International Journal of Innovative Research and Scientific Studies, 8(1) 2025, pages: 1516-1529

IJIRSS
International Journal of Innovative Research & Scientific Studies

**ISSN:** 2617-6548

URL: www.ijirss.com

# Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps

Mostafa Hussam Mostafa Altarawneh[1], Ahmad Althunibat[2*], Mohmmad Husien Almajali[3], Naif Alzriqat[4], Seif Alazzam[5]

[1]*Petra University, Jordan.*
[2]*Department of Software Engineering, Faculty of Science and Information Technology, Al-Zaytoonah University of Jordan, Jordan.*
[3]*Al-Zaytoonah University, Jordan.*
[4,5]*Philadelphia University, Jordan.*

Corresponding author: Ahmad Althunibat (*Email: a.thunibat@zuj.edu.jo*)

## Abstract

In recent times, the widespread use of the Internet by various social groups has led to an increase in cyber risks and threats. Consequently, it has become crucial to educate these groups, particularly younger age groups, on the importance of cybersecurity to prevent them from falling victim to these risks. The study will focus on the comprehension of factors affecting cybersecurity among school students and the prevention of cyber threats and risks targeting the younger generation. A cross-sectional survey was conducted on students from middle school in Jordan, using a standardized questionnaire with 37 questions distributed under three categories: demographic data, cybersecurity awareness, and influencing factors. For this particular research study, the responses gathered from the open-ended questionnaire were analyzed, where multiple regression analysis was conducted, and five major research hypotheses were proposed and verified. The results indicate that it can be deduced that the level of knowledge about passwords, social networking sites, and legal aspects influences the level of cybersecurity awareness among the students. Other significant correlates of awareness were self-perceived awareness and education in cybersecurity; the model accounted for 67.5% of the variance in levels of awareness. The study also establishes that awareness of cybersecurity issues must be based on knowledge and should incorporate an educational process that targets young people. Critical sections to be covered by the specialized programs are password protection and appropriate use of the Internet. It is recommended that within the institutions delivering education, there should be constant cybersecurity training sessions with an emphasis on activities such as simulations and workshops conducted by experts to improve their awareness and subsequent action among learners.

**Keywords:** Cyber risks, Cybersecurity awareness, Cybersecurity education, Knowledge gaps, Legal implications.

**DOI:** 10.53894/ijirss.v8i1.4696
**Funding:** This study received no specific financial support.
**History: Received:** 17 December 2024/**Revised:** 21 January 2025/**Accepted:** 29 January 2025/**Published:** 14 February 2025

**Competing Interests:** The authors declare that they have no competing interests.
**Authors' Contributions:** All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
**Transparency:** The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
**Publisher:** Innovative Research Publishing

## 1. Introduction

The Internet has become integral to modern life, involving everyone in their day-to-day activities in various aspects such as learning, entertainment, and interaction among children. However, the enhanced and frequent use of internet activities among the young group of people exposes them to numerous cybersecurity threats. These include exposure to vulnerabilities such as phishing, contracting malware, violation of privacy, and social engineering techniques that can result in the impersonation or piracy of personal information or unauthorized access to data [1]. Children and teenagers, due to their limited knowledge and experience in identifying online threats, are particularly vulnerable [2].

The growth of these threats targeting children proves that there is an evident necessity to improve children's cybersecurity literacy through education. Various programs have been initiated around the world aimed at teaching children about online safety, but what has been done is still inadequate concerning the core aspects of cybersecurity [3]. These threats pose a higher risk since students primarily utilize Information Technology (IT) tools in their day-to-day studies.

Although there are ongoing efforts to encourage students to understand the risks involved in engaging in online activities, existing research studies fail to capture the effects of numerous factors that influence students' perception of the dangers of using the internet. Much of the previous research includes general recommendations, for instance, not to use particular sites and not to share data with anyone. However, there are several weaknesses, such as password handling, personal attitudes and perceptions towards cybersecurity, awareness of security risks related to social networks, and legal knowledge [4].

However, no research examines these variables and how they influence young students as a whole. Most importantly, middle school students (ages between 13-15 years) constitute the target group because, at that age, children transition from limited Internet use to increased Internet use in social networking and learning. This research aims to fill this gap by investigating the role of multiple variables and how they collectively influence students' cybersecurity awareness.

Thus, the requirement for an appropriate cybersecurity education model has emerged, taking into account that the threats are growing and targeting younger people. Although many students comprehend the general ideas of good passwords, the majority of them do not apply them regularly. Studies have shown that since mastering difficult-to-memorize passwords is a challenge, students are likely to create weak passwords and expose themselves to potential threats [5]. Additionally, when they engage in social media activities without sufficient knowledge of privacy features and security measures, they further expose themselves to cyber crimes [6].

This research is based on the fact that the current theoretical model of cybersecurity awareness is rather limited and lacks specific aspects of cybersecurity that are crucial in today's workplace, including passwords, social media, and legal issues. Therefore, if students acquire such knowledge, educational institutions can promote a reduced increase in students' vulnerability by helping them experience safer Internet usage.

The study highlights the growing need to teach cybersecurity in schools to mitigate the increasing risks associated with Internet use. A model was developed to explore the factors contributing to cybersecurity awareness, and several hypotheses were proposed to examine their impact. The model includes five key components: knowledge of browser security, knowledge of social network platforms, self-perception of cybersecurity awareness, knowledge of legal issues, and cybersecurity education.

All the components play an important role in an individual's perception of cybersecurity in general. To this end, five hypothesis statements were developed to ascertain the relevance of each of these components regarding the study. Based on the knowledge of passwords and their management, Hypothesis H1 suggests that password management knowledge significantly enhances cybersecurity awareness. Hypothesis H2 states that knowledge in the use of browsers enhances cybersecurity awareness, while Hypothesis H3 deals with self-perception of cybersecurity awareness. Hypothesis H4 posits that increasing students' awareness through cybersecurity education would be effective, while H5 focuses on the effectiveness of legal knowledge in improving awareness levels regarding responsible actions on the internet and the law. Therefore, such hypotheses help to identify the prospects of different elements that comprise the comprehensive knowledge of cybersecurity.

This implies that although there are many cybersecurity awareness programs in place, they do not cater to middle school students. These programs are generally not very specific for this age group, considering the issues of freedom and security at these ages. The central research question is thus focused on unveiling the correlation or contribution of password creation and management, knowledge of social networks, cybersecurity education, and legal literacy to the enhancement of students' cybersecurity awareness. The main research question is: "How do password management, social network knowledge, cybersecurity education, and legal awareness collectively impact the cybersecurity awareness of students aged 13 to 15?"

This research aims to investigate students' factors related to security awareness in middle school, create a model of awareness and a training program covering technical and legal aspects, as well as general education techniques, and propose recommendations for enhancing training measures in schools to protect students from cyber threats.

The remainder of this paper is organized as follows: Section 2 discusses the related works, and Section 3 presents the proposed awareness model. Section 4 details the methodology used to assess cybersecurity awareness, while Section 5 presents the results and discussion based on the dataset collected in this study. Finally, Section 6 provides the conclusions and recommendations.

## 2. Related Work

The concept of cybersecurity, according to Sarker, et al. [7], is a law used to protect communications and information technology systems from electronic attacks and various threats on the Internet. It is linked to several aspects, including measures to protect information technology, data, communications, and the primary information it contains, its processing, its transmission, and so on. The International Telecommunication Union (ITU) defines cybersecurity as "the set of security tools, policies, concepts, security safeguards, guidelines, risk management approaches, procedures, training, best practices, safeguards, and technologies that can be used to protect the cyber environment." In addition to the organization's and user's assets, cybersecurity strives to ensure that the security characteristics of the organization and user's assets are achieved and maintained against relevant security risks in the cyber environment [8]. Cybersecurity at the present time has become a technical challenge for societies and governments alike, and although it constitutes a great challenge, awareness of this challenge is still limited. However, the public's behavior towards dealing with the Internet does not reflect the required level of awareness [9]. We can describe cybersecurity as an activity or event to protect communications and information systems from exploitation, unauthorized access, or hacking attempts. Therefore, knowledge of cybersecurity helps prevent people from cyber threats such as ransomware [10]. Cybersecurity awareness is not only about knowledge but also about converting what has been learned into real practice, which is a continuous process that requires modification in subsequent iterations to improve its usability as well as its sustainability [11]. Cybersecurity awareness is defined as "a methodology for Internet users to be sensitive to various cyber threats and the vulnerability of computers and data to these threats." It is also defined as the degree to which the user can understand the importance of information security and their duties in practicing cybersecurity, ensuring high levels of information control to protect the organization's data and networks [8]. Cybersecurity awareness campaigns focus primarily on raising the level of cybersecurity awareness for users. The success of such security campaigns depends primarily on methods of communicating information and ensuring that users are aware of the rules of information security and act accordingly [1].

