Journal of Educational Studies and Multidisciplinary Approaches (JESMA)

www.jesma.net

E-Shield:Design, Implementation, And Evaluation of a Cybersecurity Education Program – a 6th Grade Example

Phd (s), Fatma ŞAHİN[1]
Prof. Dr. Semra DEMİR BAŞARAN[2]

To cite this article:

Sahin, F. & Demir-Basaran, S. (2025). E-Shield: Design, Implementation, And Evaluation of a Cybersecurity Education Program – A 6th Grade Example. *Journal of Educational Studies and Multidisciplinary Approaches (JESMA), 5* (1), 15-28. https://doi.org/10.51383/jesma.2025.118

The Journal of Educational Studies and Multidisciplinary Approaches(JESMA) is an international scientific, high-quality open access, peer-viewed scholarly journal that provides a comprehensive range of unique online-only journal submission services to academics, researchers, advanced doctoral students, and other professionals in their field. This journal publishes original research papers, theory-based empirical papers, review papers, case studies, conference reports, book reviews, essays, and relevant reports twice a year (March and September)

[1] Fatma Sahin, Erciyes Universty, Kayseri, Türkiye, fatmadagdelensahin@gmail.com

[2] Prof.Dr. Semra Demir-Basaran, Erciyes University, Kayseri, Türkiye, sdemir@erciyes.edu.tr

Journal of Educational Studies and Multidisciplinary Approaches (JESMA)
Volume 5, Issue 1 Year 2025 ISSN:2757-8747

E-Shield: Design, Implementation and Evaluation of a Cybersecurity Education Program – A 6th Grade Example

Fatma Sahin https://orcid.org/0000-0002-8686-0057

Semra Demir Basaran https://orcid.org/0000-0002-5245-7657

ARTICLE INFORMATION

Original Research

DOI: 10.51383/jesma.2025.118
Received 27 January 2025
Revision 15 March 2025
Accepted 19 March 2025

ABSTRACT

This study examines the development, implementation, and evaluation processes of the e-Shield instructional program, designed using the Morrison, Ross, and Kemp model to enhance sixth-grade students' knowledge, skills, and awareness of cybersecurity. With the rapid advancement of technology, cybersecurity has become a crucial issue for both individuals and society. However, a review of the literature indicates that students lack sufficient knowledge and awareness regarding cybersecurity. To address these deficiencies, effective instructional programs must be developed. Accordingly, the e-Shield instructional program was implemented with 18 students over 16 lesson hours. The study was designed as a single-group quasi-experimental research model using a pre-test and post-test to examine changes in students' knowledge, skills, and awareness. The results showed a significant increase in students' cybersecurity knowledge and awareness. In particular, students became more conscious about safe internet use, cyberbullying, creating secure passwords, and social media security. Additionally, the findings revealed that the program was highly effective in developing cybersecurity skills throughout the process. This study emphasizes the importance of cybersecurity education at the elementary school level and highlights the contribution of instructional programs in this field. The research serves as a guide for future cybersecurity education programs and represents a significant step in equipping students with the ability to navigate the digital world consciously and securely.

Keywords: Cybersecurity, Instructional Program, Program Development, e-Shield, Digital World, Social Media Rules

This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original authors and source are credited.

Introduction

Today, technology is being used highly effectively in every aspect of our lives; however, while it provides us with great conveniences, it also brings certain problems. These issues include privacy and confidentiality violations (Cybersecurity Ventures, 2019), technology addiction and its associated social problems (Huang & Huang, 2024), new ethical challenges introduced by artificial intelligence (Nguyen et al., 2023), and cybersecurity concerns (Namukasa et al., 2025). The concept of the Internet of Everything (IoE), which refers to the interconnection of all electronic devices, has particularly increased concerns regarding cybersecurity. Due to the Internet of Things (IoT), even cyberattacks through baby monitors have become a common type of attack (Ahmad, 2023). The rapid integration of technology into our lives has necessitated the need for more conscious users at both individual and institutional levels (Nguyen et al., 2023).

Currently, the rate of digital media and technology use among children is rapidly increasing, with usage times among young people and children reaching remarkable levels (Sağlam, 2024). It is known that individuals who actively use the internet encounter significant problems such as online sexual abuse, exposure to obscene or harmful content (Çakır, 2022), personality disorders, addiction, the development of negative habits, an inability to distinguish which personal data can be shared, and oversharing details of private life (Donat Bacıoğlu, 2022). Reports in the media frequently highlight numerous dramatic cases of computer fraud, theft, and abuse that lead to large-scale crimes (Whitman & Mattford, 2021). To mitigate the negative aspects of the internet, individuals must develop an awareness of online security, understand potential risks, and acquire the necessary knowledge to protect themselves (Ahmad et al., 2022). The online environment presents numerous risks, particularly for children. The primary dangers they encounter while using the internet include cyberbullying, personal information security threats, harmful content, and unwanted communication with strangers (Livingstone & Stoilova, 2021). For this reason, it is essential to raise children's awareness of internet security.

