Available online at www.ijournalse.org

Emerging Science Journal

(ISSN: 2610-9182)

Vol. 9, Special Issue, 2025

"Emerging Trends, Challenges, and Innovative Practices in Education"

Effectiveness of the Daniel Model in Enhancing Primary Students' Learning of Cybersecurity Concepts

Ali A. Al-Barakat [1, 2*], Rommel M. AlAli [3*], Omayya M. Al-Hassan [4], Eid M. Kanaan [1, 2], Yusra Z. Aboud [3], Ali K. Abdullatif [5]

[1] *Department of Education, University of Sharjah, Sharjah 27272, United Arab Emirates.*

[2] *Faculty of Educational Sciences, Yarmouk University, Irbid 21163, Jordan.*

[3] *The National Research Center for Giftedness and Creativity, King Faisal University, Al-Ahsa 31982, Saudi Arabia.*

[4] *Department of Psychological Sciences, College of Education, Qatar University, Doha, Qatar.*

[5] *Department of Arabic Language, College of Arts, King Faisal University, Al Ahsa 31982, Saudi Arabia.*

Abstract

This study investigated the effectiveness of Daniel's Model in teaching cybersecurity concepts to ninth-grade students in Amman, Jordan. A quasi-experimental design with two groups was employed; the experimental group received instruction based on Daniel's model, while the control group followed traditional teaching methods. The sample consisted of 120 students, was selected from ten international schools via convenience sampling, and was randomly assigned to the groups. Data were collected using a 33-item knowledge test covering four key domains of cybersecurity. Analysis in SPSS included an independent samples t-test and a paired samples t-test; in addition, effect size (η^2) was calculated to understand the magnitude of the model impact. A higher score of digital threat knowledge and skills in terms of prevention, ethical behaviors, and data protection related to the model taught was noticeable among the experimental group, since the effect size (η^2) varied from large (0.34) to very large (0.62). Also, in the delayed test, the experimental group showed no decline in performance, demonstrating that the model was effective in teaching knowledge and digital practices. Considering the results, it is recommended that Daniel's Model, combined with interactive techniques and scenario building, be integrated in teaching digital ethics and use of technology, in addition to training teachers on systematic implementation of desired, sustained outcomes of the model.

Keywords:
Cybersecurity Education;
Daniel's Model;
Digital Safety Skills;
Interactive Learning Strategies.

Article History:

Received:	27	December	2025
Revised:	28	March	2026
Accepted:	03	April	2026
Published:	21	April	2026

1- Introduction

Digital threats have grown exponentially over the past two decades, placing cybersecurity at the forefront of national and international policy priorities [1, 2]. Governments have focused on developing national strategies to protect critical infrastructure from cyberattacks, establishing specialized agencies to address digital risks, and strengthening international cooperation in cyber defense and threat response [3, 4]. These strategies primarily emphasize protecting institutions, digital systems, and sensitive data, while promoting the exchange of information and expertise among national and international entities to counter digital threats [5-7].

* **CONTACT**: aalbarakat@sharjah.ac.ae; ralali@kfu.edu.sa

DOI: http://dx.doi.org/10.28991/ESJ-2025-SIED1-029

© 2025 by the authors. Licensee ESJ, Italy. This is an open access article under the terms and conditions of the Creative Commons Attribution (CC-BY) license (https://creativecommons.org/licenses/by/4.0/).

The advancement of technology in the education sector and the use of online learning platforms have, in turn, increased the possibility of exposure to cybersecurity-related risks [8-10]. It has become imperative to teach school students the safe and ethical use of technologies along with providing them with the technologies and devices [11, 12], which, in other words, means providing students with safe online practices and the awareness to manage and mitigate risks related to digital technology, e.g., data breaches, cyber extortion, and cyberbullying [13, 14].

Reports from the National Cybersecurity Center (NCSC) in Jordan have indicated that there have been numerous attempts to breach data in schools, which signifies the need for data protection at educational institutions consistent with legislation and regulations adopted by NCSC [15]. The Jordanian Ministry of Education has developed policies to promote data security at schools, including obtaining digital frameworks, monitoring systems, and protection protocols [16, 17]. Efforts to teach students' cybersecurity skills, however, are inadequate, as most strategies rely on awareness-raising campaigns that have limited duration and impact on students' behaviors [18, 19].

Several studies show how middle and secondary school students gain little understanding of cybersecurity risks when instruction is mainly based on theory and lectures [20-27]. Teaching focuses on information and concept delivery, but lacks hands-on application learning in real-world digital settings, leaving students unprepared to face online challenges [28-33]. Previous studies [34, 35] show that students receiving only theoretical instruction do not possess data protection skills to face cyberattacks, underscoring the inadequacy of these strategies. Other studies [13, 16, 20, 36-40] show that when lectures are not supported with practical activities, the gained knowledge is lost almost immediately, and long-term retention of critical cybersecurity concepts is hindered.

Also, several studies have stated that experiential learning is an effective way to improve learning about cybersecurity, as it allows students to practice skills and simulate digital threats and knowledge application in solving real problems [36-39, 41, 42]. In line with these studies, the Daniel Constructivist Model is an effective model, as it is based on learning through experience. It promotes students' engagement with the content, enhancing their skills of critical thinking, problem-solving, and independent and collaborative decision-making [3, 13, 36]. A quasi-experimental study [16] reported that using Daniel's Model in cybersecurity education improved students' digital risk-safe decision-making and problem-solving.

Principles of real-world relevance, peer learning, and promoting think and pair analytical and critical problem-solving, as well as divergent thinking and autonomy, are included in Daniel's Model [17, 37, 39]. Earlier studies, Hong et al. [34] and Antunes et al. [35], showed that learners, using educational models like Daniel's Model, were able to assess numerous scenarios involving digital threats and preventive measures, contributing to sustained behavioral awareness and adaptive, practical, and behavioral competencies in cybersecurity. Al-Barakat et al. [10] highlighted the positive effects of experiential learning in the cybersecurity curriculum context in enhancing students' safe practices and reducing errors in the use of digital technologies.

Since there are many harms like cyberbullying, digital breaches, and cyber extortion in the non-ideal world of digital learning paralleled with behavioral threats that drain students' digital awareness, Daniel's model helps in cultivating behavioral and ethical dimensions in students when using technology and fosters a sense of accountability, critical active thinking, and self-regulation concerning risky digital activities [37, 41].

When Daniel's model is integrated into cybersecurity education, it is exciting to think about how it can develop practical skills, safe digital practices, and critical thinking. In the Arab studies context, it fills a particular research void as most studies have not documented the use of experiential learning and assessed its impact on students' behaviors and practical, real-life skills in the field of cybersecurity [14, 23, 24, 42].

The studies conducted in the Arab context regarding the use of Daniel's Model in cybersecurity education, specifically in the middle and high school stages, are still lacking. Most studies consider only young primary school students or only theorize levels of awareness, often without providing the experiential learning opportunities necessary to develop enduring behaviors and the skills to protect oneself from insecurity [23, 24, 43]. Few studies have been conducted regarding the digital behaviors of students in the long run because of applying Daniel's Model.

By applying the Daniel's Model to Cybersecurity Education for ninth grade students in Jordan, this study intends to fill the research gap and assess both the immediate and long-term impacts of the model. Also, by applying experiential and interactive learning techniques, it contributes to fostering and promoting safe digital practices instead of simply providing short-term theoretical awareness. Moreover, it provides valuable evidence for educators and curriculum developers on how to design comprehensive and effective cybersecurity education programs, contributing to the development of students equipped with the awareness and practical skills necessary to address future digital challenges.

Considering the provided background, the main research question is stated as: How effective is Daniel's model in teaching concepts related to cybersecurity to ninth-grade students in Jordan? This is turned into two additional questions:

1. Are there statistically significant differences at ($p = 0.05$) in the mean scores of cybersecurity concepts between students taught using Daniel's Model and those taught through the traditional method?
2. Are there statistically significant differences at ($p = 0.05$) in the mean scores of cybersecurity concepts within the experimental group between the immediate post-test and the delayed post-test?

Further along the lines of the introduction, the research questions, and the identified gap in the literature, the next part of the research focuses on the review of literature theorized with sufficient justification for the research to be carried out. The next part concentrated on presenting the research methodology, especially the parts that deal with the quantitative research methods. The following part is the presentation of the results, supplemented by thorough and analytical discussion. The last part concludes by summarizing the major findings, followed by suggestions to be acted on, especially to serve the purpose of guiding those who intend to carry out research in the future.