All software products should have security features, but when kids are involved, security issues become much more vital. One of the most important aspects of security is cybersecurity; when children are involved, cybersecurity refers to all the online risks that could harm them and the protective measures that can be taken for them and their caregivers, including the knowledge that children have about the different cybersecurity risks. Researchers in the field of child–computer interaction (CCI) have long been concerned with protecting children's privacy and security. A 2013 literature review [12] provided an overview of the state of CCI research. The infiltration of social and cloud technologies in CCI and the ensuing threats to children's security and privacy were one of the four main issues they highlighted for the CCI community. Due to their upbringing in an environment where technology permeates every aspect of their lives, children today face hazards that previous generations would have thought unthinkable [12]. Findings demonstrate that cybersecurity awareness programs are beneficial for kids; in order to guarantee better cybersecurity knowledge and abilities, these initiatives must be strengthened. The need for this education is supported by the fact that cyber dangers are always changing. Smith [13] stresses the need for teaching the next generation cybersecurity and digital literacy. It is dangerous for children to believe that they won't face threats from their peers. Children are especially vulnerable since they do not fully understand the dangers that come with the gradual collection of personal information [14]. Although they frequently have strong feelings about their private information being disclosed online to their parents, friends, and other people, they continue to be ignorant of other participants in digital ecosystems, such as platforms, app developers, bad actors, and others [14, 15].

Even though children are aware of the importance of using strong passwords, some of them choose simple passwords because they are easier to remember. The password creation, password maintenance, and authentication stages make up the password management lifecycle, and it is important to take users' password behaviors into account from a broad perspective. Individual factors, the capacities and constraints of the human information processor, and the relationships across stages in the lifecycle are reflected in the behaviors of users [16]. According to a study on password generation involving 81 individuals [5], the first position in the password is dominated by capital letters, and the rate of capital letters decreases significantly at the second position, while the rate of lowercase letters increases significantly at position two. However, according to new password standards released by the National Institute of Standards and Technology (NIST), lengthier passwords, or passphrases, are encouraged, and complexity requirements—that is, the need for a mix of character types—are loosened [17]. Online safety education often targets parents or children and emphasizes protecting personal information, reporting or avoiding cyberbullying, and preventing young people from being sexually exploited [18, 19]. The Internet & American Life Project [20] of the Pew Research Center has conducted focus groups and online surveys to learn more about the views and behaviors of U.S. youth regarding social media privacy. They discovered a low level of concern over third-party access to social media data, a rise in the online sharing of personal information (in comparison with previous data), and active use of privacy measures to manage information and distribute it selectively. Ninety-one percent of these teenagers said they had shared images of themselves online, and most of them had also shared personal details like their location, email address, and real name.

## 3. Proposed Awareness Model

Technological advancements in computer applications and computing environments have facilitated the growth of unstructured social networks and active applications, often used by thousands of users simultaneously. However, these same platforms have also been exploited by cybercriminals, hackers, and other malicious actors to identify and exploit system vulnerabilities [21]. As a result, cybersecurity has emerged as a significant challenge in today's digital world, with an increasing need to raise awareness and educate internet users about the potential threats and vulnerabilities they face online [22].

The increasing exposure of younger generations to the internet, despite their familiarity with digital tools, has highlighted the importance of intensifying cybersecurity education in schools. Understanding how the human factor influences children's online behavior and attitudes is essential to strengthening their awareness of cyberattacks and promoting responsible digital citizenship [23]. A proposed model provides specific criteria that target the advancement of cybersecurity awareness through:

Knowledge and self-awareness of cybersecurity, understanding of legal issues related to cybersecurity, and education are designed to have a positive impact on children's cybersecurity awareness, as described below (see Figure 1).

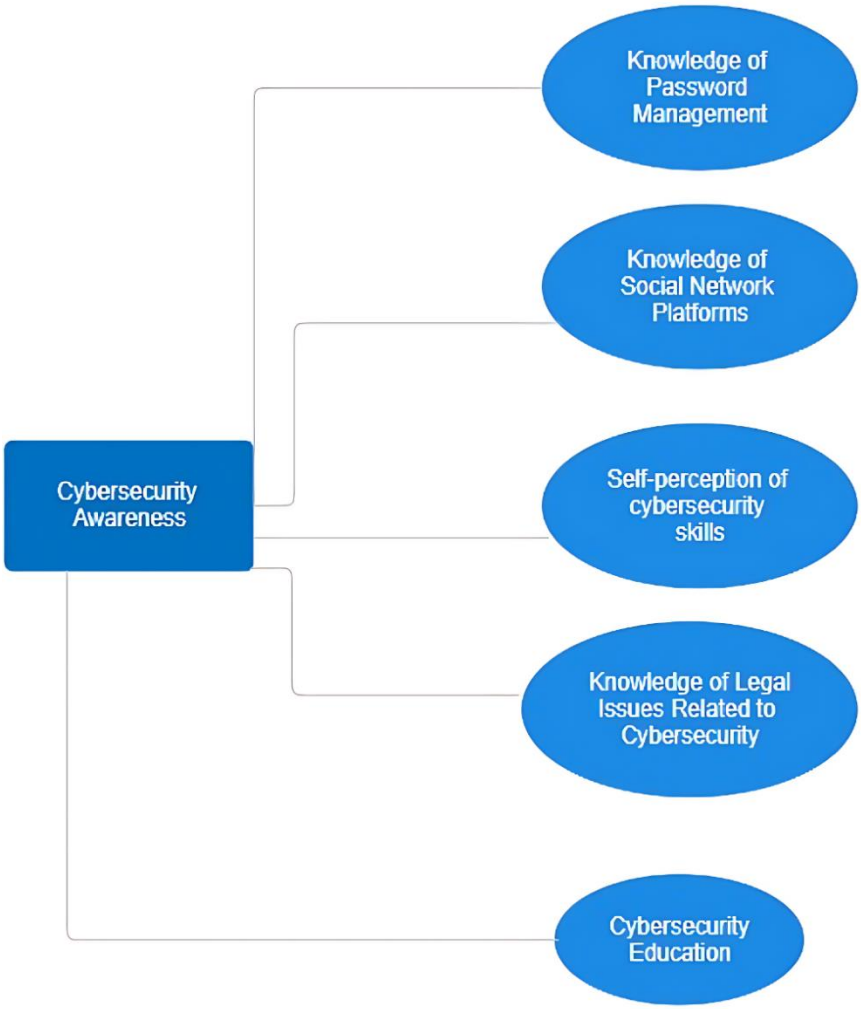


**Figure 1.**
Cybersecurity awareness model.

### *3.1. Cybersecurity Awareness*

The growing focus on cybersecurity awareness can be directly linked to the rise in cybercrime incidents and cybersecurity errors. Awareness is critical for all individuals, as no one is immune to the potential risks and consequences of cyberattacks. Protected sensitive information specifically needs tight security measures because it requires the prevention of unauthorized access [21]. The human aspect of cybersecurity requires individuals to demonstrate responsible behavior when using modern technology. Cybersecurity incident occurrences decrease when people become more mindful of these issues because this constitutes the primary approach to managing human-caused security issues [11]. IT security awareness programs teach people how to identify security risks in information systems together with proper risk response procedures. People need to understand both the threats against their digital assets and the importance of protection because these security programs build essential security culture foundations [4]. Basic security education must be understood together with internet activity surveillance for irregular behaviors to recognize cybersecurity threats and their negative consequences [24].