Studies have shown that children do not fully comprehend the risks they encounter in the digital world and require guidance on online security (Broadband Commission for Sustainable Development, 2019). Research has shown that children do not fully comprehend the risks they encounter in the digital world and need guidance on online safety (Broadband Commission for Sustainable Development, 2019). Since children perceive the internet as an entertaining and informative environment, they do not adequately consider the potential dangers they may face (Ali et al., 2023). Since they are in a period where they begin to gain independence in technology use and value this independence, raising awareness and providing guidance on this issue are highly important (Ayyash et al., 2024).

According to a 2024 report prepared by cybersecurity experts from STM, an organization that provides technological and intellectual infrastructure for the Ministry of National Defense and the Turkish Armed Forces, data from 26 billion users has been leaked. Similarly, a study conducted by the Ponemon Institute in 2020 revealed that data breaches in large corporations worldwide resulted in billions of dollars in losses, primarily due to inadequate security measures. The National Institute of Science and Technology (NIST) in the United States has projected a significant demand for cybersecurity professionals, with an estimated shortage of nearly 3 million experts in the coming years (Whitman & Mattford, 2021). The same report predicts that by 2030, the increasing number of internet-connected electronic devices will create even greater vulnerabilities, making them potential targets for cyber threats.

Research on safe internet use has been conducted worldwide, and training programs have been designed to raise awareness in this field. Various organizations, such as the Australian Computer Society in Australia, the Cybersecurity Centre in the United Kingdom, and the National Centers of Academic Excellence and the National Initiative for Cybersecurity Education in the United States, have been working on designing and implementing cybersecurity education programs (Hajny et al., 2021).

Videnovik et al. (2024) conducted a training program using collaborative learning and game-based learning methods to impart knowledge and skills in cybersecurity. Although the research focused on

methodology, it demonstrated that the training effectively contributed to students' acquisition of knowledge and skills as well as the development of positive attributes. Similarly, Pirta-Dreimane et al. (2024) developed and implemented a technology-supported cybersecurity program called CAPE and examined its outcomes. The research findings indicated that the implemented cybersecurity education program positively influenced students' cybersecurity awareness and behaviors.

In Australia, a cybersecurity awareness scale was applied to mining company employees. The results showed that while 65% of the workers had general awareness of information security, their actual knowledge level was 77%, their attitudes toward the subject scored 76%, and their ability to demonstrate secure behaviors was only 54% (Yılmaz, 2015). Özçakanat et al. (2021) examined cybersecurity risks in banks in their study. The research emphasized that security vulnerabilities in institutions largely stem from human factors and that, due to a lack of knowledge and awareness, individuals can sometimes become part of a cyber attack.A study conducted in Kahramanmaraş among 2,449 primary and secondary school students used a researcher-developed scale to assess their awareness of cybersecurity in information technologies (Tekerek & Tekerek, 2013). The study found that students had very low awareness levels regarding critical security topics, mainly due to inadequate education and training programs. Consequently, it recommended that cybersecurity education be strengthened. Similarly, Sel (2013) conducted interviews with a group of 60 middle school students to assess their awareness of privacy settings on social media platforms. The study found that 70% of the students had no knowledge of social media privacy policies. After an awareness campaign, an improvement in their understanding was observed, reinforcing the importance of educational interventions.

The integration of the digital world into every aspect of our lives, especially with people becoming producers through social media accounts, has brought along digital data traces. A digital footprint, commonly referred to as a "digital trace," consists of data left behind in digital environments (Buitrago-Ropero, 2020). A deeper examination of digital traces reveals that even if an individual deletes a piece of online information, data mining techniques may still retrieve it. As a result, a digital profile is constructed based on users' online activity, allowing artificial intelligence to analyze behavior and capture their attention. For instance, even without actively engaging with advertisements, users may encounter targeted ads simply because they previously viewed a product, often due to lengthy and unread privacy policies (Erdem Erkul, 2021).

Sanin (2022) conducted a study with secondary school students to examine their awareness of cybersecurity, particularly in relation to digital footprints and data security. The findings indicated that many students were either unaware of the risks associated with their digital footprints or did not take them seriously, exposing them to potential cyber threats. Similarly, Demir (2021) studied university students' awareness of cybersecurity and concluded that education is the most effective solution for addressing cybersecurity challenges.

Based on these findings, the need for education on cybersecurity has become evident, leading to the development of the E-Shield instructional program. Given that students at the 6th-grade level are at a transitional stage, where they increasingly interact with technology (Haddock et al., 2022), it was deemed appropriate to design the program at the middle school level.