2- Literature Review

Cybersecurity is recognized as a field of knowledge and practice today. It focuses on defending a user's digital system and protecting him from an ever-widening range of cyber threats that have become a societal issue affecting all digitally engaged age groups [15, 33-37]. Hence, digital security literacy has become one of the 21st century's indispensable competencies. It is associated with an individual's ability to interactively learn and perform in society and economy [2, 6], as, with the pervasiveness of smart devices, the ability to develop and maintain certain online practices has become a necessary and life-sustaining skill [16, 28].

Integrating cybersecurity principles at the school level began as a strong educational trend in 2020 through new educational frameworks that guide students' spotting digital opportunities while understanding online threats. Students are trained in digital safety practices and learn to make sound decisions critical in cyber protection [24]. Early teaching of cyber protection principles enhances the students' ability to protect their identity and resist electronic control, extortion, and surveillance, promoting their protective digital responsibility.

Due to the rise and complexity of cyber threats, there has been a greater worldwide focus on cybersecurity education. Growing emphasis on this issue is no longer an auxiliary element in education but rather a core requirement to be integrated in curricula; it is not a technical competence but a culturally ingrained and sustained composite practice [29-31]. This perspective has prompted focusing on the importance of programmed educational interventions that promote the simulation of real-world risks and the protective practices that assess the credibility of the information and the act of conscious filtering of content, especially those related to privacy [32, 33].

Cybersecurity education also has a considerable impact on students' social and emotional well-being. Growing cyber threats of blackmail, harassment, and predatory deception have made learning environments more dangerous and exploitative [10, 13, 34, 35]. A well-implemented cybersecurity education fosters a culture of digital safety and responsible positive digital behavior in educational spaces [38].

Blažič & Blažič [24] reported that active teaching strategies that include simulation and game elements motivate and improve students' ability to recognize and defend against cyber threats. Other studies [14, 19, 21, 22, 42, 44] confirmed that when students are placed in active scenarios, they acquire critical and analytical thinking skills that go beyond the typical classroom situation.

Incorporating Daniel's model to teach cybersecurity has become a popular choice in pedagogy. It allows students to safely interact with real digital environments and learn to make sound judgments and respond to risks appropriately [20-23, 45]. This model also aids in the creation of learning environments where teachers blend theory and practice, which is critical in bridging the theory-to-practice gaps and developing sustainable behaviors in cybersecurity.

Cybersecurity education from K–12 has been recognized by multiple scholars and organizations as a teachable and strategic investment in countering future digital threats [24]. Training is better received early than in later years, where the adult learner is often restricted by time, motivation, and other factors that limit the effectiveness of training [25, 46-48]. In the Arab World, the need to design and implement pedagogy and curriculum frameworks that encompass the cybersecurity educational, pedagogical, and assessment challenges has been emphasized [4, 39, 40]. Practical Cybersecurity Camps (C3-2021) serve as an example of the provision of interactive pedagogy in cybersecurity education by simulating a range of threats and the advanced skills required to counter them [48, 49].

Studies have documented the increased digital risk school-aged children are exposed to, such as cyberbullying, online predation, and limited digital literacy of their parents [23, 26, 49]. Since the COVID-19 pandemic, there has been increased dependence on online platforms; as a result, cybercrimes have proliferated, resulting in negative psycho-social and behavioral issues [17, 22, 50]. This underscores the need for continuous cybersecurity education programs that enhance the awareness of digital risk and develop more active defensive actions among learners. Such educational programs are crucial in countering cyber threats and their detrimental impact on people and businesses. Moreover, educating people in cybersecurity enhances their responsibility as digital citizens, leading to healthier and safer school environments for students to use technology [14, 26].

Despite the clear advantages, there is still a lack of interactive empirical literature on the use of Daniel's model in the Arab world's educational literature, especially in basic education, where there is virtually no organized literature on the impact of such models. Offered cybersecurity topics are entirely theoretical; this clearly calls for the use of more researched innovative models providing experiential teaching for the development of positive behavioral patterns around digital safety in learners.

3- Research Methodology

3-1- Study Design

The current study utilized a quasi-experimental study design to determine the impact of a Daniel's Model-based training program on the comprehension of some selected concepts of cybersecurity of ninth-grade students. Participants were divided into two equivalent groups (experimental and control). The fact that all the participants came from the same social and cultural background helped reduce the effect of external variables and reinforced the internal validity of the research design.

To minimize the influence of extraneous variables and ensure the reliability of the findings, both groups took a pre-test measuring their cognitive and performance levels of cybersecurity competencies before the intervention was executed. When the training was completed, a post-test was offered to both groups to evaluate the changes in performance, allowing the assessment of the effectiveness of the training designed to enhance students' understanding and develop preventive digital practices while in the cybersecurity context. The structure of the design was as follows:

- **Experimental Group:** $O_1 \rightarrow X \rightarrow O_2$
- **Control Group:** $O_1 \rightarrow — \rightarrow O_2$

Where:

- **O_1** = Pre-test assessing cognitive and performance skills in cybersecurity
- **O_2** = Post-test assessing cognitive and performance skills in cybersecurity
- **X** = Daniel's Model–based training program.

Thus, the structural method of the design of the research is represented in the following Figure 1.

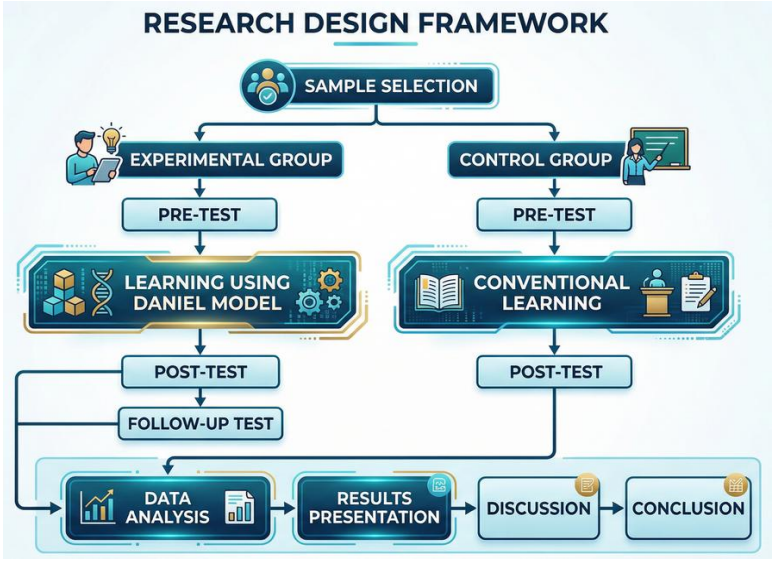

Figure 1. Research design

3-2-Study Sample

The sample consisted of 120 students of primary education level in the capital Amman, Jordan, who were selected from ten private schools using convenient sampling based on the schools readiness and ability to provide the training program implementation in the schools instruction. Participants were divided into two equal size and general academic characteristics groups as follows:

- ***Experimental Group:*** 60 students underwent a training program based on the Daniel's Model
- ***Control Group:*** 60 students underwent study of cybersecurity content taught through conventional methods.

To confirm the initial equivalence of the two groups, a test measuring the participants' knowledge of cybersecurity was administered prior to the start of the intervention. Results of the independent samples t-test showed a significance of 0.072 (see Table 2 in data collection section), indicating that at the alpha level of 0.05, no statistically significant difference existed between the groups' mean scores on the pre-test. This confirmed the groups were homogeneous at the start, and a fair comparison of post-test scores could be made to measure the effects of the training program.

Moreover, to address the possible confounding variables associated with the teacher, the same teachers were assigned to both the experimental and control groups. Hence, the same teaching style and instructional quality were provided for both groups, so the differences in student performance could be attributed to the Daniel's Model–based training intervention. Explanation of the model's steps and relevant interactive teaching strategies, along with guided practice, were designed to help teachers assist students understand the digital risks and the ways to protect themselves and act responsibly.

3-3-Daniel's Model–Based Learning in Developing Cybersecurity Concepts

The training program employed Daniel's Model while training teachers as a guiding framework in developing interactive instructional activities to teach and strengthen learners' cybersecurity concepts. This model was adopted because of its recognized effectiveness in combining the cognitive, behavioral, and constructive levels of learning to help students understand digital threats, gain protective strategies, and practice responsible digital behavior. According to [8, 44], the model has nine components that are interlinked, as illustrated in Figure 2.