*3.2. Impact of Knowledge of Password Management on Cybersecurity Awareness*

The fundamental aspect of cybersecurity training focuses on password management principles. The protection of online accounts requires passwords that have at least twelve characters made up of letters, symbols, and numbers. Students need instructions related to password security to develop stronger cybersecurity awareness [25]. Understanding password confidentiality among children leads them to embrace safe practices, thus decreasing their risk of cyber threats [26].

For years, passwords have served as the main access security method for physical and digital systems. Modern-day passwords continue to serve as a primary defense mechanism for protecting user access because appropriate password handling practices enhance cybersecurity awareness [27].

*Hypothesis ($H_1$): Knowledge of password management significantly enhances cybersecurity awareness.*

*3.3. Impact of Knowledge of Social Network Platforms*

Social media plays a significant role in information dissemination and image building, where user awareness positively influences the disclosure of information [28]. These platforms enable users to gather enormous amounts of data, which creates both beneficial and adverse effects. Unintended consequences, such as unauthorized access to personal information, can result in security breaches widely reported in the media, including cybercrimes like identity theft and the usurpation of personal information [28]. The transparency of social media accounts increases the risk of exposure or hacking, leading to potential security losses [6]. Hackers often employ social engineering techniques to obtain users' personal data, granting them access to sensitive information without requiring additional compensation. Additionally, the active participation of students on social media, coupled with occasional sharing of sensitive content, reveals that a majority of students engage actively on these platforms, potentially exposing themselves to security risks [25].

*Hypothesis ($H_2$): Knowledge of social network platforms has significantly enhanced cybersecurity awareness.*

*3.4. Impact of Self-Perception of Cybersecurity Awareness on Cybersecurity Awareness*

Self-perception of cybersecurity awareness plays a vital role in shaping an individual's cybersecurity awareness. A person's understanding of their abilities and place in the digital world influences how they approach cybersecurity issues. Self-perception improvement achieved through education and awareness delivers informed users who behave cautiously online, which helps to enhance overall cybersecurity awareness [29]. The growing number of cyberattacks now focuses on human weaknesses, which requires individuals to keep themselves safe by adopting proactive safety measures. Individuals with self-awareness in cybersecurity develop improved decision-making abilities, which decrease their exposure to cyberattacks [3].

*Hypothesis ($H_3$): Self-perception of cybersecurity Awareness significantly enhances cybersecurity awareness.*

*3.5. Impact of Cybersecurity Education on Cybersecurity Awareness*

Enhancing cybersecurity awareness faces its main barrier from educators and students having insufficient knowledge and expertise. Acquiring knowledge in cybersecurity becomes essential to develop individual skills that help recognize and deal with cyber threats. Educational institutions, together with domestic units and state authorities, should develop cybersecurity training to boost overall security consciousness among the population [10, 26]. Running Capture the Flag (CTF) competitions features real-world security drills that help participants enhance their cybersecurity awareness and knowledge about potential threats [30]. The scientific community also contributes by raising awareness and improving education on cybersecurity issues [31].

*Hypothesis ($H_4$): Cybersecurity education significantly enhances cybersecurity awareness.*

*3.6. Impact of Knowledge of Legal Issues on Cybersecurity Awareness*

Children need to understand legal concepts related to cybersecurity to improve their awareness levels. Children who understand cyberbullying laws, data privacy regulations, and online scam rules become more aware of the legal effects of their online activities, which leads them to develop appropriate internet behavior. The legal awareness level holds critical importance because it safeguards personal information and promotes ethical digital citizenship [32]. Understanding their rights and legal online conduct gives children the ability to use the digital world with enhanced security and conduct. By acquiring these understanding principles, children become more secure online while creating a safer online environment for everyone.

*Hypothesis ($H_5$): Knowledge of legal issues related to cybersecurity significantly enhances cybersecurity awareness.*

## 4. Methodology

*4.1. Research Tools*

The research implemented surveys to collect data through questionnaires because this method is commonly used in quantitative investigations. The questionnaires were designed to collect information that aligns with the research objectives. They were distributed electronically via Google Forms and sent to children's schools, allowing respondents to complete them directly. The researcher received the results immediately, making online surveys a time-efficient and cost-effective approach that also overcomes geographical limitations. The questionnaire comprises 37 questions, organized into the following sections:

Section One: This section contains eight questions aimed at collecting demographic information from the respondents, such as age, gender, and basic usage of smart devices.

Section Two: This section includes 29 questions focused on assessing the cybersecurity awareness of children. These questions are divided into five categories: knowledge, self-perception of cybersecurity awareness, and cybersecurity education. They are based on previously conducted research [1, 2, 25, 33-35]. The questions in this section explore students' behavior and their understanding of cybersecurity concepts when using the internet.

The analysis of the intercorrelation among variables was conducted using the Statistical Package for the Social Sciences (SPSS). To facilitate the interpretation of the collected data, the demographic characteristics of the sample were analyzed using descriptive statistics. Additionally, correlation analysis was employed to identify relationships between the key variables, while multiple regression analysis was applied to assess the contributions of password management, cybersecurity training, and legal literacy to students' overall cybersecurity awareness.

This study is therefore qualitatively different from other similar studies in the following ways. Unlike other prior research in the domain of cybersecurity awareness that may usually involve qualitative methodologies, such as interviews or descriptive analyses, the present research employs a more extensive quantitative analysis. In an important way, multiple regression analysis, in particular, enables the determination of the significance of all these components on focal aspects such as password management, cybersecurity training, and legal awareness. This is done to increase the internal validity of the research, unlike most research studies that consider each factor of the independent variable in isolation from the other factors while determining its effects on the dependent variable, in this case, students' cybersecurity awareness. Furthermore, prior research has included mainly the overall or older learners, while the present study is concerned with MS students only (ages 13-15), which has been a neglected age range in previous research.

### *4.2. Study Setting and Participants*

The survey was initially designed in English and subsequently translated into Arabic to ensure clarity for the students and to prevent any potential confusion, given that Arabic is their native language. To validate the questionnaire, it was reviewed by a specialist with extensive knowledge and experience. The specialist assessed each item in terms of language accuracy, alignment with the research objectives, and appropriateness of wording. The specialist made alterations to specific phrases by recommending new additions, revisions, and reformulations.

The study focused on a group of teenagers, specifically middle school students in Jordan. The total population of this group across all Jordanian governorates was 20,736 children, aged between 13 and 15 years. Using the statistical equation $\frac{z^2 \times p \times (1-p)}{E^2}$, it was determined that the sample size should exceed 250 students. This age group was chosen due to the scarcity of studies focused on it, making this research unique in Jordan. Additionally, this stage is when children begin using the internet daily, making them the most relevant demographic for examining issues related to cybersecurity education.

To ensure the comprehensibility of the questionnaire and to gauge the students' ability to respond, a pilot questionnaire was distributed to 10 children. Following this, 300 questionnaires were distributed to middle school students in Amman, Jordan, with 275 being retrieved. The researcher visited the schools, presented the questions, and clarified any items that the students found challenging. There was notable interaction with the children during this process. After the students completed the questionnaires, all were collected. Schools were selected based on the population density of the area to ensure accurate and representative results.

### *4.3. Inclusion and Exclusion Criteria*

Participants must be between 13 and 15 years old. Those who are younger than 13 years old or older than 15 years old were excluded because the focus of this study was on the level of cybersecurity awareness among middle school students.

### *4.4. Research Strategy*

The questionnaire was coded and entered into the computer to extract statistical results after collecting the required data and information about the study variables. The data collected from members of the study sample through the field study were processed using the Statistical Program for the Social Sciences (SPSS). Specifically, we used the following statistical methods to address the objectives of the study and evaluate its hypotheses: Honesty was measured using the self-honesty coefficient, and reliability was assessed using Cronbach's alpha coefficient.