Research Purpose

This study aims to design, implement, and evaluate the E-Shield instructional program. Accordingly, the study seeks to answer the following research questions:

1. How effective is the E-Shield program in helping students acquire knowledge on cybersecurity?

2. To what extent does the E-Shield program help students develop cybersecurity-related skills and behaviors?

3. How does the E-Shield program impact students' awareness levels regarding cybersecurity?

4. Do the program’s learning objectives fully meet the identified needs?

5. Is the sequence of objectives appropriately structured?

6. Are the allocated instructional times aligned with students' learning needs?

7. Are the materials and instructional strategies used in the program effective and sufficient?

This study employs the Morrison, Ross, and Kemp instructional design model to structure the E-Shield program. This model is known for its flexibility, student-centered approach, and cyclical structure, allowing for necessary revisions and improvements (Morrison et al., 2012). A review of the literature confirms that cybersecurity challenges have increased alongside technological advancements, emphasizing the growing importance of cybersecurity knowledge and awareness. Therefore, the development and implementation of an educational program in this field are considered essential.

Methods and Materials

Research Design

For the purpose of this study, a one-group pretest-posttest design, one of the pre-experimental designs within quantitative research, was deemed appropriate. This model includes only one group, referred to as the experimental group. The impact of the intervention is assessed by administering tests before and after the intervention (Özmen & Karamustafaoğlu, 2019). In this study, the dependent variables are students' knowledge, skills, and attitudes, while the independent variable is the E-Shield instructional program.

Study Group

The study group consists of 6th-grade students from a middle school in the Gemerek district of Sivas, Turkey. The demographic characteristics of the study group are presented in Table 1.

Table 1. Demographic Information of the Study Group

Gender	Number of Participants	Percentage
Male	8	45%
Female	10	55%
Total	18	100%

Data Collection Tools

For data collection, an achievement test, an attitude scale, and a checklist were used. The achievement test was created with a pool of 25 questions and was reviewed by subject matter experts for content validity. A measurement and evaluation expert provided feedback on face validity, leading to modifications in some questions. Four questions, which measured similar learning outcomes, were merged into a single question. After the initial implementation, item discrimination and item difficulty analyses were conducted. Questions 5 and 15 were found to be too easy, while the first sub-question of Question 1 was too difficult, so adjustments were made accordingly. Items 13, 14, and 16, which had discrimination values below 0.20, were removed from the test, while questions 1, 3, 9, 22, and 23 were revised and strengthened. Ultimately, the final version of the achievement test consisted of 19 questions. The Digital Data Security Awareness Scale (DDSAS) is an attitude scale consisting of 32 items. The awareness statements were structured using a five-point Likert scale, with the following options: Strongly Agree (5), Agree (4), Neutral (3), Disagree (2), Strongly Disagree (1). Higher scores on the scale indicate higher awareness of digital data security. All items in the scale are positively worded. The exploratory and confirmatory factor analyses were conducted as part of the validity and reliability analyses of the scale. The suitability of the data for factor analysis was assessed using the Kaiser-Meyer-Olkin (KMO) test and Bartlett's Test of Sphericity, and the appropriateness of the data was confirmed by the KMO and Bartlett statistics (KMO = .951, $\chi^2 = 15113.267$, $p < .001$). Since the KMO value is greater than the threshold value of .600 and the Bartlett's Test of Sphericity result is significant, the sample is considered suitable for factor analysis. The factor loadings of the items range between .506 and .689, and the Cronbach's Alpha (α) internal consistency coefficient is .945. Accordingly, the measurement results can be considered highly reliable.

The checklist was developed to assess psychomotor behaviors within the program. Each behavior was broken down into its subcomponents, and a total of 10 skills were assessed. Students were asked to

demonstrate the expected behaviors, and their performance was recorded as "Yes" (if they performed the behavior) or "No" (if they did not). Student performance was evaluated in percentages.
The study was approved by the Institutional Ethics Committee.

Design of the E-Shield Cyber Security Instructional Program

The E-Shield program, as the independent variable in this study, was developed following the Morrison, Ross, and Kemp instructional design model. The key steps in the development process are as follows:

1. Needs Assessment. The program was designed for 6th-grade middle school students. Initially, a needs analysis was conducted to determine whether such an instructional program was necessary. A literature review confirmed the need for a cybersecurity instructional program. From a needs classification perspective, the program addresses both normative needs and felt needs. Other need types were not assessed in this study. Normative need is the evaluation of the target audience according to national standards. In this context, if a "digital citizen" is considered the norm defined as an individual who understands their rights and responsibilities in online environments then students' lack of alignment with this norm suggests an educational need. Perceived need can be defined as the desire to close the gap between the target audience's current performance and the ideal performance (Morrison, Ross & Kemp; 2012, pp. 31-50).

2. Learner and Context Analysis. Following the identification of the need, a learner and context analysis was conducted. The target audience consists of 6th-grade students at Middle School. Given their age group, their cognitive, emotional, and developmental characteristics were considered during the program design. The students' previous academic performance was evaluated by analyzing their grades from previous years, particularly in Information Technologies and Software courses, to assess their prior knowledge.
Individual learning styles were not specifically analyzed in this design; instead, general effective teaching methods and techniques for this age group were examined. A widely recognized model for learning styles is Fleming's VARK model, which classifies learners based on their visual, auditory, reading/writing, and kinesthetic preferences. Research suggests that visual and kinesthetic methods are more effective for 6th-grade students, as they tend to prefer interactive and visually engaging learning approaches (Fleming & Baume, 2006). An analysis of students' previous report cards showed that 26 students (63%) had a year-end average of 70 or above. Additionally, two students were identified as having learning difficulties.
The context analysis was conducted in terms of: Directive Context, Instructional Context, Transfer Context. Directive Context: Students have high motivation and interest in using new technologies. They recognize that this instruction will help them protect themselves from online threats. In the privacy and security unit, which briefly covers this topic, students showed curiosity and interest but lacked adequate knowledge and awareness. The analyses related to the instructional context are presented in Table 2.