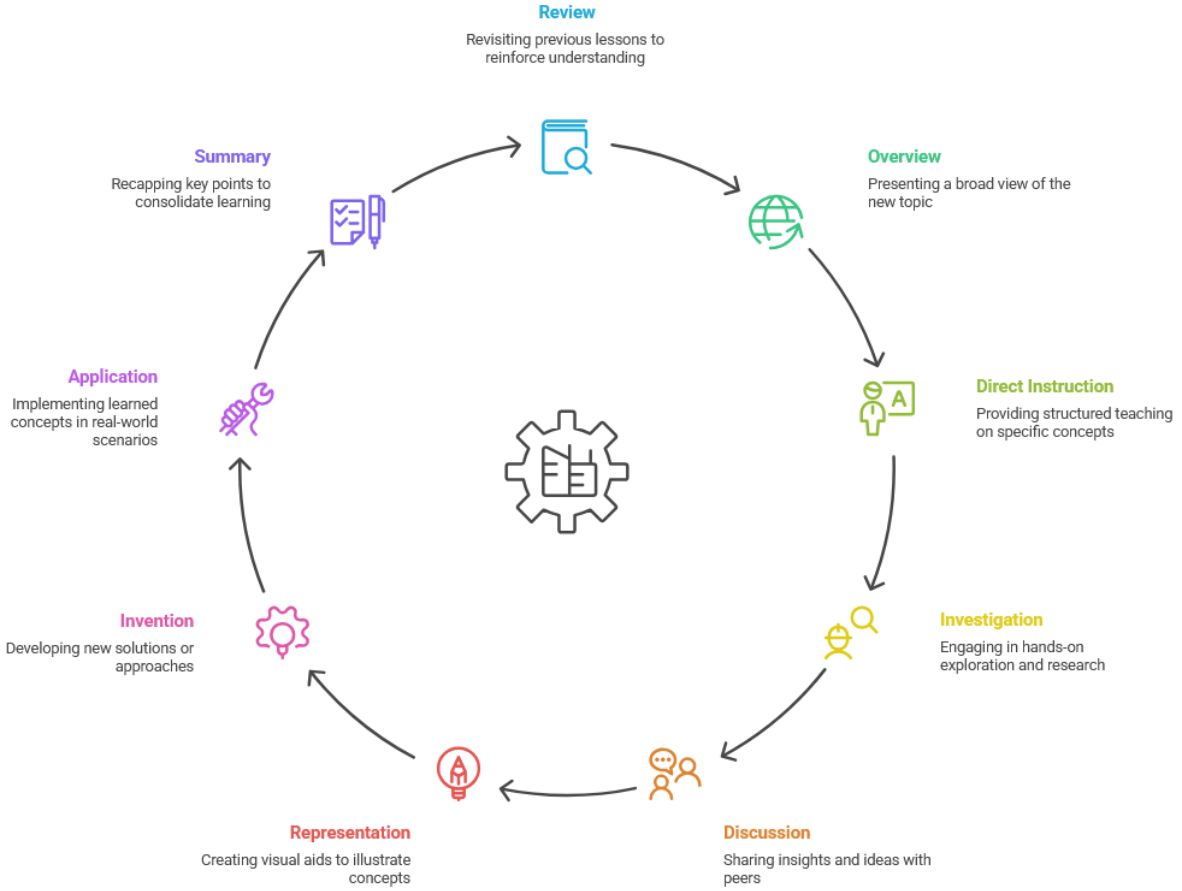

Figure 2. Stages of implementing Daniel's Model for developing cybersecurity concepts

The training program was carefully developed and implemented in alignment with the nine components of the Daniel's Model. The program spanned two weeks, with each day consisting of a 3-hour block featuring a mix of theory and a practical element. The activities included workshops, structured discussions, simulations, and co-planning lessons. Using observation checklists, tasks, and reflective journals, Daniel's Model fidelity and delivery consistency were monitored. This training empowered teachers to obtain and practice novel competencies, psychologically and pragmatically, to understand and teach the principles of cybersecurity in real classrooms, create and implement instructional activities, and support students in cultivating advanced critical and ethical reasoning on digital issues. The following activities were included in the training program:

1. ***Orientation*:** Teachers were presented with program expectations and goals, the initial importance of cybersecurity, and the importance of helping students learn about online threats and how to protect themselves along with safe ways to engage online. Teachers were directed to the learning expectations of the units and were asked to facilitate discussions on learning goals.
2. ***Content Delivery*:** Teachers presented students with some of the foundational concepts of cybersecurity and some active teaching strategies that promote and maintain student engagement while focusing on the virtualization of concepts.
3. ***Hands-on Exploration*:** Teachers initiated and developed experimental learning activities that enabled them to examine digital problems, make reasonable decisions about how to protect their personal information, and enact appropriate cybersecurity practices.
4. ***Collaborative Discussion*:** Teachers engaged in peer-to-peer interaction activities to create and refine educational dialogues that define and clarify educational problems through collaborative strategic thinking to enhance the critical thinking of students and to address multiple dimensions of learning.
5. ***Knowledge Representation*:** Teachers were facilitated to assemble their instructional design toolkits, create educational infographics, and utilize a variety of learning scaffolds that support students in organizing their thoughts and expressing their ideas.
6. ***Innovative Instruction*:** Teachers were stimulated to create participatory assignments that replicated real-world digital dangers and showed how to apply cybersecurity skills.
7. ***Classroom Implementation*:** Teachers applied the strategies into practice by guiding students in developing critical thinking, safe and responsible internet usage, and digital behavior within the designed educational activities.
8. ***Monitoring and Feedback*:** Teachers were instructed about the techniques of student response capturing, assessing student learning outcomes, designing instructional feedback, and adapting instructional approaches to student learning outcomes.
9. ***Reflection and Evaluation*:** Teachers engaged in systematic reflection and evaluation of the program, focusing on the effectiveness of instruction, student learning outcomes, and future improvements.

3-4- Cybersecurity Concepts Test

The Cybersecurity Concepts Test was created to gauge ninth-grade students' understanding of cybersecurity concepts as well as their safe digital practices. The test was designed to measure students' awareness and knowledge of the behavioral and cognitive dimensions of cybersecurity and indicate their ability to practice safe behaviors in the digital world.

The items of the test were designed to be in harmony with students' cognitive and language abilities. The items focused on comprehension, analysis, and decision-making in real-life digital scenarios. The scenarios were designed in a way that the students would meet in online activities that they engage in daily and have simple, straightforward language with no technical terms.

The test integrated fundamental firewalls and cybersecurity concepts with a risk management framework and applied security skills. The digital cybersecurity assessment consisted of thirty-seven multiple-choice questions in its initial version, divided into the following four areas of concentration:

1. ***Cybersecurity Concepts and Their Importance*:** This area assesses student comprehension of fundamental concepts of cybersecurity and their relevance to protecting devices, personal information, and topical security, along with safe practices in everyday digital interactions.

2. ***Digital Threats and Risks*:** This area assesses student awareness of technological threats, suspicious activities, malware and phishing, hacking, cyberbullying, and identity theft.
3. ***Cyber Protection and Security Practices*:** This area assesses student comprehension of cyber protective behaviors, their demonstrated willingness to practice preventive security behaviors of developing and maintaining strong passwords, setting up two-step authentication, and keeping devices and software up to date.
4. ***Responsible Digital Behavior*:** This area assesses understanding and maintaining ethical and legal standards of behavior and interaction online, such as respecting the right to privacy, communicating constructively, refraining from abusive behavior, reporting unsafe content, and promoting positive digital citizenship.

3-5- Validity and Reliability of the Test

The test was examined by specialists in curriculum and pedagogy, educational technology, measurement and evaluation, and cybersecurity to guarantee content validity. Every member of the committee was a seasoned professional who had designed assessment instruments for the relevant age group. The focused-on criteria were whether the questions accurately represented the concepts they intended to measure; the language was clear; the questions were phrased correctly; the answer choices were consistent with the standards of objective test construction; and whether the items were effective in measuring students' cognitive and affective skills. Four items were eliminated, and three others were modified based on the committee's comments to improve congruence and conceptual precision. Consequently, the last version of the test consisted of thirty-three items.

To assess reliability, the test was administered to 33 students who were not part of the main study sample, and the test was given to these students as a second administration two weeks later. The Pearson correlation coefficient of the two test administrations was 0.92, indicating reliability and consistency over time. Evidence from the analysis also suggested a range of difficulty indices of between 0.39 and 0.76, with discrimination indices between 0.40 and 0.75, confirming that the items were of good quality and that the test was able to effectively differentiate between high-achieving and low-achieving students.