To describe the characteristics of the study sample and show the extent to which it reflects the features of the society from which it was taken, descriptive statistics were employed. To ensure that there was no strong correlation (multicollinearity) between the independent variables, the tolerance and variance inflation factor were used, in addition to Pearson correlations, to examine the relationship between the variables. Finally, to evaluate the relationship between the study variables, we used multiple linear regression analysis.

### *4.5. Instrument Validation and Reliability Result*

The Pearson correlation coefficient was calculated for each item in relation to the corresponding field, revealing statistically significant and acceptable correlation values. As a result, none of the items were removed. The pilot phase involved designing and testing the questionnaire and procedures to ensure that the target audience comprehended the response options and could answer the questions meaningfully, as intended by the researcher [36]. According to Sudman [37], 20 to 50 cases are generally sufficient to identify major issues in the questionnaire. In this research, the questionnaire was tested with a sample of 10 children in Jordan. It is important that respondents in pilot studies closely resemble those in the main study. The experimental study produced acceptable reliability results, validated through the Cronbach's Alpha test [38]. The validity and reliability of the questionnaire were confirmed by applying Cronbach's alpha coefficient, as detailed in Table 1.

Cronbach's Alpha was used to assess the reliability of the research instrument, while the square root of the reliability coefficient was applied to measure validity. The Cronbach's Alpha values for individual questionnaire variables ranged from 62% to 86%, and the corresponding self-validity coefficients ranged from 79% to 93%. The overall Cronbach's Alpha for the entire questionnaire was 91%, with a self-validity coefficient of 95%. These values exceed the minimum acceptable threshold of 60%, which is standard in social and educational studies.

**Table 1.**
Validity and reliability of Cronbach's alpha coefficient.

| Variables | Number of items | Cronbach's alpha | Coefficient of self-validity |
|---|---|---|---|
| Knowledge of password management | 6 | 0.69 | 0.83 |
| Knowledge of social network platforms | 4 | 0.63 | 0.79 |
| Self-perception of cybersecurity awareness | 5 | 0.62 | 0.79 |
| Knowledge of legal issues related to cybersecurity | 5 | 0.86 | 0.93 |
| Cybersecurity education | 4 | 0.78 | 0.88 |
| Awareness | 5 | 0.72 | 0.85 |
| Cronbach's alpha: Values of 0.70 or higher are considered acceptable. | | | |
| Coefficient of self-validity: Values ranging from 0.60 to 0.90 are typical for satisfactory reliability. | | | |

*4.6. Questionnaire Scale*

A five-point Likert scale was employed to lower the "level of frustration among respondents" while also raising response rates and quality [38]. The interviewer can easily read the entire scale description when using a five-point scale (1 being "strongly disagree," 2 being "disagree," etc.). Dawes [39] illustrates that, as shown in Table 2, the scale represents (5, 4, 3, 2, 1) in that order: Neutral, Strongly Disagree, Disagree, Strongly Agree, Agree.

**Table 2.**
Example for Likert five-point scale.

| 3.1.1.2 Self-perception of cybersecurity awareness | | | | | |
|---|---|---|---|---|---|
| | **Strongly agree** | **Agree** | **Not sure** | **Disagree** | **Strongly disagree** |
| I have to identify a phishing email or social engineering attack | | | | | |

In light of the aforementioned, the study's arithmetic average values will be discussed in the order listed below: three.

**Table 3.**
Responses of the sample members.

| The value of the arithmetic mean | Response standard |
|---|---|
| From 1.00 - 2.33 | Low |
| 2.34 - 3.67 | Average |
| From 3.68-5.00 | High |

## 5. Results and Discussion

Children's current awareness was assessed, knowledge gaps were identified, and variables influencing their awareness were examined. Data collection was conducted using study tools, followed by data processing with a statistical program to produce the results. Hypotheses were tested using regression analysis to achieve the study's objectives, answer its questions, and validate the hypotheses. The outcomes of the hypothesis testing are discussed, highlighting the findings and their implications.

*5.1. Research Distribution*

Basic demographic data about respondents were collected in the first part of the questionnaire. These characteristics include age, gender, education level, school affiliation, children's smart device usage habits, favorite apps, and online shopping habits. Among the sample, male participants constituted 70.1%, while female participants constituted 29.9%. Figure 2: Age Distribution of the Children shows.

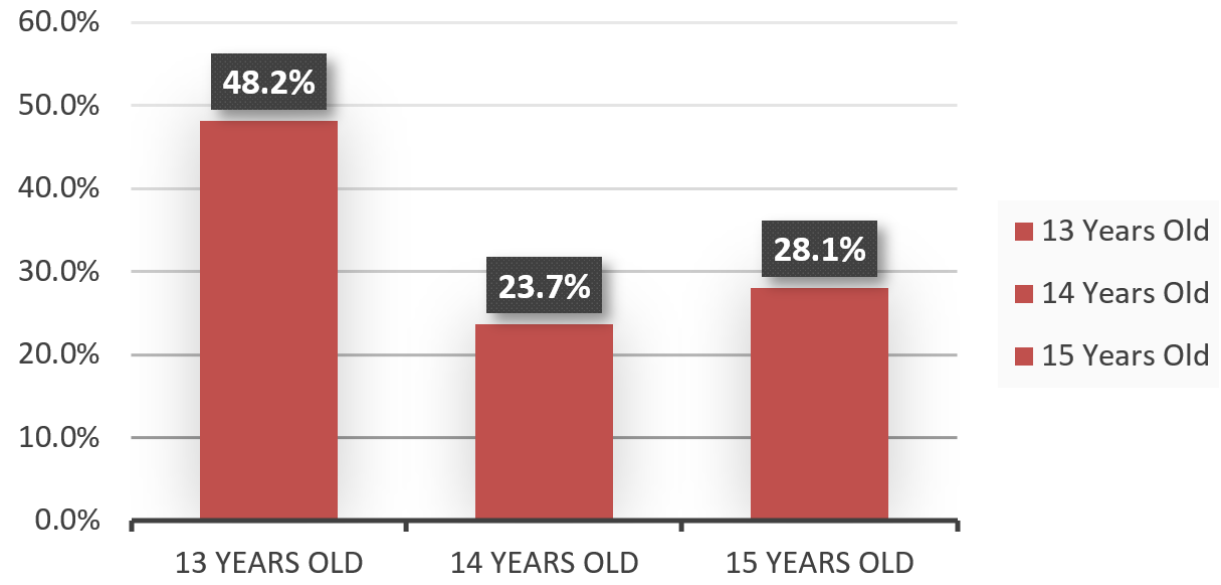


**Figure 2.**
Age distribution of the children.

The age distribution of the children in the research is shown in the image above, where approximately half of the sample is 13 years old, and the rest of the children are between 14 and 15 years old.

