostaras, N. The Evaluation of an Online Virtual Game Environment (SimSafety) using HOU's Software Quality Laboratory. In Proceedings of the Social Applications for Lifelong Learning, Patra, Greece, 4–5 November 2010; pp. 63–67. Available online: https://www.researchgate.net/profile/Michalis_Xenos/publication/258514592_The_Evaluation_of_an_Educational_Game_SimSafety_using_HOU\T1\textquoterights_Software_Quality_Laboratory/links/02e7e52878f212271a000000/The-Evaluation-of-an-Educational-Game-SimSafety-using-HOUs-Software-Quality-Laboratory.pdf_ (accessed on 24 February 2020).
21. Griffith Institute. The ACMA Cybersmart Outreach Program Evaluation. Qualitative Report. 2011. Available online: https://www.semanticscholar.org/paper/The-ACMA-cybersmart-outreach-program-evaluation%3A-Beavis-Pendergast/4e3b9f8b6779887949402d72cbfcc8c7d35bc0eb (accessed on 8 April 2020).

22. Nicolaidou, I.; Venizelou, A. "Be smart when online!": Kids learn how to protect personal data, stop cyber-bullying and avoid hackers. In Proceedings of the 9th International Conference of Education, Research and Innovation, Seville, Spain, 14–16 November 2016; pp. 3374–3383. [CrossRef]
23. Thalheimer, W.; Cook, S. How to calculate effect sizes from published research: A simplified methodology. *Work-Learn. Res.* **2002**, 1–9.
24. Cohen, J. A power primer. *Psychol. Bull.* **1992**, *112*, 155–159. [CrossRef] [PubMed]
25. Dunn, P.K.; Richardson, A.; Oprescu, F.; McDonald, C. Mobile-phone-based classroom response systems: Students' perceptions of engagement and learning in a large undergraduate course. *Int. J. Math. Educ. Sci. Technol.* **2013**, *44*, 1160–1174. [CrossRef]