Using Macdonald's Omega and Composite Reliability (CR), the construct validity of the findings was assessed, and an advanced analysis of the internal consistency of the variables was performed. Both Omega and CR internal reliability ranged from 0.917 to 0.942 and 0.914 to 0.939, respectively, exceeding the 0.70 benchmark desired. Average Variance Extracted (AVE) values ranged from 0.617 to 0.708, exceeding the 0.50 minimum target and demonstrating convergent validity. As per the established criteria of having the square root of AVE for each of the constructs to exceed the domain's correlations with other constructs, the discriminator validity was also examined, as each metric measured a distinct domain of cybersecurity awareness. Construct validity results are summarized in Table 1.

Table 1. Construct Validity and Reliability Indices for the Study Constructs

Constructs	Items	Macdonald's Omega (ω)	CR	AVE	√AVE
Cybersecurity concepts and their importance	7	0.917	0.914	0.617	0.785
Digital threats and risks	9	0.942	0.939	0.625	0.790
Protection methods and digital security	8	0.939	0.935	0.708	0.841
Responsible digital behavior	9	0.934	0.927	0.701	0.837

Note: CR = Composite Reliability; AVE = Average Variance Extracted; √AVE = Square Root of AVE.

The test was administered within a 45-minute period, providing students a sufficient time for thoughtful analysis and ensuring accurate measurement of their understanding of cybersecurity concepts and practical digital behaviors.

3-6- Data Collection and Analysis

A pre-test on cybersecurity concepts was administered to both the experimental and control groups to ensure equivalence in the level of digital concepts before starting the experiment. Results were analyzed using SPSS, where means and standard deviations were calculated, and an Independent Samples t-test was conducted to examine statistically significant differences between the two groups in the pre-test, as shown in Table 2 and Figure 3.

Table 2. The t-test results for group equivalence verification

Group	No.	Mean	St. dev.	df.	t-value	Sig.
Experimental	60	10.21	3.12	118	1.98	0.072
Control	60	10.33	3.05			

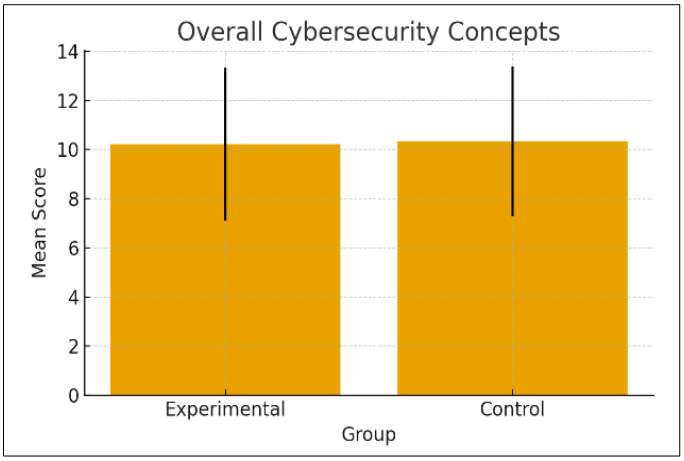

Figure 3. Pre-Test Score Means of Cybersecurity Concepts for the Experimental and Control Groups

Results in Table 2 and Figure 3 show no statistically significant differences between the mean scores of students in the experimental and control groups, where t = 1.98 at a significance level of 0.072, which is higher than the conventional level (0.05). This indicates the equivalence of the two groups in their level of cybersecurity concepts before applying the training program, supporting the credibility of interpreting post-test differences as resulting from the implementation of Daniel's model.

The intervention lasted for sixteen weeks, with three 45-minute-long sessions per week. The experimental group was taught using Daniel's model while the control group received education via the conventional method. Specific strategies were implemented to maintain fidelity to Daniel's Model throughout the intervention. Standardized observation checklists were used, and the research team performed routine checks to ensure the instructor model was implemented the same way for all the sessions. This ensured adherence to the frameworks, maintaining the quality and consistency of the intervention.

Post-test data was analyzed, as means and standard deviations for each group were computed. A t-test was performed to identify statistically significant differences in groups' performance at $p \leq 0.05$, and to analyze the differences within the experimental group between immediate and delayed post-tests administered 3 months later.

4- Results

4-1- Results of the First Question

The purpose of the first research question was to determine the effectiveness of Daniel's Model on cybersecurity concepts of the ninth-grade students. At the end of the intervention, students were given a post-test on cybersecurity concepts. T-test values were calculated to examine the existence of statistically significant differences between the experimental and control groups at ($p = 0.05$). The results are shown in Table 3 and Figure 4.

Table 3. Post-Test Results for Cybersecurity Concepts by Domain: Experimental vs. Control Groups

Domains	Group	N	Mean	SD	df	T-Value	Sig. (p-value)	Eta Squared (η^2)
Understanding the Concept and Importance of Cybersecurity	Experimental	60	6.74	0.733	118	6.21	0.002	0.48
	Control	60	4.95	1.668	118			
Digital Threats and Risks	Experimental	60	8.22	0.868	118	5.31	0.007	0.39
	Control	60	5.27	2.428	118			
Cyber Protection and Safety Practices	Experimental	60	7.67	0.935	118	6.98	0.000	0.53
	Control	60	5.36	2.497	118			
Responsible Digital Behavior	Experimental	60	8.72	0.733	118	4.79	0.008	0.34
	Control	60	4.98	3.734	118			
Total Score	Experimental	60	31.35	1.62	118	8.14	0.000	0.62
	Control	60	20.56	4.01	118			

Note: Maximum domain scores vary by number of items. Total maximum score = 33. η^2 (eta-squared) indicates the proportion of variance in scores attributable to the instructional method.

Table 3 and Figure 4 show that the experimental group achieved better results than the control group in every assessed area. This demonstrates that Daniel's Model provides students with effective cybersecurity education regarding ethical skills and practical abilities.

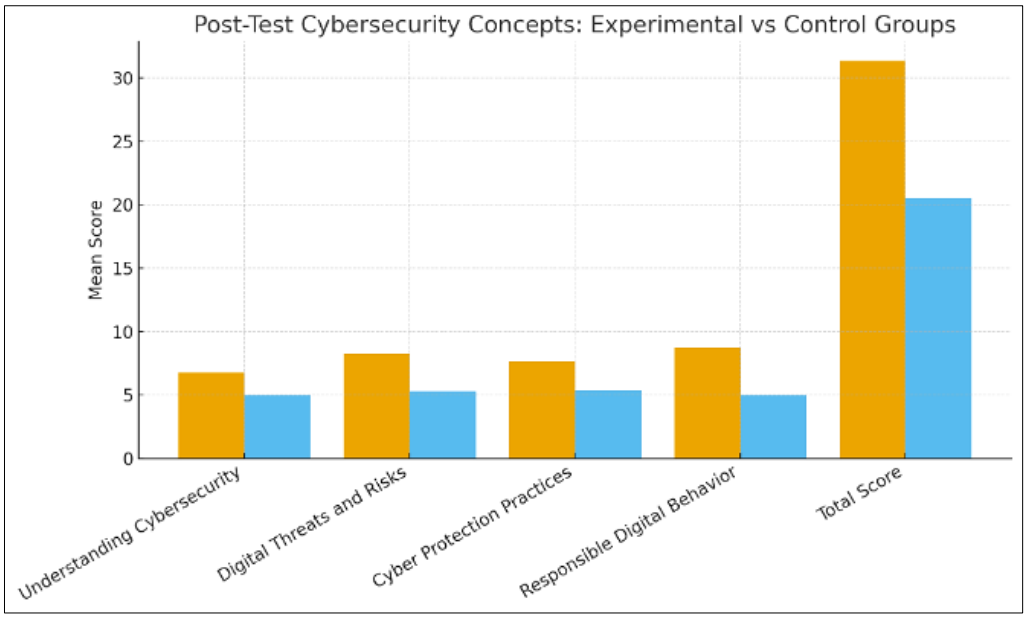

Figure 4. Performance Score Means of the Experimental and Control Groups on the Post-test

The experimental group in Understanding the Concept and Importance of Cybersecurity achieved better results than the control group because their mean score reached 6.74, while the control group scored 4.95. The two groups showed similar fundamental knowledge yet the t-test results ($t = 6.21$, $p = 0.002$) showed that students who received conventional instruction performed significantly worse than those who learned through Daniel's Model. The teaching method created a major impact on student conceptual understanding because its effect size ($\eta^2 = 0.48$) showed a strong influence. The results showed students learned cybersecurity concepts better through Daniel's Model because it used practical learning methods combined with actual examples and step-by-step guidance.