Table 2. Instructional Environment Context

Factor	Considerations
Lighting	The lighting in the school's Information Technologies classroom is suitable for education.
Noise	The Information Technologies classroom is in a separate building along with the library, making it a quiet environment.
Temperature	The heating system with radiators is sufficient. Ventilation is available.
Seating Arrangement	The seating arrangement has been predetermined, and each student has an assigned computer.
Equipment	Each student has the necessary equipment.

In the analysis related to the transfer context, it was determined that students will be able to apply the knowledge and skills gained from the instruction in real-life experiences in the future. Since technology is integrated into all aspects of life, regardless of the career paths they choose, students will continue to interact with technology throughout their lives.Even if cybersecurity does not contribute directly to their professional careers, they will still use technology for entertainment or communication. Therefore, ensuring security in digital environments is a crucial skill that they will need throughout their lives.

3. Task Analysis. Within the scope of task analysis, both content analysis and method analysis were conducted.Content Analysis,The instructional content includes the following key topics:Basic Concepts of Cybersecurity,Safe Internet Usage,Malicious Software,Social Media and Digital Identity Management,Firewalls and Access Control,Cloud Data Storage and Data Security,Steps to Take When Facing Cybersecurity Issues
The method analysis is presented in Table 3 below;

Table 3. E-Shield Program Method Analysis

Objective	Step	Tip
Configuring Privacy Settings	1.Open your profile. 2.Click on the three dots in the upper right corner. 3.Select the 'Privacy' tab. 4.Set your account privacy settings to 'private'.	
Activating Antivirus and Security Software	1.Locate and open the antivirus software installed on your computer. 2.In the antivirus interface, find the 'Settings' or 'Protection' option. 3.Locate and enable the 'Real-Time Protection' or 'Real-Time Scanning' option. 4.Activate this option.	It is usually represented by an icon on the desktop or in the taskbar. This option is typically found on the main screen, at the top, or in the side menu.
Managing Cookie Settings	1.Open your browser. 2.Click on 'Settings'. 3.Select the 'Privacy and Security' option. 4.Choose the option related to cookies. 5.Modify the cookie settings as needed.	
Clearing Browser History and Cache	1.Open your browser. 2.Go to 'Settings'. 3.Select 'History'. 4.Clear browsing data. 5.Select the time range. 6.Select and clean the types of data to be cleaned.	The settings menu is usually represented by three dots in the upper right corner. Cookies, history, cache, etc.
Check firewall settings.	1.Click on the Start menu and go to Settings. 2.Select the 'Privacy and Security' option. 3.In the left menu, click on 'Windows Security'. 4.Choose the type of network you are connected to. 5.Select the type of network you are connected to 6.Select the "Enable firewall" option and save.	It may appear as a gear icon. Private or public
Storing data in the cloud.	1.Log in to your preferred cloud application. 2.Find the upload option. 3.Select the file or folder you want to upload.	You can choose which users can access the file.

	4.Click the upload option to start the upload. 5.Set your sharing and access settings.

4. Instructional Objectives. The learning objectives of the program were determined and categorized into facts, concepts, principles and rules, methods, interpersonal skills, or attitudes. The purpose of this categorization is to design instruction aligned with the objectives and to conduct objective-based assessments. The objectives were then sequenced in the next stage. The prerequisite method was used to determine the sequence of objectives. This method is based on a hierarchical structure of prerequisite skills, ensuring that prerequisite learning occurs before more advanced topics. Additionally, the objectives were arranged from simple to complex, easy to difficult, and known to unknown, while also prioritizing topics that are expected to engage students' interest. The elaboration theory was used for sequencing the skill-based learning objectives. The task expertise order was followed, meaning that tasks were taught from the simplest to the most complex (Morrison, Ross & Kemp, 2012).

5. Instructional Strategies. After sequencing the objectives, an expanded content-performance matrix was developed, and appropriate instructional strategies were identified.The content-performance matrix, developed by Merrill (1983, Morrison, Ross & Kemp, 2012, pp. 161-185), is used to determine the strategies necessary to achieve each objective.For the development of this instructional program, the matrix included details such as:What the content is? Which objective it addresses? Which category it falls into (fact, concept, principle, rule, method, interpersonal skill, or attitude)The steps to be followed in the initial presentation and generative strategies.This ensures standardization, so that any instructor implementing the program follows the same structured approach.