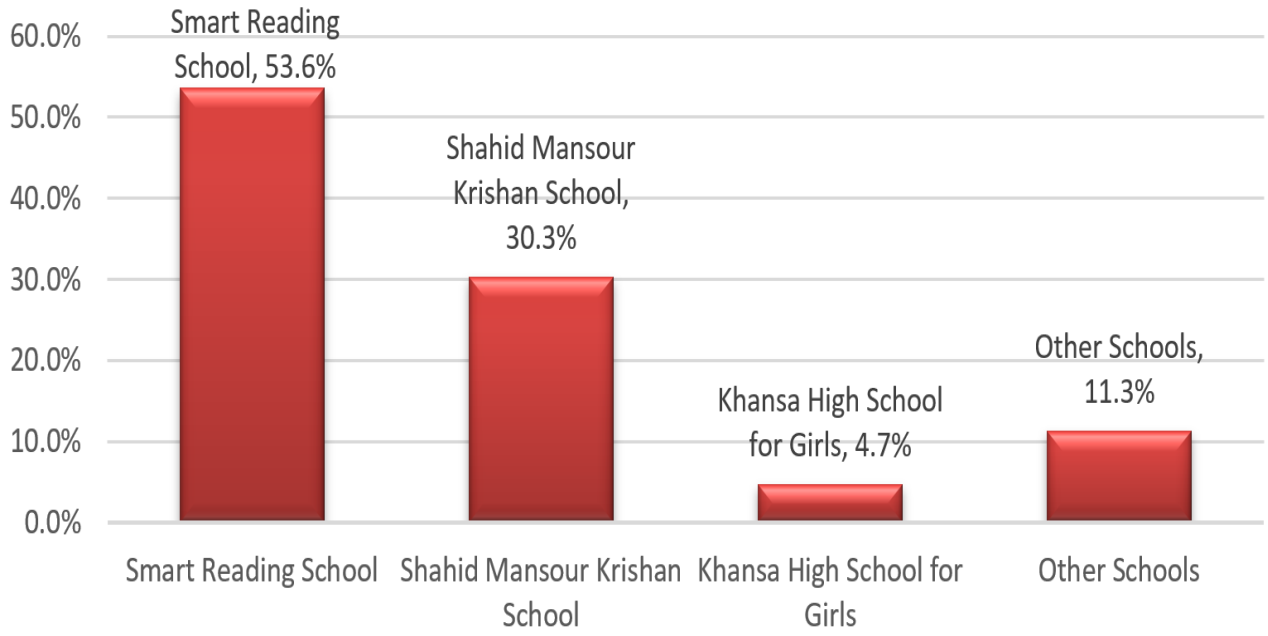


**Figure 3.**
School affiliation.

Children who participated in the survey belong to different schools. Among the schools, the Smart Reading School in Amman contributed the most data at 53.6%. The Martyr Mansour Krishan School in Amman also came in second place in terms of contribution, providing more than 30% of the questionnaire.

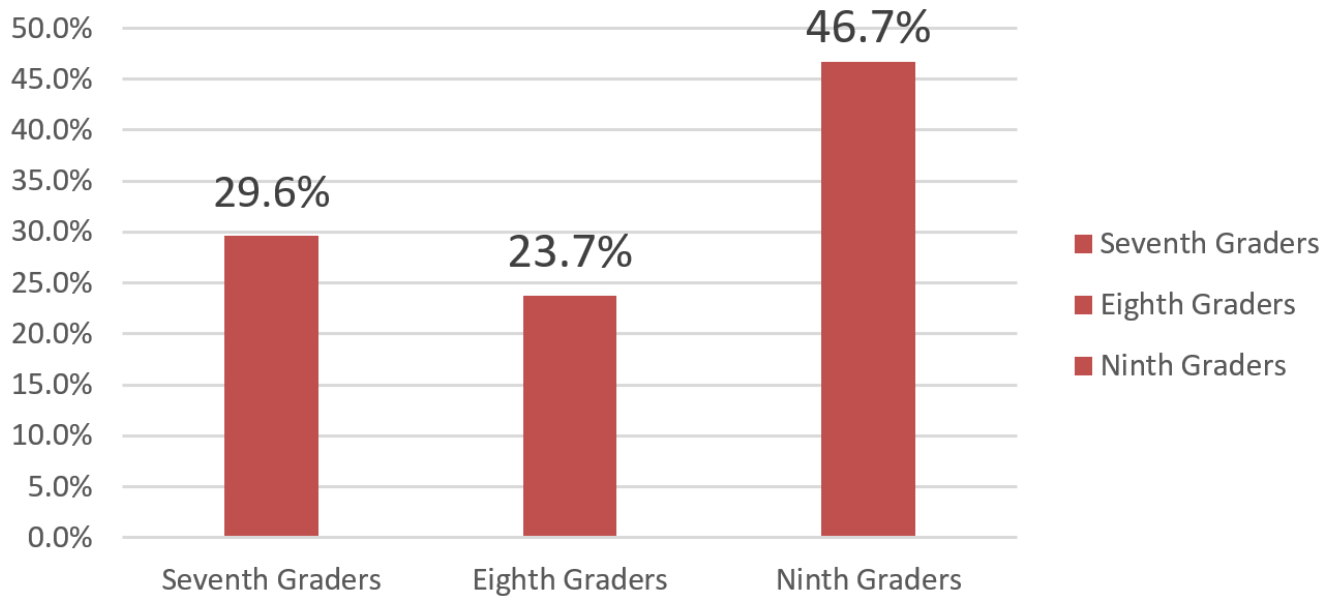


**Figure 4.**
Grade distribution.

The age distribution displayed in the previous figure suggests that nearly half of the children in the study should be in the ninth grade; however, it is possible that some of the children are in grades that do not correspond to their expected ages. The grade distribution of the study's participants is depicted in the figure above.

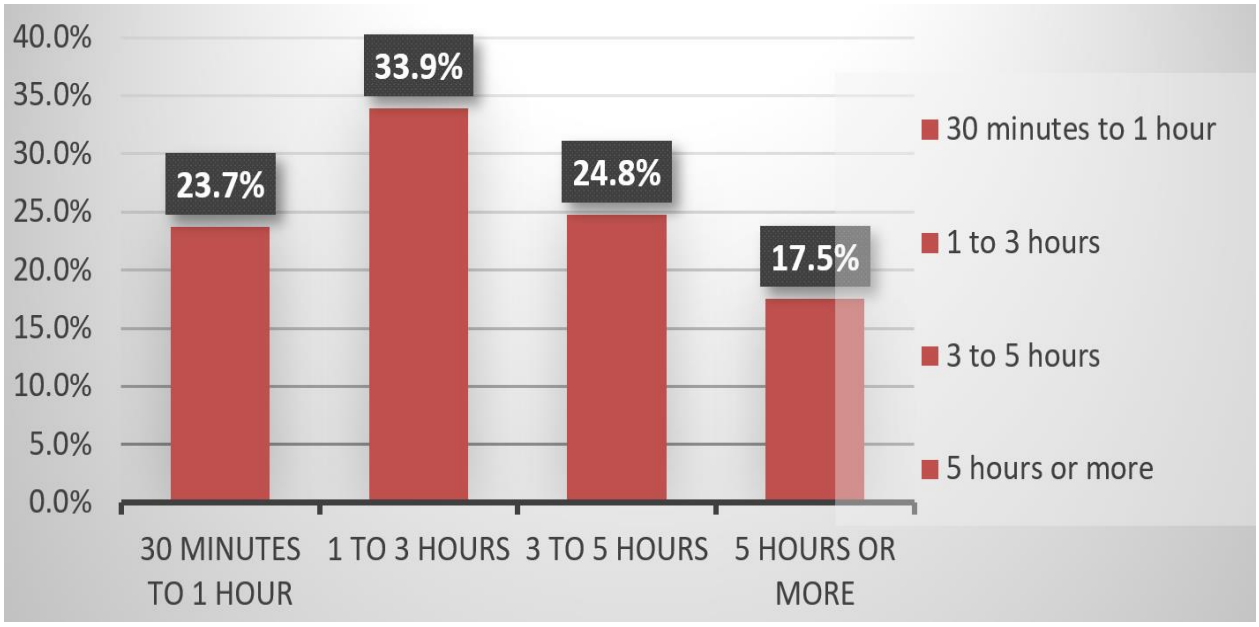


**Figure 5.**
Daily Internet Usage time.

It should be noted that while the majority of the sample reported that they use the Internet for one to three hours per day, approximately 25% of the children surveyed reported that they use the Internet for three to five hours per day. Although research on cybersecurity issues makes it reasonable to consider a child's online time, the results do not reflect the total time children spend in front of a screen.