In Digital Threats and Risks, the experimental group achieved a mean score of 8.22, which was notably higher than the control group (5.27). The t-value of 5.31 and p-value of 0.007, together with a large effect size ($\eta^2 = 0.39$), indicate that the difference between the two groups is both statistically and practically significant. These results demonstrate that students taught by Daniel's model were better able to understand digital threats, including computer viruses, phishing, online scams, financial fraud, cyber fraud, and cyber bullying. Daniel's model, which includes various theories and simulative scenarios, as well as discussions and problem-centered approaches (PCA), offers students the opportunity to analyze and understand multiple threats, beyond the rote memorization required for passing exams.

The experimental group demonstrated better understanding of the Cyber Protection and Safety Practices, obtaining an average score of 7.67, while the control group scored 5.36. The results ($t = 6.98$, p 0.000) and effect size ($\eta^2 = 0.53$). This provides strong evidence of the applicability of Daniel's Model for building pertinent skills in cybersecurity. More specifically, the students in the experimental group demonstrated a greater ability to implement protective measures, i.e. strong passwords, regular software updates, two-factor authentication, and the adoption of safe digital practices. The findings showed the direct applicability of the experiential learning activities within Daniel's Model to facilitate the transfer of theoretical knowledge into practical behaviors.

Regarding Responsible Digital Behavior, the experimental group significantly outperformed the control group, obtaining an average of 8.72 while the control group averaged 4.98. The statistical values ($t = 4.79$, $p = 0.008$, $\eta^2 = 0.34$). This proves the positive effects. Therefore, Daniel's Model had a valuable effect on the participants' positive behavioral changes towards the ethical and responsible use of the internet. The experimental group members demonstrated an understanding of digital ethics related to online privacy, responsible and constructive online communication, and the ability to identify and report online abuse. The model's focuses on reflective thinking and ethical decision-making, as well as real digital environments where students must think about and manage real consequences.

Across all dimensions, the experimental group recorded a mean score of 31.35 (SD = 1.62), where the control group had a significantly lower mean score of 20.56 (SD = 4.01). With a t-value of 8.14 and, p-value of 0.000. This reveals that there is a statistically significant difference between the two groups. The very large effect size ($\eta^2 = 0.62$) indicates that there was a transformative effect of the Daniel's Model on the participants' overall knowledge, awareness, and practices related to cybersecurity.

The results, therefore, show that Daniel's Model is effective in enhancing various facets of cybersecurity learning and in furthering the cognitive, behavioral, and ethical aspects of the students. Along with the embedded active learning, cooperative-pairs problem solving, and real-world digital interactions, Daniel's Model fosters understanding, lasting behavioral change, and the application of cybersecurity. The Daniel's Model, unlike most instructional strategies, seems to truly prepare students to interact with the digital world in a safe, ethical, and responsible manner.

4-2- Results of the Second Question

This question examined the performance of the experimental group in delayed post-test compared to the immediate post-test for the concepts in cybersecurity. In this regard, means and standard deviations of the experimental group's score for both immediate and delayed applications were computed, as illustrated in Table 4 and Figure 5.

Table 4. Paired Samples t-test Results Comparing Immediate and Delayed Post-Test (Follow-up) for the Experimental Group

Domains	Group	N	Mean	SD	df	T-Value	Sig. (p-value)	Eta Squared (η²)
Understanding the Concept and Importance of Cybersecurity	Immediate	60	6.74	0.733	59	0.65	0.518	0.007
	Delayed	60	6.80	0.667	59			
Digital Threats and Risks	Immediate	60	8.22	0.868	59	0.57	0.570	0.005
	Delayed	60	8.28	0.725	59			
Cyber Protection and Safety Practices	Immediate	60	7.67	0.935	59	0.36	0.720	0.002
	Delayed	60	7.70	0.875	59			
Responsible Digital Behavior	Immediate	60	8.72	0.733	59	0.60	0.550	0.006
	Delayed	60	8.79	0.698	59			
Total Score	Immediate	60	31.35	1.62	59	0.72	0.475	0.009
	Delayed	60	31.40	1.56	59			

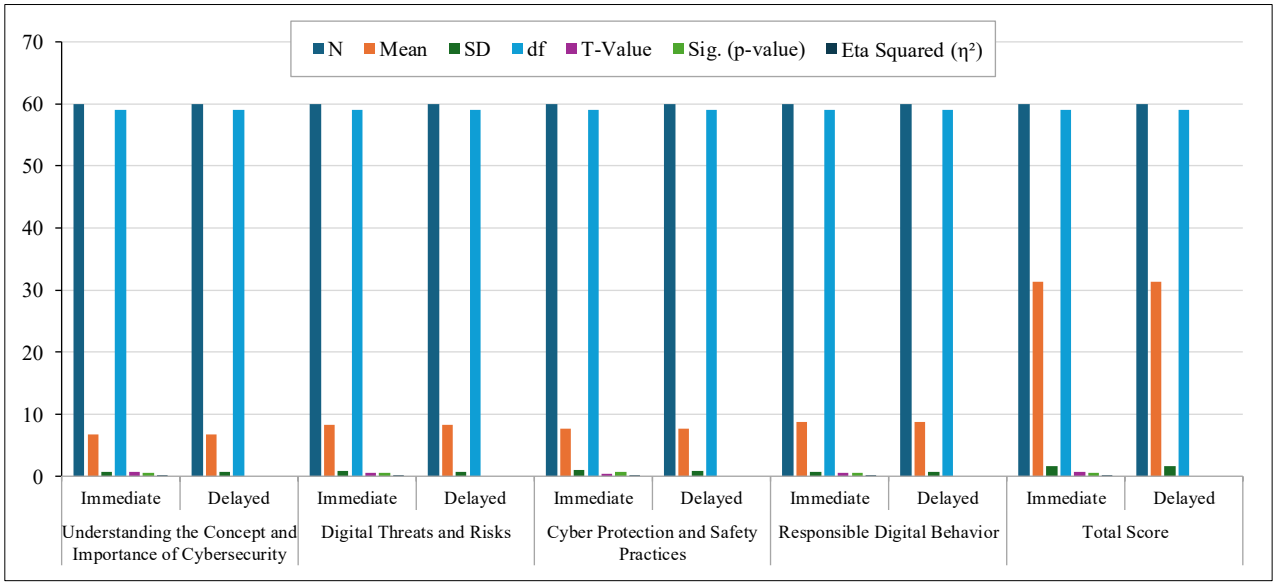

Figure 5. Performance of the Experimental Group: Immediate Post-test versus Delayed Post-test (Follow-up)

Table 4 and Figure 5 reveal a slight but consistent increase in the experimental group's mean scores in the delayed post-test compared to the immediate post-test across all dimensions, as well as in the overall score. Specifically, the mean score for Understanding the Concept and Importance of Cybersecurity increased from 6.74 to 6.80, Digital Threats and Risks from 8.22 to 8.28, Cyber Protection and Safety Practices from 7.67 to 7.70, and Responsible Digital Behavior from 8.72 to 8.79. Similarly, the overall mean score increased from 31.35 to 31.40.

The noted improvements may be modest but pedagogically relevant. They all point to improvement in the understanding of the most important learning aspect (short-term/long-term learning gains). The lack of evidence of learning loss is important since the interval between the tests is often an indicator of learning loss. In educational research, the fact that there is no learning loss is often an indicator of progress. In this case, progress is understood to be the result of learning, not short-term memorization.

The standard deviation values between immediate and delayed post-tests show minimal variation, which indicates students achieved more consistent results. The results demonstrated that all students in the experimental group made

progress without any exceptional cases. Daniel's Model produces this result because it promotes inclusive learning through its design, which combines student collaboration with hands-on digital experience and multiple opportunities to work with real-world digital content that benefits students with different learning needs.

Statistically wise, the results from the paired-samples t-test indicated no significance at the $p \leq 0.05$ level between the mean scores of the immediate and delayed post-tests. These results can be attributed to normal fluctuations and not differences in scores due to changes in performance. The evidence of such normal fluctuations is even more certain with the effect size values of $0.002 \leq \eta^2 \leq 0.009$. These values strongly indicate that there is no chance that the changes in the scores between the two test administrations could have caused a significant difference.