6. Instructional Message. To prepare instructional materials, including text, visuals, videos, and activities, a guidebook was developed as part of the message design phase.The content was structured according to the predetermined sequence of objectives, ensuring that every step of the instructional process was clearly outlined. Upon completing this stage, it was determined that the program should have a total duration of 16 hours.In the message design, pre-instructional strategies such as summaries and advance organizers were used. The key points in texts were highlighted, and a consistent typology was maintained throughout the guidebook (Morrison, Ross & Kemp; 2012, pp. 81-102). Additionally, images and graphics were selected based on their explanatory functions rather than decorative purposes.

7. Evaluation Tools. To measure the effectiveness of the program, the following assessment tools were developed:1. Achievement Test,2. Digital Data Security Awareness Scale (DDSAS),3. Checklist.

Data Collection Process

The data collection process began in the first week of February and was completed in ten days. At the beginning of the process, the achievement test and the attitude scale were administered as a pre-test. The E-Shield program, designed as a 16-hour intervention, was implemented. Throughout the program, students' psychomotor skills were assessed using a checklist. After the instructional program, the achievement test and the attitude scale were administered again as post-tests. A paired-samples t-test and effect size analysis were conducted to determine the significance of the difference between pre-test and post-test scores.

Data Analysis

The Digital Data Security Awareness Scale (DDSAS) was analyzed using a statistical program. Responses on the 5-point Likert scale were scored and ranked from highest to lowest. A normality analysis of the scale was conducted, confirming that the data followed a normal distribution. The internal consistency of the scale was assessed using Cronbach's Alpha coefficient. As a result of the analysis, the overall reliability coefficient of the scale was found to be $\alpha = .83$. This value indicates that the scale has a high level of reliability.

For the achievement test, Shapiro-Wilk test was conducted to analyze t he normality of score distributions, as the group size was less than 50. Since the distribution was normal, a paired samples t-test was used for comparison. The internal consistency of the achievement test was assessed using

Cronbach's Alpha coefficient. The analysis results indicated that the overall reliability coefficient of the test was α = .86, which demonstrates a high level of reliability.
The checklist was used to evaluate whether students acquired the intended psychomotor behaviors. The checklist was completed for each student throughout the process. The percentage of students demonstrating the expected skills was calculated.

Findings

In the findings section of the study, a performance test and an attitude scale were used to determine the effectiveness of the program from the pre-test to the post-test. The performance test and attitude scale were administered in a pre-test and post-test format at the beginning of the process and after the program was implemented, and the obtained scores were analyzed using a statistical program. Additionally, a checklist was completed by observing students throughout the process to assess the extent to which they acquired the skills.

Findings on Students' Academic Performance

The distribution of scores from the achievement test is presented in the table below. Since the sample size was less than 50, the Shapiro-Wilk test was used to assess normality distribution. For the reliability analysis, the test-retest method was used, and the correlation between tests was above 0.80, indicating high reliability.

Table 4. Normality Test for the Achievement Test

	Shapiro-Wilk Test		
	Statistic	Df	*p*
Pre-test	.927	18	.172
Post-test	.951	18	.447

As seen in Table 4, the pre-test and post-test distributions of the group ($p>.05$) are normal distributions. Therefore, a paired sample t-test was conducted for the change between the pre-test and post-test.

Table 5. Achievement Test Statistics

	$\bar{X}$	*N*	SD	Std.Error
Pre-test	12.78	18	2.211	,521
Post-test	16.44	18	1.617	,381

As seen in Table 5, the mean score of the group's post-test (16.44) is higher than the mean score of the pre-test (12.78).

Table 6. Paired Samples t-Test for Change in Group Performance

Comparison	$\bar{X}$	*SD*	Std. Error	*t*	*p*
Pre-test - Post-test	-3.667	1.328	.313	-11.710	.000

As shown in Table 6, when examining the group's pre-test and post-test results ($t_{(17)}$= -11,710; $p < .05$), a significant difference was observed in favor of the post-test scores. When examining the effect size, Cohen's d value was calculated as 2.76. This result indicates that the e-Kalkan instructional program has a significant impact on addressing students' knowledge gaps in cybersecurity.

The data obtained from the checklist also revealed that students generally acquired the expected skills. Specifically: 84% of students (15 out of 18) were successful in 3 of the skills, 78% of students (14 out of 18) were successful in 1 skill, All students successfully demonstrated the remaining skills. Thus, it can be concluded that the E-Shield program was highly effective in teaching cybersecurity-related skills.

Findings on Students' Attitudes

First, the Shapiro-Wilk test was conducted to examine the distribution of scores obtained from the attitude scale. The results are presented in Table 7.

Table 7. Attitude Scale Normality Test

To examine the distribution of scores obtained from the attitude scale, the Shapiro-Wilk test was conducted. The results are presented in Table 7.

	Statistic	Df	*p*
Pre-test	,936	18	,247
Post-test	,961	18	,629

As shown in Table 7, the scores obtained from the attitude scale exhibit a normal distribution for both the pre-test and post-test ($p > .05$). Therefore, changes in student attitudes were measured using a paired samples t-test. The reliability of the scale, measured using Cronbach's Alpha, was 0.83 for the pre-test and 0.87 for the post-test. Based on these results, it can be concluded that the scores obtained from the scale are reliable.