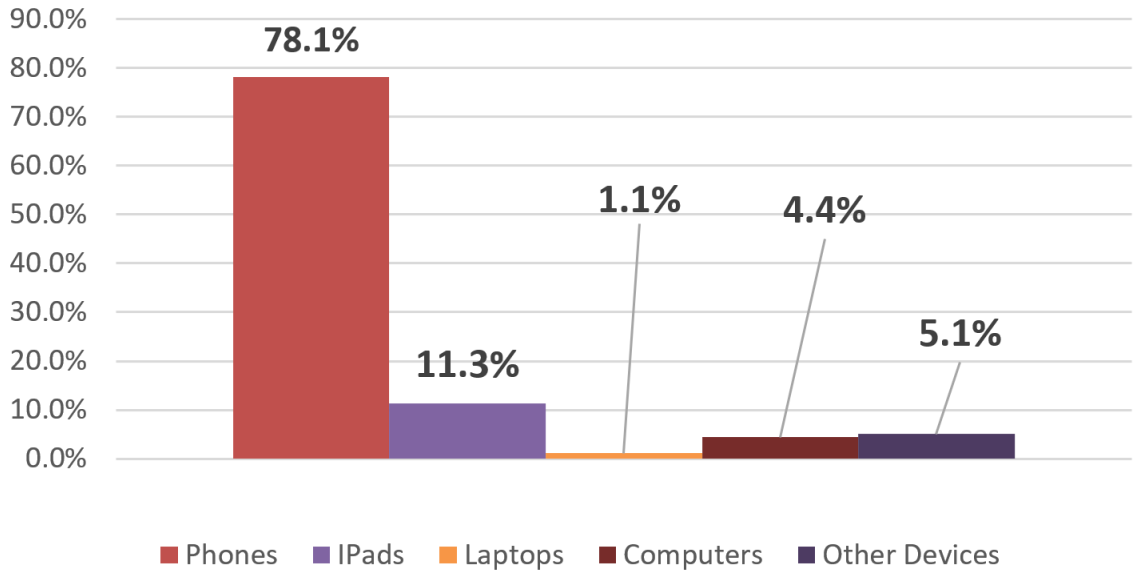


**Figure 6.**
Smart device usage.

As could be anticipated from kids their age, smartphones accounted for more than 78% of all device usage, followed by iPads (11.3%), laptops and PCs (about 5.5%), and other smart devices (the remaining 5% of the samples).

*5.2. Hypothesis Testing*

In the examination of the interrelationship and the impact of the variables on cybersecurity awareness, the study adopted multivariate regression analysis. The Pearson correlation coefficient is assumed to take values from -1 to 1 and specifies the strength and direction of relationships between pairs of variables. A value of -1 indicates a perfect negative correlation, 1 indicates a perfect positive correlation, while 0 shows no correlation. The associated p-values, which indicate statistical significance, are significant if less than 0.05, demonstrating that the relationships are not due to chance. These results were sufficient to note that all the variables were correlated with each other through a strong positive linear relationship, as they provided positive Pearson correlation coefficients. An increase in one variable corresponded to an increase in another, signifying that an increase in such variables within the questionnaires can be used to enhance cybersecurity skill outcomes. All p-values are below 0.01, which is very significant statistically. The multiple regression analysis of the predictors on cybersecurity awareness yielded statistical significance in the model. A p-value of less than 0.001, combined with a significantly high F-statistic equal to 111.303, confirms the relevance of the predictors indicated within the model. The adjusted $R^2$ was found to be 0.675, indicating that 67.5% of cybersecurity awareness would be explained by independent variables, showing a good fit for the model. The key findings were that cybersecurity knowledge received the highest positive Pearson coefficient at 0.605, followed by cybersecurity education at 0.357, which evidently pointed out large effects on cybersecurity awareness. The regression model attested to the importance of predictors like knowledge of password management, self-perception of cybersecurity awareness, knowledge of social network platforms, and cybersecurity education in making predictions toward cybersecurity awareness. It was also reflected that the knowledge associated with password handling and securing social network platforms had a positive influence on children's cybersecurity awareness because these two variables explained the variations in their cybersecurity awareness. The adjusted $R^2$ is 0.298, showing a moderate level of variance explained by cybersecurity awareness through the predictors. More specific regression results further pinpoint the significant positive effects of self-perception of cybersecurity awareness, cybersecurity education, and knowledge of legal issues related to cybersecurity on children's level of awareness. The statistical significance (p-value = 0.000) of these factors emphasized the major importance of enhancing the awareness and protection of children against cyber threats.

**Table 4.**
Results of simple regression analysis of the cybersecurity awareness.

| Hypothesis | R | $R^2$ | Unstandardized coefficients | t | F Stat | SIG | Results | (Constant) | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | | | P value | | B | T | SIG |
| H1 | 0.421 | 0.175 | 0.523 | 7.664 | 58.741 | 0.000* | Positive | 1.777 | 7.035 | 0.000 |
| H2 | 0.541 | 0.29 | 0.547 | 10.606 | 112.491 | 0.000* | Positive | 1.845 | 10.398 | 0.000 |
| H3 | 0.717 | 0.512 | 0.821 | 16.952 | 287.387 | 0.000* | Positive | 0.614 | 3.338 | 0.001 |
| H4 | 0.414 | 0.168 | 0.493 | 7.502 | 56.277 | 0.000* | Positive | 2.072 | 9.463 | 0.000 |
| H5 | 0.488 | 0.235 | 0.473 | 9.220 | 85.015 | 0.000* | Positive | 1.945 | 10.109 | 0.000 |

**Note:** *p < 0.001: Strong statistical significance.
**p < 0.01: Moderate statistical significance.
**p < 0.05: Weak statistical significance.

*5.3. Results Discussion*

Several conclusions on the factors giving rise to students' cybersecurity awareness emerged from the regression analysis. The maximum influences were noted in the spheres of passwords and cybersecurity, as well as the awareness of laws and cybersecurity education, while the influence of social networks' knowledge was lower. Out of the five factors, password management knowledge was considered the most important determinant of awareness ($\beta = 0.523$, $p < 0.01$). This is in accordance with the previous studies by Lee and Choong [5], which noted that the proper management of passwords reduces the cyber-attacks experienced by students. Similarly, learners with good password knowledge will not encounter various internet dangers, as identified by Alharbi and Tassaddiq [25]. This regularity underlines the need to incorporate password management into the training aspect of cybersecurity education for students to foster good practices. Another research that also yielded positive findings was the impact of cybersecurity education on students' awareness, whereby the coefficient was equal to 0.493 and the significance was < 0.01. This is in agreement with Chandarman and Van Niekerk [2], as they mentioned that teaching cybersecurity issues in the school curriculum contributes greatly to the impartation of knowledge concerning secure conduct on the World Wide Web. [26] also emphasized the need for simulation and role-playing as some of the important and effective techniques in training and teaching practice.

On the other hand, social network knowledge had no statistically significant value ($p > 0.05$) and was in contrast to Herath, et al. [6]. Sarker, et al. [7] analyzed social network knowledge and showed it to have a high correlation with total cybersecurity awareness. As for the possible reasons that explain such specific results, it is necessary to include the fact that modern generations, in fact, students, do not have profound knowledge of privacy settings and safety measures. This implies that although students are very keen users of social media networks, they often lack adequate knowledge on how to safeguard themselves. Further research could inquire whether a more individual approach, in which clients are instructed on certain privacy settings, yields a different result. Legal awareness ($\beta = 0.473$, $p < 0.01$) was another significant factor that agreed with the study conducted by Alharbi and Tassaddiq [25] on the legal implications of online behavior. They should also be taught about legally relevant matters such as cyberbullying, privacy infringements, and sharing personal data with others. Taken together, these results show that there is broad awareness of topics including password management and cybersecurity training, but a need to further improve social network awareness in the training domain.

In the subsequent section, findings are made regarding the work's research question: 'In what ways do password management, social network knowledge, cybersecurity education, and legal awareness contribute to the students of the age group 13-15 years with respect to cybersecurity awareness?' From the results of the regression analysis, password management, cybersecurity education, and legal awareness demonstrated a considerable impact, while the influence of social network knowledge appeared relatively small.

This research highlights the vital connection between children's understanding of cybersecurity and their real-world ability to protect themselves online. By exploring the relationship between knowledge of Password Management, Knowledge of Social Network Platforms, Knowledge of Legal Issues Related to Cybersecurity, Althunibat, et al. [40]; Althunibat, et al. [41]; Althunibat, et al. [42]; Alnuhait, et al. [43]; Althunibat [44] and Althunibat, et al. [45], self-perception, and Cybersecurity Education, the findings emphasize the need for age-appropriate and specialized educational programs. Building cybersecurity knowledge in schools turns out to be essential, yet reinforcing both secure online practices and self-assurance needs more attention for children to properly handle online threats. Children possess greater success in safeguarding their online safety when they have better self-knowledge and cybersecurity awareness. Research conducted previously demonstrated a strong correlation between higher cybersecurity awareness and better online protection skills. Lamond, et al. [26]; AlRifaee, et al. [46]; Awaji, et al. [47] and Althunibat, et al. [48] found that children who have knowledge about cybersecurity practice better security measures in order to protect their digital safety. The experimental findings validate the hypothesis, demonstrating that cybersecurity principles directly improve practical abilities. Self-perception plays a crucial role in forming their behavior patterns when they operate in digital environments [49-51]. Children who view themselves as knowledgeable in cybersecurity take better precautions by making smart choices during potential internet danger situations. Students require both technical cybersecurity instruction and the development of competency and confidence in these practices simultaneously.