These outcomes should not be considered a negative factor regarding instructional intervention. Rather, they show that the learning gains through the Daniel's Model were maintained over time. There was no decline in the students' performance. In retention studies, not having statistically significant decline is considered a positive result. A positive result is especially true when there is a slight increase in the mean scores.

Overall, the results show that Daniel's model led to an immediate enhancement of students' knowledge and skills in cybersecurity. The model also encouraged the retention of the cognitive and the behavioral aspects over time. This trend illustrates the model's effectiveness in promoting constructivist learning through internal and deep understanding and thorough meaning-making. It also reflects the ability of the model to go beyond surface learning and rote learning.

The results support the effectiveness of Daniel's Model in assisting students in building digital competencies, such as identifying cyber risks, employing protective measures, and the responsible and ethical use of technology. Furthermore, the results support the current trends in teaching practices that are active, participatory, and student-centered in the teaching of cybersecurity. Unlike the conventional, lecture-based teaching that is, in most instances, a passive experience for students, the design of Daniel's model facilitates knowledge construction among students, which rises to higher cognitive levels. This enhances the students' conceptual understanding and behavioral mastery.

The results of the study confirm Daniel's model's short-term effectiveness as well as the necessity of building on this model for the long-term retention of knowledge, skills, and ethical behavior about cybersecurity. Given the growing digital complexities, it is essential to provide students with fundamental and enduring competencies in cybersecurity, which reinforces the need for the use of experiential and constructivist model(s) in teaching at the primary education level.

5- Discussion

5-1- Discussion of the First Research Question

The results showed that students who were taught using Daniel's Model had a better understanding of the components across all domains of cybersecurity knowledge than students in the control group. Students learn about protective measures and responsible behavior through digital tools in the constructivist model which promotes their active learning participation. The model achieved success through activities that presented authentic learning scenarios while students worked together to investigate topics using different methods that fostered their social learning with peers during the entire lesson.

The large effect size values showed that the differences between the experimental and control groups were real in a practical sense. Students who learned through Daniel's Model achieved higher knowledge levels and better skills and ethical understanding than students who received conventional teaching methods. Students demonstrated both positive and exceptional development in their abilities to recognize and handle cyber threats and their duties to use the internet properly. The model produces authentic academic performance improvements that exceed the normal range of student achievement changes.

The research results confirm previous studies that examined how students learn better through experiential, constructivist, and simulation-based learning methods in cybersecurity education. For example, Blažič & Blažič [24] noted that students' online security risk awareness and critical evaluative digital decision-making of online services were substantially improved using simulation-based instruction. The research results showed that students who used Daniel's Model achieved better results in their concept learning and their digital risk awareness and online responsibility skills. The research established two main findings that demonstrated that cognitive learning produced both immediate and long-lasting effects that proved to be both intense and persistent.

Earlier studies [14, 51-55] state that interactivity with computers allows students to build higher-order thinking skills, including analysis, critical thinking, and problem-solving. The current study concurs with these studies since students in the experimental group were better able to identify, assess, and articulate responses to various cyber threats. This study demonstrates that with appropriately designed instructional models, such as Daniel's Model, the cognitive and analytical improvements can be achieved at the primary education level.

The findings are consistent with the studies by Monteith et al. [22] and Pencheva et al. [21], who have established that human attention functioning with anticipatory awareness creates vital elements that lead to better cybersecurity practices. The students in this research study learned to recognize different cyber threats through their improved ability

to identify phishing attacks and malware incidents and social engineering schemes. The research results demonstrate that students can connect their knowledge understanding to their decision skills and prevention methods through systematic experiential learning methods, which previous research failed to achieve.

Research conducted earlier [20, 23, 56, 57] demonstrated that digital-field unethical conduct continues to spread without control because educational institutions lack proper teaching methods and digital learning programs fail to include ethical content. The research results indicate Daniel's model provides an effective solution to handle this problem by helping students develop ethical thinking abilities and reflection skills and digital conversation methods, which leads to their better management of digital privacy and digital communication ethics. The students documented an increase in dangerous digital content that appeared without proper authorization. The research shows that digital ethics behaviors can be learned through time-based education programs, which do not require students to develop their understanding through casual learning experiences.

The findings of the current study align with earlier research [28, 58], which emphasized the role of hands-on activities in building functional digital skills. Members of the experimental group were not only able to articulate the main ideas of cybersecurity, but they were also able to apply these ideas through creating strong passwords, using multi-factor authentication, and adjusting the settings of a system to be secure. This study contributes to existing research by demonstrating the ability to develop these skills in a standard school setting and that specialized labs, external programs, or sophisticated technology are not needed. This contrasts with some earlier studies that confirmed the need for such resource-based environments to assure quality cybersecurity education.

This study contributes to the limited Arabic body of research regarding the implementation of Daniel's Model in cybersecurity education. Furthermore, as most earlier studies focused on a single dimension, awareness or technical skills, the current study, however, could show significant and interrelated improvements across three domains of education—knowledge, skills, and attitudes, making it a valuable contribution to the existing body of research about cybersecurity education, both internationally and regionally.

The results support the growing idea that more interactive, constructivist, and experiential learning approaches yield better outcomes than lecture-based approaches for teaching cybersecurity. Nevertheless, the current study contributes to the field by shedding light on the retention of desirable learning outcomes over time. It also highlights the importance of integrating instruction, such as Daniel's Model, into school curricula to provide learners with the necessary holistic constructivist cybersecurity knowledge, skills, and DN (digital/ethics) so that they can assume responsible and active roles in protecting their digital environments and those of their communities in the future.

5-2- Discussion of the Second Research Question

The results showed that students of the experimental group were able to sustain their understanding and application of cybersecurity concepts over time without learning decay. This result aligns with Blažič & Blažič [24], who reported that the constructive learning theory studies, involving real, digital tasks, and cognitive processing, were deeper and more meaningful. However, although several studies stated learning outcomes almost exclusively immediately following instruction, most empirical studies that used a post-test to provide empirical evidence to strengthen cognitive retention have documented cumulative learning gains, and during the elapsed time, learning did not diminish.

The sustained performance may be attributed to the design of Daniel's model, which differs from other models in which instructional design is typically short-term and content-focused. Like the experiential learning models referenced by Blažič and Blažič [36] and Dimitriadou & Lanitis [42], Daniel's Model urges students to engage in problem-solving of real digital tasks that require critical thinking, practice, and reflection. So, in the current study, concepts of cybersecurity were not taught as isolated facts but rather as integrated and well-organized cognitive structures, which enables students to retrieve and transfer knowledge to use in novel digital environments well beyond the formal instructional time.

In contrast to earlier studies [23, 28, 58] that reported a gain in student awareness in cybersecurity, the current results show a more significant change from a shallow awareness to a deep, behavioral comprehension. Students were more aware of the dangers of digital environments, more protective of their own personal information, and more appreciative of the dangers of their own digital practices. This change is in line with the constructivist learning theory, which argues that lasting comprehension occurs when learners interact meaningfully with the material, rather than just memorize it. This study shows that experiential teaching enables students to gain deep knowledge that they can consistently practice.

The results reaffirm the claims of Pencheva et al. [21] and Monteith et al. [22], who emphasized the role of focus and proactive attention in promoting threat awareness. Like those studies, students were able to identify phishing, malware, cyberbullying, and online fraud. However, unlike those studies, the current one contributes to the body of evidence that suggests that students do not lose these abilities but retain them over time. This finding supports Amankwa's [20], which argued that instructional models, Daniel's in particular, restrict students' accessibility to cyber threats through cognitive and behavioral persistence.

Moreover, the lack of change in practicing protective digital behaviors (using strong passwords, enabling dual-factor authentication, updating software regularly, and being careful online), which aligns with best practices provided by international organizations (ex., ISTE and UNESCO), supports Bandura's social learning theory [10, 16], since students

had the opportunity to practice the modeled behavior repeatedly and in collaborative and simulated activities, which enabled them to model what they had learned and to demonstrate ethical and responsible behavior while operating online.

Statistically wise, the small differences indicate that learning outcomes were stable rather than declining, which is evidenced by the small eta squared (η^2) values and the mean scores of both immediate and delayed post-tests. This signifies effective knowledge consolidation and aligns with Blažič & Blažič [24] but extends their claims by showing that interactivity not only facilitates learning but also promotes the retention of learning.