Table 8. Statistics for Scores Obtained from the Attitude Scale

	$\bar{X}$	Sd	Std. Error
Pre-test	124.61	19.321	4.554
Post-test	144.11	16.859	3.974

As seen in Table 8, the average pre-test scores obtained from the attitude scale were 124.61, whereas the post-test average scores were measured as 144.11. This indicates an increase in students' post-test scores compared to their pre-test scores.

Table 9. Paired Samples t-Test for Pre-Test and Post-Test Scores of the Attitude Scale

Comparison	$\bar{X}$	*SD*	Std. Error	*t*	*p*
Pre-test - Post-test	-19.500	15.966	3.763	-5.182	.000

As seen in Table 9, the paired samples t-test results indicate a significant difference between the pre-test and post-test scores obtained from the attitude scale ($t_{(17)}$= -5.182; $p < .05$). When examining the effect size, Cohen's d value was calculated as 1.22. This result indicates that the e-Kalkan training program has a strong impact on enhancing students' awareness and attitude levels.

Discussion And Conclusion

The results of the E-Shield educational program indicate that students' knowledge levels on cybersecurity significantly increased. This finding aligns with the existing literature. For example, Quayyum et al. (2021) reviewed 56 peer-reviewed studies and concluded that the most frequently used method to prevent cybersecurity issues and address information security deficiencies is education. Similarly, Yiğit and Seferoğlu (2019) evaluated information security based on five factors and found that undergraduate students who received education on this topic had a more substantial knowledge base. In the United States, the CyberPatriot competition is implemented as an educational program aimed at informing students about cybersecurity, and the program has been reported to increase students' knowledge levels (CyberPatriot, 2025). Likewise, many organizations conduct initiatives to enhance digital security awareness and increase students' knowledge and consciousness about online safety. Examples include:Google’s "Be Internet Awesome" initiative, Australia’s "Cyber Smart Challenge", Global Digital Citizen Foundation's cybersecurity training programs.

The E-Shield program was also found to positively influence students' attitudes toward cybersecurity and significantly enhance their awareness. In their research, Kweon et al. (2021) examined the relationship between cybersecurity education and organizational security issues. Their study of 7,089 companies found that those that provided cybersecurity training faced fewer security incidents. This

indicates that awareness, along with knowledge and skills, plays a crucial role in cybersecurity. The use of videos, role-playing, and dramatizations in the E-Shield program helped students internalize the topic, making the learning process engaging and interactive. This result is consistent with findings in the literature. For instance, Mages (2018) emphasized that incorporating drama activities into classroom settings has a positive impact on student engagement and active participation.

Educational programs are considered essential and effective in raising awareness of cybersecurity. Ünver (2012) noted that, in Turkey, graduate programs, non-governmental organizations (NGOs), and government institutions are actively involved in conducting awareness initiatives on this topic. On a global scale, significant efforts are being made to increase cybersecurity awareness. For example:"Safer Internet Day" is celebrated in 150 countries, promoting awareness through educational events and activities (SID, 2025). The UK CyberFirst program provides cybersecurity training and competitions for female students, supporting their career planning in this field (CyberFirst, 2025).

The E-Shield program was also found to be effective in equipping students with essential cybersecurity skills. The "demonstration and practice" method was primarily used in skill acquisition, and this approach was found to be effective. This finding aligns with prior research. For instance: Keskinkılıç (2019) concluded that the demonstration and practice method led to more permanent learning outcomes in geometry classes. Şahin (2024) found that using the demonstration and practice method in coding education significantly improved students' coding skills. Kan (2008), in his study on effective teaching methods in mathematics, determined that the most effective method for enhancing student achievement was the demonstration and practice approach.

A cybersecurity-themed song created for the program was also observed to have a positive impact on students' awareness. Students were able to quickly learn and enjoy singing the lyrics. Similar findings are reflected in previous studies, which highlight the role of music in enhancing learning experiences. For example, Tandoğdu Kılıç (2023) emphasized in his research that music positively influences brain functions related to learning.

However, the analysis of achievement test and attitude scale results revealed that there were two topics that students struggled to grasp. This suggests that the E-Shield program was not entirely effective in conveying these specific objectives:1. Types of Digital Footprints: This topic was part of the program's objectives, but since it was explained through a lecture-based approach, it may not have been effectively learned. Designing interactive activities for this topic could improve understanding.2. Safely Removing Hardware: This topic was not included in the program's objectives, indicating a gap that needs to be addressed in future revisions.

The time allocated for learning objectives in the E-Shield program was found to be appropriate. However, it is suggested that more time be allocated for lessons involving role-playing and creative drama since students enjoyed these activities, engaged creatively, and focused better on the topics. Overall, the E-Shield program successfully covered its intended objectives. However, it was found to be less effective in teaching "types of digital footprints" (as indicated by the achievement test) and "safely removing hardware" (as indicated by the attitude scale). The sequence of objectives was deemed appropriate, and the activities and strategies used in the program were found to be effective and suitable for achieving the goals. Additionally, the time allocated for each objective was considered appropriate.