The varying cybersecurity knowledge between different age segments identifies inadequacies in present-day educational practices. A standardized learning approach does not deliver effective results because children who differ in developmental levels have diverse learning abilities. The need exists for customized education programs to approach cybersecurity knowledge differently, as they will lead to a complete understanding across all age groups. Results show that continuous education efforts for maintaining and growing Cybersecurity Awareness are necessary for the future. The fast development pace of cyber threats makes it doubtful that one educational intervention will provide adequate protection. Children need continuous adaptive training to remain prepared for new digital world threats that emerge in their online environments. The following are some ideas for improving kids' cybersecurity abilities in an enjoyable and practical way: To address the issues identified, several actions can be taken. The educational materials must be customized for different student ages to address their current developmental characteristics and learning abilities. Strategic approaches will create a firm cybersecurity base for children to grasp security threats and develop suitable risk mitigation plans. Current cybersecurity threats continue to develop, where a singular educational effort won't suffice. Therefore, children need regular updates in their training sessions to maintain preparedness for digital risks that change frequently.

Additional password security through eye scan implementation helps protect systems from shared passwords and unauthorized users. The technique presents a workable safeguard for child account protection. Moreover, integrating interactive tools like games into educational programs can be highly effective, as games are used in teaching methods [52-

54]. Games that model real-life situations exposing personal information risks enable children to grasp the outcomes, together with explicit warning messages and details.

The inclusion of videos featuring cybersecurity specialists discussing online safety dangers and its essentiality represents a crucial part of educational programs that offer interactive learning resources for children. The framework of cybersecurity education requires equal attention to the existing legal systems that protect child privacy in educational platforms. Children need laws to protect their privacy, particularly through the use of educational platforms. Additionally, such initiatives benefit from authorized educational policies that guarantee standard implementation and structured guiding principles for continuous cybersecurity education in schools.

## 6. Conclusions and Future Work

This study introduced a novel cybersecurity awareness model for children, addressing a significant gap in previous research. The results proved that password management, cybersecurity education and training, and legal knowledge boost students' cybersecurity knowledge, although not as much as social network knowledge. It emphasizes the need for designing and incorporating timely and relevant cybersecurity education in schools.

More rigorous research could be conducted to incorporate additional parameters into the model or to apply it to other age groups. Further studies on policies should be undertaken to investigate how national and international policies can enhance the approach to making cybersecurity education a standard at a much wider level.

## References


[1] A. A. Al Shamsi, "Effectiveness of cyber security awareness program for young children: A case study in UAE," *International Journal of Information Technology and Language Studies,* vol. 3, no. 2, pp. 8-29, 2019.

[2] R. Chandarman and B. Van Niekerk, "Students' cybersecurity awareness at a private tertiary educational institution," *The African Journal of Information and Communication,* vol. 20, pp. 133-155, 2017.

[3] S. Parimalam, I. F. Kasmin, Z. M. Z. Abidin, and H. Vasudavan, "Cybersecurity awareness among teenagers and children using self-learning system," *International Journal of Data Science and Advanced Analytics,* vol. 4, pp. 131-138, 2022. https://doi.org/10.69511/ijdsaa.v4i0.154

[4] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?," *arXiv preprint arXiv:1901.02672,* 2019.

[5] P. Y. Lee and Y. Y. Choong, "Human generated passwords–the impacts of password requirements and presentation styles," in *In Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings 3 (pp. 83-94). Springer International Publishing,* 2015.

[6] T. B. G. Herath, P. Khanna, and M. Ahmed, "Cybersecurity practices for social media users: A systematic literature review," *Journal of Cybersecurity and Privacy,* vol. 2, no. 1, pp. 1–18, 2022. https://doi.org/10.3390/jcp2010001

[7] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: An overview from machine learning perspective," *Journal of Big Data,* vol. 7, pp. 1-29, 2020. https://doi.org/10.1186/s40537-020-00318-5

[8] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *International Journal of Child-Computer Interaction,* vol. 30, p. 100343, 2021. https://doi.org/10.1016/j.ijcci.2021.100343

[9] H. De Bruijn and M. Janssen, "Building cybersecurity awareness: The need for evidence-based framing strategies," *Government Information Quarterly,* vol. 34, no. 1, pp. 1-7, 2017. https://doi.org/10.1016/j.giq.2017.02.007

[10] E. Amankwa, "Relevance of cybersecurity education at pedagogy levels in schools," *Journal of Information Security,* vol. 12, no. 4, pp. 233-249, 2021. https://doi.org/10.4236/jis.2021.124013

[11] S. Chaudhary, V. Gkioulos, and S. Katsikas, "Developing metrics to assess the effectiveness of cybersecurity awareness program," *Journal of Cybersecurity,* vol. 8, no. 1, p. tyac006, 2022. https://doi.org/10.1093/cybsec/tyac006

[12] J. C. Read and P. Markopoulos, "Child–computer interaction," *International Journal of Child-Computer Interaction,* vol. 1, no. 1, pp. 2-6, 2013. https://doi.org/10.1016/j.ijcci.2012.09.001

[13] J. Smith, "Imparting digital literacy and cybersecurity awareness to young learners," *Journal of Educational Technology,* vol. 14, no. 2, pp. 87–101, 2018.

[14] L. Pangrazio and N. Selwyn, "My data, my bad...' young people's personal data understandings and (counter) practices," in *In Proceedings of the 8th International Conference on Social Media & Society (pp. 1-5)*, 2017.

[15] S. Livingstone, M. Stoilova, and R. Nandagiri, "Conceptualising privacy online: What do, and what should, children understand?," *Parenting for a Digital Future,* pp. 1-4, 2018.

[16] Y. Y. Choong, "A cognitive-behavioral framework of user password management lifecycle," presented at the In Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 2 (pp. 127-137). Springer International Publishing, 2014.

[17] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Draft nist special publication 800-63-3 digital identity guidelines national institute of standards and technology." Los Altos, CA: NIST Special Publication, 2017, pp. 800–63B.

[18] Nemours KidsHealth, "Online safety," Retrieved: https://kidshealth.org/en/teens/internet-safety.html. 2021.

[19] Government of British Columbia, "Online safety," Retrieved: https://www2.gov.bc.ca/gov/content/erase/online-safety. 2021.

[20] A. Smith, "Where teens seek online privacy advice," pew research center," http://www.pewinternet.org/2013/08/15/where-teens-seek-online-privacy-advice/, 2013.