Furthermore, the results contrast with Pencheva et al. [21], who investigated how teacher work activities create different needs than what students require when performing cybersecurity tasks. The Model of Daniel employs behavioral methods alongside cognitive techniques to solve the identified knowledge gap. The research by Monteith et al. [22], Rademaker [23], and Robins [26] focused on responsible digital citizenship as an end-of-the-line strategy; this study offers new empirical insights by illustrating the possibilities and value of such practices in everyday life.

The research study confirms previous findings about experience-based and constructive training methods that enhance cybersecurity education. Daniel's model is effective in the short and long term through enabling students to develop and retain knowledge and skills, especially in cybersecurity and digital citizenship. This impact is a value-add compared to standard pedagogical models; it demonstrates the need for more innovative, sustainable, and practice-oriented pedagogies to equip students to meet the complex and ever-changing demands posed by cybersecurity in the 'real world' digital environments.

6- Conclusion

The research data shows that Daniel's Model implementation in cybersecurity education brought major improvements to ninth-grade students who learned digital citizenship and gained practical skills and learned ethical conduct. The program educated students to identify cybersecurity principles as a single system, which demonstrated their ability to identify and manage various cyber threats.

The participants showed better protective practices because they used strong passwords with multi-factor authentication and they managed their personal data correctly and they followed proper online behavior ethics. The research results demonstrate that Daniel's Model enables students to develop complete digital competencies through academic learning and hands-on skills development and maintenance of ethical standards. The research findings expand Arabic cybersecurity education knowledge because they show constructivist teaching methods with interactive learning approaches help primary school students achieve effective learning outcomes.

The Model of Daniel established a successful connection between theoretical concepts and their actual application. The model used scenario-based learning, which combined collaborative problem-solving with interactive digital experiences that let students directly engage with content to build their critical thinking abilities and understand ethical digital practices. This method enabled students to learn new information and skills right away while also helping them keep the knowledge for an extended period because their test scores from the follow-up assessment showed improvement. The research shows that teachers need to direct experiential learning activities because they require ongoing education to learn both teaching approaches and digital equipment operation. The research confirms that Daniel's Model provides an effective method to develop students' sustainable digital literacy and their ability to practice ethics online and solve problems effectively. The research demonstrates how the model affects curriculum development and teaching methods that should be used in cybersecurity education programs.

6-1- Limitations and Future Research Directions

The research selected ninth-grade students from private international schools in Amman through convenience sampling. The program implementation became possible through this approach, but the research results cannot be applied to different educational levels or school environments or geographic locations. The study faces limitations in external validity, which requires researchers to exercise caution when they want to use these results for studying different groups of people. Scientists need to study participants from diverse backgrounds in upcoming research to determine which results apply to different population groups. The cybersecurity test showed excellent validity and reliability, but using one assessment tool restricted the measurement of students' complete behavioral responses and their actual digital skills. Research should focus on developing new assessment approaches that include observational checklists and performance-based tasks and reflective student reports to evaluate students' complete digital knowledge and skills and ethical conduct.

Considering the above limitations, future studies could also broaden the participants to include students from other areas and other school levels to gain further perspectives. Research using mixed methods of assessment, including scenario-based assessment, interviews, and observations from the classroom, would fine-tune understanding of the cognitive, behavioral, and moral competencies. Further research could examine the impact of Daniel's Model on other competencies such as analytical reasoning, problem-solving, and overall academic achievement. Other than cybersecurity, the model could be applied to other facets of digital education, especially in technological literacy and life skills, as it would enable students to meet digital challenges with confidence, responsibility, and competence, and in the process, contribute to the emergence of a digitally literate and competent generation.

7- Declarations

7-1- Author Contributions

Conceptualization, A.A.A., R.M.A., and O.M.A.; methodology, A.A.A., A.K.A., R.M.A., and O.M.A.; validation, A.A.A., R.M.A., O.M.A., and N.A.I.; formal analysis, A.A.A., E.M.K., O.M.A., and Y.Z.A.; data curation, A.A.A., E.M.K., O.M.A., and Y.Z.A.; writing—original draft preparation, A.A.A. and R.M.A.; writing—review and editing, A.A.A.; supervision, A.A.A.; project administration, A.A.A. All authors have read and agreed to the published version of the manuscript.

7-2- Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7-3- Funding

This work was financially supported, for authors affiliated with King Faisal University only, by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. KFU260544].

7-4- Acknowledgements

The authors affiliated with King Faisal University gratefully acknowledge the Deanship of Scientific Research at King Faisal University for providing financial support for this research. The authors from the University of Sharjah and Yarmouk University also extend their sincere appreciation to their respective institutions. The authors further thank all participants who took part in this study for their time and valuable contributions.

7-5- Institutional Review Board Statement

This study was reviewed and approved by the Deanship of Scientific Research at King Faisal University with the approval number: KFU-REC-2025Mar-EA000653, dated 13/3/2025.

7-6- Informed Consent Statement

Informed consent was obtained from all subjects involved in the study.

7-7- Conflicts of Interest

The authors declare that there is no conflict of interests regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

8- References

[1] Zucule de Barros, M. J., & Lazarek, H. (2018). A cyber safety model for schools in Mozambique. ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy, 2018-January, 251–258. doi:10.5220/0006573802510258.

[2] Huraj, L., Lengyelfalusy, T., Hurajová, A., & Lajčin, D. (2023). Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students. TEM Journal, 12(2), 623–633. doi:10.18421/TEM122-05.

[3] Lamond, M., Prior, S., Renaud, K., & Wood, L. A. (2025). Teachers' perspectives and practice of cybersecurity education in primary schools. Discover Education, 4(1), 312. doi:10.1007/s44217-025-00471-0.

[4] Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime. International Journal of Research in Business and Social Science, 11(4), 384–396. doi:10.20525/ijrbs.v11i4.1714.

[5] Ismail, M., Madathil, N. T., Alalawi, M., Alrabaee, S., Al Bataineh, M., Melhem, S., & Mouheb, D. (2024). Cybersecurity activities for education and curriculum design: A survey. Computers in Human Behavior Reports, 16. doi:10.1016/j.chbr.2024.100501.

[6] Lamond, M., Renaud, K., Wood, L., & Prior, S. (2022). SOK: Young Children's Cybersecurity Knowledge, Skills & Practice: A Systematic Literature Review. ACM International Conference Proceeding Series, 14–27. doi:10.1145/3549015.3554207.

[7] Yassin, W. A. K., & Raji, Z. H. (2012). The Constructivist Approach: Models and Strategies for Teaching Scientific Concepts. Noor Al-Hassan Library, Baghdad, Iraq.

[8] Pusey, P., & Sadera, W. A. (2011). Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. Journal of Digital Learning in Teacher Education, 28(2), 82–85. doi:10.1080/21532974.2011.10784684.

[9] Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, 30. doi:10.1016/j.ijcci.2021.100343.

[10] Al-Barakat, A. A., AlAli, R. M., Alotaibi, S. B., Alrosaa, T. M., Abdullatif, A. K., & Zaher, A. M. (2026). The contribution of early science education in developing children awareness of carbon footprints. Scientific Reports, 16, 4271. doi:10.1038/s41598-025-34469-3.

[11] Nicholson, J., Terry, J., Beckett, H., & Kumar, P. (2021). Understanding young people's experiences of cybersecurity. ACM International Conference Proceeding Series, 200–210. doi:10.1145/3481357.3481520.

[12] Lui, A., Womack, C., & Orton, P. (2025). Collaborative online international learning as a third space to improve students' awareness of cybersecurity. Education and Information Technologies, 30(10), 13835–13856. doi:10.1007/s10639-025-13336-8.

[13] Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. Computers and Security, 95. doi:10.1016/j.cose.2020.101827.

[14] Catota, F. E., Granger Morgan, M., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1), 1. doi:10.1093/cybsec/tyz001.

[15] NCSC-JO. (2025). The Jordanian national cybersecurity framework. National Cyber Security Center – Jordan. Available online: https://ncsc.jo/ (accessed on March 2026).

[16] Al-Barakat, A. A., Al-Hassan, O. M., AlAli, R. M., Al-Hassan, M. M., & Al sharief, R. A. (2023). Role of female teachers of childhood education in directing children towards effective use of smart devices. Education and Information Technologies, 28(6), 7065–7087. doi:10.1007/s10639-022-11481-y.

[17] Bataineh, R. F., Bataineh, R. F., AlAli, R. M., Alotaibi, S. B., Al-Barakat, A. A., Al-Saud, K. M., Aboud, Y. Z., & Ibrahim, N. A. (2025). Digital Frontiers: The Transformative Potential of E-Learning in Cultivating Arab Primary School Learners' Creativity. SAGE Open, 15(4), 21582440251408317. doi:10.1177/21582440251408317.