Suggestions

1. Cybersecurity education should not be limited to a specific age group but should be designed to be adaptable for all age groups. The program should be expanded with more advanced or more fundamental modules based on age levels.
2. To enhance children's cybersecurity knowledge, it is essential to involve families in the learning process. Information sessions for parents can be organized, and guidance on safe internet usage at home can be provided.
3. Follow-up studies should be conducted to track the long-term impact of the program. The retention and sustainability of the knowledge, skills, and awareness gained should be evaluated.
4. Efforts should be made to contribute to the development of national and international cybersecurity education policies. The program's outcomes can provide valuable data to inform educational policies.

References

Ahmad, M. S. (2023). *Cyber security with IoT, vulnerabilities, threats and attacks* [Unpublished master's thesis]. Üsküdar University.

Ahmad, N., Laplante, P. A., DeFranco, J. F., & Kassab, M. (2022). "A cybersecurity educated community." *IEEE Transactions on Emerging Topics in Computing*, 10(3), 1456-1463. https://doi.org/10.1109/TETC.2021.3093444

Ali, S., Haykal, H. A., & Youssef, E. (2023). Child sexual abuse and the internet: A systematic review. *Human Arenas*, 6, 404-421. https://doi.org/10.1007/s42087-021-00228-9

Ayyash, M., Alsboui, T., Alshaikh, O., Inuwa-Dutse, I., Khan, S., & Parkinson, S. (2024). Cybersecurity education and awareness among parents and teachers: A survey of Bahrain. *IEEE Access*, 12, 86596-86617. https://doi.org/10.1109/ACCESS.2024.3416045

Broadband Commission for Sustainable Development (2019). Child online safety: Minimizing the risk of violence, abuse and exploitation online. *ITU and UNESCO*. https://unesdoc.unesco.org/ark:/48223/pf0000374365?posInSet=1&queryId=1a93f340-75cf42d8-adfe-4f4b718fcad3

Buitrago-Ropero, M. E., Ramírez-Montoya, M. S., & Laverde, A. C. (2020). Digital footprints (2005–2019): A systematic mapping of studies in education. *Interactive Learning Environments*, 31(2), 876–889. https://doi.org/10.1080/10494820.2020.1814821

CyberFirst. (2025, January). *Overview of CyberFirst*. https://www.ncsc.gov.uk/cyberfirst/overview

CyberPatriot. (2024, January 18). *AFA CyberCamp overview*. https://www.uscyberpatriot.org/afa-cybercamps/overview

Cybersecurity Ventures. (2019). *2019 Official Annual Cybercrime Report*. Herjavec Group. https://www.herjavecgroup.com/2019-official-annual-cybercrime-report/prnewswire.com+8

Çakır, K. (2022). *Sexual crimes committed on the internet and social networks* [Unpublished master's thesis]. Marmara University.

Demir, M. (2021, March). Investigation of the current state of information security and cybersecurity education in our country from an international security perspective. *International Security Symposium*, Istanbul Rumeli University.

Donat Bacıoğlu, S. (2022). Cyber risks awaiting children and young people in the 21st century. *Current Approaches in Psychiatry*, 14(1), 29-37. https://doi.org/10.18863/pgy.896800

Erkul, R. E. (2021). What kind of future do artificial intelligence and big data promise? *TRT Academy*, 6(11), 192-201.

Fleming, N., & Baume, D. (2006). Learning styles again: VARKing up the right tree! *Educational Developments*, 7, 4-7. http://www.johnsilverio.com/EDUI6702/Fleming_VARK_learningstyles.pdf

GİG. (2025, January 18). *Safer Internet Day*. https://www.gig.org.tr

Haddock, A., Ward, N., Yu, R., & O'Dea, N. (2022). Positive effects of digital technology use by adolescents: A scoping review of the literature. *International Journal of Environmental Research and Public Health*, 19(21), 14009.

Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., & De Nicola, R. (2021). Framework, tools, and good practices for cybersecurity curricula. *IEEE Access*, 9, 94723-94747. https://doi.org/10.1109/ACCESS.2021.3093952

Huang, Y., & Huang, H. (2024). Exploring the effect of attachment on technology addiction to generative AI chatbots: A structural equation modeling analysis. *International Journal of Human–Computer Interaction*, 1–10. https://doi.org/10.1080/10447318.2024.2426029

Jang-Jaccard, J., & Neppal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5).

Kan, A. (2008). A comparison of scaling approaches used to measure psychological variables. *Theory and Practice in Education*, 4(1), 2-18.

Keskinkılıç, V. (2019). *The effect of the demonstration method in the geometry learning area of the 6th grade mathematics course on student success and retention* [Unpublished master's thesis]. Kırşehir Ahi Evran University.

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers,* 23, 361-373.

Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying online risk to children. *CO:RE - Children Online: Research and Evidence*. https://doi.org/10.21241/ssoar.71817

Mages, W. K. (2018). Does theatre-in-education promote early childhood development? *Early Childhood Research Quarterly*, 45, 224-237. https://doi.org/10.1016/j.ecresq.2017.12.006

Michael, E., & Whitman, H. J. (2021). *A model curriculum for programs of study in cybersecurity workforce development.* Kennesaw: KSU Institute for Cybersecurity Workforce Development.

Morrison, G. R., Ross, S. M., & Kemp, J. E. (2012). *Effective instructional design*. (İ. Varank, Ed., Translated to Turkish). Bahçeşehir University Press.

Namukasa, M., Chaparro Osman, M., Ficke, C., Piasecki, I., OConnor, T., & Carroll, M. (2024). Evaluation of an Internet of Things Device-Based Educational Approach to Engage a More Diverse Cybersecurity Workforce. *International Journal of Human–Computer Interaction*, 41(2), 1364–1380. https://doi.org/10.1080/10447318.2024.2314349

Nguyen, A., Ngo, H. N., Hong, Y., Dang, B., & Nguyen, B. P. T. (2023). Ethical principles for artificial intelligence in education. *Education and Information Technologies*, 28(4), 4221-4241.

Özçakanat, Ö., Özdemir, O., & Mazak, M. (2021). İşletmelerde Siber Güvenlik Riskleri ve Bilgi Teknolojileri Denetimi: Bankaların Siber Güvenlik Uygulamalarının İncelenmesi. *Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi,* 5(2), 246-270. https://doi.org/10.31200/makuubd.978263

Özmen, H., Karamustafaoğlu, O. (2019). *Eğitimde Araştırma Yöntemleri*. Ankara: Pegem Akademi

Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K., Grabis, J., Lugo, G.R. & Bonders, M. (2024). Try to ESCAPE Cybersecurity Incidents! A Technology-Enhanced Learning Approach. *Technology, Knowledge and Learning*. https://doi.org/10.1007/s10758-024-09769-8

Ponemon Institute. (2020). *Cost of a data breach report.* https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343.

Safer Internet Day (2025). *Safer Internet Day 2025*. https://saferinternet.org.uk/safer-internet-day/safer-internet-day-2025

Sağlam, T. (2024). Çocuklarda teknoloji kullanimi ve dijital ebeveynlik. *Birey ve Toplum Sosyal Bilimler Dergisi*, 14(1), 123-129. https://doi.org/10.20493/birtop.1496639

Sel, H. (2013, January). Erişim, güvenlik ve gizlilik boyutunda ortaokul öğrencilerinin Facebook kullanımı. XV. *Akademik Bilişim Konferansı*. Akdeniz Üniversitesi.

Sanin, E. (2022). *The relationship between secondary school students' digital footprint awareness and information security awareness* [Unpublished master's thesis]. Hacettepe University.

STM. (2024, May). *Cyber threat situation report*. www.Stm.com.tr

Şahin, F. (2024). *Oyun temelli öğretim yöntemi ile gösterip yaptırma yöntemine göre verilen kodlama eğitiminin ortaokul öğrencilerinin akademik başarılarına etkisinin incelenmesi* [Unpublished master's thesis]. Tokat Gaziosmanpaşa Üniversitesi.

Tandoğdu Kılıç, S. (2023) Etkili bir öğrenme aracı olarak müziğin kullanımı. *Korkut Ata Türkiyat Araştırmaları Dergisi*, (13), 1502-1516. https://doi.org/10.51531/korkutataturkiyat.1377217

Tekerek, M. & Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education*, 2(3), 61-70.

Ünver, M. (2012). *Ulusal Siber Güvenliğin Sağlanmasında Farkındalık Çalışmaları. https://www.academia.edu/24842057/Ulusal_Siber_G%C3%BCvenli%C4%9Fin_Sa%C4%9Flanmas%C4%B1nda_Fark%C4%B1ndal%C4%B1k_%C3%87al%C4%B1%C5%9Fmalar%C4%B1*

Videnovik, M., Filiposka, S. & Trajkovik, V. (2024). A novel methodological approach for learning cybersecurity topics in primary schools. *Multimed Tools Applications*. https://doi.org/10.1007/s11042-024-20077-2

Yılmaz, E. (2015). *Öğretmenlerin dijital veri güvenliği farkındalığı* [Unpublished doctoral dissertation]. Anadolu Üniversitesi.

Yiğit, M. F., & Seferoğlu, S. S. (2019). Examining students' cybersecurity behaviors based on the Big Five personality traits and various other variables. *Mersin University Journal of the Faculty of Education*, 15(1), 186-215. https://doi.org/10.17860/mersinefd.437610

Biographical notes:

Fatma Şahin: Fatma Şahin completed her BA in Information Technology Education and her MA in Information Technology. She is currently a PhD student in Curriculum and Instruction. She also works as an Information Technology teacher in a public school.

Semra Demir Başaran: Dr. Semra Demir Başaran works as a professor in the department of curriculum and instruction. Her research interests include instructional design, program development, program evaluation, teacher education, and inclusive education.