[21] S. Al-Janabi and I. Al-Shourbaji, "A study of cyber security awareness in educational environment in the middle east," *Journal of Information & Knowledge Management,* vol. 15, no. 01, p. 1650007, 2016. https://doi.org/10.1142/s0219649216500076

[22] W. C. H. Hong, C. Chi, J. Liu, Y. Zhang, V. N.-L. Lei, and X. Xu, "The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates," *Education and Information Technologies,* vol. 28, no. 1, pp. 439-470, 2023. https://doi.org/10.1007/s10639-022-11121-5

[23] M. Antunes, C. Silva, and F. Marques, "An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context," *Applied Sciences,* vol. 11, no. 23, p. 11269, 2021. https://doi.org/10.3390/app112311269

[24] D. Reddy and V. Rao, "Cybersecurity awareness: The moderating role in the relationship between cybersecurity awareness and compliance," in *In Proc. Amer. Conf. Inf. Syst*, 2016, pp. 1–5.
[25] T. Alharbi and A. Tassaddiq, "Assessment of cybersecurity awareness among students of Majmaah University," *Big Data and Cognitive Computing*, vol. 5, no. 2, p. 23, 2021. https://doi.org/10.3390/bdcc5020023
[26] M. Lamond, K. Renaud, L. Wood, and S. Prior, "SOK: Young children's cybersecurity knowledge, skills & practice: A systematic literature review," in *In Proceedings of the 2022 European Symposium on Usable Security (pp. 14-27)*, 2022.
[27] Y. Ma and N. W. Twyman, "Cybersecurity: Personal information and password setup," *Association for Information Systems*, vol. 20, pp. 1–6, 2018.
[28] P. K. Sari and A. Prasetio, "Knowledge sharing and electronic word of mouth to promote information security awareness in social network site," presented at the In 2017 International Workshop on Big Data and Information Security (IWBIS) (pp. 113-117). IEEE, 2017.
[29] K. S. Crandall, J. A. McDonald, and J. A. McDonald, "High school students' perceptions of cybersecurity: An explanatory case study," *Issues in Information Systems*, vol. 20, no. 3, pp. 74–82, 2019. https://doi.org/10.48009/3_iis_2019_74-82
[30] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, "Cybersecurity knowledge and skills taught in capture the flag challenges," *Computers & Security*, vol. 102, p. 102154, 2021. https://doi.org/10.1016/j.cose.2020.102124
[31] C. Catalano, A. Pagano, A. Piccinno, and A. Stamerra, "Cartoons to improve cyber security education: Snow white in browser in the middle," in *In Proceedings of the 9th International Symposium on End-User Development (pp. 3–11). https://ceur-ws.org/Vol-3408/short-s3-11.pdf*, 2023.
[32] O. Olasehinde-Williams and A. O. Dunmade, "Cyber ethics and digital citizenship," 2023.
[33] Z. Zulkifli, N. N. A. Molok, N. H. Abd Rahim, and S. Talib, "Cyber security awareness among secondary school students in Malaysia," *Journal of Information Systems and Digital Technologies*, vol. 2, no. 2, pp. 28-41, 2020. https://doi.org/10.31436/jisdt.v2i2.151
[34] P. T. Mai and A. Tick, "Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam," *Acta Polytechnica Hungarica*, vol. 18, no. 8, pp. 67-89, 2021. https://doi.org/10.12700/aph.18.8.2021.8.4
[35] M. A. Alqahtani, "Cybersecurity awareness based on software and e-mail security with statistical analysis," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, p. 6775980, 2022. https://doi.org/10.1155/2022/6775980
[36] S. Presser *et al.*, "Methods for testing and evaluating survey questions," *Methods for Testing and Evaluating Survey Questionnaires*, pp. 1-22, 2004. https://doi.org/10.1093/poq/nfh008
[37] S. Sudman, "Applied sampling,"in handbook of survey research, P. Rossi, J. Wright, and A. Anderson, Eds." New York, NY, USA: Academic Press, 1983, pp. 145–149.
[38] S. B. Sachdev and H. V. Verma, "Relative importance of service quality dimensions: A multisectoral study," *Journal of Services Research*, vol. 4, no. 1, p. 93, 2004.
[39] J. Dawes, "Do data characteristics change according to the number of scale points used? An experiment using 5-point, 7-point and 10-point scales," *International Journal of Market Research*, vol. 50, no. 1, pp. 61-104, 2008. https://doi.org/10.1177/147078530805000106
[40] A. Althunibat, A. Alhalaybeh, A. Hanif, K. K. Habashneh, and M. AlRifaee, "Determining the factors affecting metaverse adoption in higher learning institutions," *International Journal of Information and Education Technology*, vol. 14, no. 11, pp. 1554–1565, 2024. https://doi.org/10.18178/IJIET.2024.14.11.2186
[41] A. Althunibat *et al.*, "Detecting ambiguities in requirement documents written in arabic using machine learning algorithms," *International Journal of Cloud Applications and Computing*, vol. 14, no. 1, pp. 1-19, 2024. https://doi.org/10.4018/IJCAC.2024010101
[42] A. Althunibat, A. Alhalaybeh, A. Hanif, K. K. Habashneh, and M. AlRifaee, "Prediction of accessibility testing using a generalized linear model for e-government," *Journal of Infrastructure Policy Development*, vol. 8, no. 7, p. 3520, 2024. https://doi.org/10.4018/JIPD.2024070101
[43] H. Alnuhait, A. Alhalaybeh, A. Hanif, K. K. Habashneh, and M. AlRifaee, "Web application performance assessment: A study of responsiveness, throughput, and scalability," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 9, pp. 214–226, 2024. https://doi.org/10.14569/IJACSA.2024.0110928
[44] A. Althunibat, "Proposed test case generation model using fuzzy logic (TCGMFL)," *WSEAS Transactions on Computer Research*, 2024. https://doi.org/10.37394/232018.2024.12.16
[45] A. Althunibat, H. AlNuhait, S. Almanasra, M. H. Almajali, E. Aljarrah, and H. A. Al-Khawaja, "Culture and law enforcement influence on m-government adoption: An exploratory study," *Journal of Infrastructure, Policy and Development*, vol. 8, no. 5, p. 3353, 2024. https://doi.org/10.4018/JIPD.2024050101
[46] M. AlRifaee, S. Almanasra, A. Hnaif, A. Althunibat, M. Abdallah, and T. Alrawashdeh, "Adaptive segmentation for unconstrained iris recognition," *Computers materials & continua*, vol. 78, no. 2, pp. 1591-1609, 2024. https://doi.org/10.32604/cmc.2024.019123
[47] B. H. Awaji *et al.*, "Novel multiple access protocols against Q-learning-based tunnel monitoring using flying ad hoc networks," *Wireless Networks*, vol. 30, no. 2, pp. 987-1011, 2024. https://doi.org/10.1007/s11276-023-03534-y
[48] A. Althunibat, B. Alokush, S. M. Tarabieh, and R. Dawood, "Mobile government and digital economy relationship and challenges," *International Journal of Advances in Soft Computing & Its Applications*, vol. 13, no. 1, 2021. https://doi.org/10.14569/IJACSA.2020.0130101
[49] M. ALmahasnah, M. Almajali, A. Althunibat, B. Abuaisheh, F. Alqudah, and M. Ghazwi, "The role of anti-corruption legislation in sustainable development," *Journal of Infrastructure, Policy and Development*, vol. 8, no. 10, p. 5611, 2024. https://doi.org/10.4018/JIPD.2024100101
[50] A. Althunibat *et al.*, "Learning experience of students using the learning management system: User's perspective on the use of moodle in the university of Jordan," *Advances in Human-Computer Interaction*, vol. 2023, no. 1, p. 6659245, 2023. https://doi.org/10.1155/2023/6659245
[51] A. Althunibat, R. Amro, B. Hawashin, H. AlNuhait, S. Almanasra, and H. A. Al-Khawaja, "Automated classification of user requirements written in Arabic using machine learning algorithms," *Appl. Math*, vol. 17, no. 6, pp. 1155-1170, 2023. https://doi.org/10.18576/amis/170620

[52] A. Althunibat, F. Altarawneh, R. Dawood, and M. A. Almaiah, "Propose a new quality model for m-learning application in light of COVID-19," *Mobile Information Systems*, vol. 2022, no. 1, p. 3174692, 2022. https://doi.org/10.1155/2022/3174692

[53] A. Althunibat, M. Abdallah, M. A. Almaiah, N. Alabwaini, and T. A. Alrawashdeh, "An acceptance model of using mobile-government services (AMGS)," *CMES-Computer Modeling in Engineering & Sciences*, vol. 131, no. 2, pp. 865–880, 2022. https://doi.org/10.32604/cmes.2022.019123

[54] W. Alzyadat, M. Muhairat, A. Alhroob, and T. Rawashdeh, "A recruitment big data approach to interplay of the target drugs," *International Journal of Advances in Soft Computing & Its Applications*, vol. 14, no. 1, pp. 2–13, 2022. https://doi.org/10.15849/zujijasaca.220328.01