[18] Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., Gallus, P., & Fujdiak, R. (2025). Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education. Technology, Knowledge and Learning, 1-36. doi:10.1007/s10758-025-09840-y.

[19] Caulkins, B., Marlowe, T., & Reardon, A. (2019). Cybersecurity Skills to Address Today's Threats. Advances in Intelligent Systems and Computing, 782, 187–192. doi:10.1007/978-3-319-94782-2_18.

[20] Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of Information Security, 12(04), 233–249. doi:10.4236/jis.2021.124013.

[21] Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. IEEE Security and Privacy, 18(2), 68–74. doi:10.1109/MSEC.2020.2969409.

[22] Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Current Psychiatry Reports, 23(4), 18. doi:10.1007/s11920-021-01228-w.

[23] Rademaker, M. (2016). Assessing Cyber Security 2015. Information & Security: An International Journal, 34, 93–104. doi:10.11610/isij.3407.

[24] Blažič, A. J., & Blažič, B. J. (2025). Teaching and learning cybersecurity for European youth by applying interactive technology and smart education. Education and Information Technologies, 30(7), 9093–9120. doi:10.1007/s10639-024-13155-3.

[25] Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers and Security, 136. doi:10.1016/j.cose.2023.103585.

[26] Robins, A. (2015). The ongoing challenges of computer science education research. Computer Science Education, 25(2), 115–119. doi:10.1080/08993408.2015.1034350.

[27] Bataineh, M., & Bataineh, R. (2024). Personal Learning Environment and Writing Performance: The Case of Jordanian Young EFL Learners. SiSal Journal, 15(1), 65–85. doi:10.37237/150102.

[28] Chen, W., He, Y., Tian, X., & He, W. (2021).Exploring cybersecurity education at the K-12 level. Proceedings of SITE Interactive Conference. Association for the Advancement of Computing in Education, 108-114.

[29] Chindrus, C., & Caruntu, C. F. (2023). Challenges and Solutions in Designing a Network Architecture for Red and Blue Cybersecurity Competitions. 2023 27th International Conference on System Theory, Control and Computing, ICSTCC 2023 - Proceedings, 528–533. doi:10.1109/ICSTCC59206.2023.10308435.

[30] Cole, S. V. (2022). Impact of Capture The Flag (CTF)-style vs. Traditional Exercises in an Introductory Computer Security Class. Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE, 1, 470–476. doi:10.1145/3502718.3524806.

[31] Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. Simulation and Gaming, 51(5), 586–611. doi:10.1177/1046878120933312.

[32] Bataineh, R. F., & Alghareeb, M. B. (2025). Starfall as a Catalyst for Kuwaiti EFL Young Learners' Reading Comprehension: A Teacher's Reflections. Journal of Ethnic and Cultural Studies, 12(1), 141–153. doi:10.29333/ejecs/2338.

[33] Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. IEEE Transactions on Professional Communication, 52(2), 167–182. doi:10.1109/TPC.2009.2017985.

[34] Hong, W. C. H., Chi, C. Y., Liu, J., Zhang, Y. F., Lei, V. N. L., & Xu, X. S. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. Education and Information Technologies, 28(1), 439–470. doi:10.1007/s10639-022-11121-5.

[35] Antunes, M., Silva, C., & Marques, F. (2021). An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context. Applied Sciences (Switzerland), 11(23), 11269. doi:10.3390/app112311269.

[36] Blažic, B. J., & Blažic, A. J. (2024). Towards Modern Teaching and Effective Learning of Cybersecurity. Proceedings of International Conference on Research in Education and Science (ISTES), 10(1), 1809–1821.

[37] Burns, M. A., Johnson, V. N., Grasman, K., Habibi, S., Smith, K. A., Kaehr, A., Lacar, M. F., & Yam, B. (2023). Pedagogically Grounded Techniques and Technologies for Enhancing Student Learning. Advances in Engineering Education, 11(3), 77–107. doi:10.18260/3-1-1153-36049.

[38] Han, L., Harries, J., & Brown, P. (2013). Building a virtual constructivist learning environment for learning computing security and forensics. ITALICS Innovations in Teaching and Learning in Information and Computer Sciences, 12(1), 49–61. doi:10.11120/ital.2013.00006.

[39] Dhungana, R. K., Gurung Dr, L., & Poudyal, H. (2023). Cybersecurity challenges and awareness of the multi-generational learners in Nepal. Journal of Cybersecurity Education, Research and Practice, 2023(2), 5. doi:10.32727/8.2023.17.

[40] Rajbhandari, J., & Rana, K. (2023). Cyberbullying on Social Media: an Analysis of Teachers' Unheard Voices and Coping Strategies in Nepal. International Journal of Bullying Prevention, 5(2), 95–107. doi:10.1007/s42380-022-00121-1.

[41] Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers and Security, 119, 102756. doi:10.1016/j.cose.2022.102756.

[42] Dimitriadou, E., & Lanitis, A. (2023). A critical evaluation, challenges, and future perspectives of using artificial intelligence and emerging technologies in smart classrooms. Smart Learning Environments, 10(1), 12. doi:10.1186/s40561-023-00231-3.

[43] Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information and Knowledge Management, 15(1), 1650007. doi:10.1142/S0219649216500076.

[44] Attia, M. A., & Ali, M. (2015). Constructivism and its Applications Modern Teaching Strategies. Dar Al-Methodology, Amman, Jordan.

[45] Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. Computers and Education, 186. doi:10.1016/j.compedu.2022.104536.

[46] Taherdoost, H. (2024). Towards an Innovative Model for Cybersecurity Awareness Training. Information (Switzerland), 15(9), 512. doi:10.3390/info15090512.

[47] van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? Journal of Cybersecurity, 6(1), 1–8. doi:10.1093/CYBSEC/TYAA019.

[48] Zorlu, E. (2023). An Examination of the Relationship between College Students' Cyberbullying Awareness and Ability to Ensure their Personal Cybersecurity. Journal of Learning and Teaching in Digital Age, 8(1), 55–70. doi:10.53850/joltida.1087377.

[49] Salazar, M., Gaviria, J., Laorden, C., & Bringas, P. G. (2013). Enhancing cybersecurity learning through an augmented reality-based serious game. IEEE Global Engineering Education Conference, EDUCON, 602–607. doi:10.1109/EduCon.2013.6530167.

[50] Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children's understanding of personal data and privacy online–a systematic evidence mapping. Information Communication and Society, 24(4), 557–575. doi:10.1080/1369118X.2019.1657164.

[51] Saglam, R. B., Miller, V., & Franqueira, V. N. L. (2023). A Systematic Literature Review on Cyber Security Education for Children. IEEE Transactions on Education, 66(3), 274–286. doi:10.1109/TE.2022.3231019.

[52] Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. Applied Sciences (Switzerland), 12(5), 2589. doi:10.3390/app12052589.

[53] Pramod, D., & Raman, R. (2014). A study on the user perception and awareness of smartphone security. International Journal of Applied Engineering Research, 9(23), 19133–19144.

[54] Modise, E. (2023). Remote working responsible for surge in cybersecurity threats in Africa, according to INTERPOL. TechCabal, Lagos, Nigeria. Available online: https://techcabal.com/2023/07/04/remote-working-cybersecurity-africa/ (accessed on March 2026).

[55] Shen, L. W., Mammi, H. K., & Din, M. M. (2021). Cyber Security Awareness Game (CSAG) for Secondary School Students. 2021 International Conference on Data Science and Its Applications, ICoDSA 2021, 48–53. doi:10.1109/ICoDSA53588.2021.9617548.

[56] Huang, K., Madnick, S., Zhang, F., & Siegel, M. (2022). Varieties of public–private co-governance on cybersecurity within the digital trade: implications from Huawei's 5G. Journal of Chinese Governance, 7(1), 81–110. doi:10.1080/23812346.2021.1923230.

[57] Chang, C. Y., & Hwang, G. J. (2019). Trends in digital game-based learning in the mobile era: A systematic review of journal publications from 2007 to 2016. International Journal of Mobile Learning and Organisation, 13(1), 68–90. doi:10.1504/IJMLO.2019.096468.

[58] Santelices, R. B. (2025). A Students' Perspective on Cybersecurity Awareness and Education. International Journal of Research and Innovation in Social Science, IX(IIIS), 7976–7988. doi:10.47772/ijriss.2025.903sedu0597.