Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Bridging Knowledge and Behavior: A Mixed-Methods Study of Adolescent Cybersecurity Literacy and Its Implications for Child Protection in Jordan

Mohammed Ghallab

mo92ghallab@gmail.com

German Jordanian University

Sahar AlMakhamreh

German Jordanian University

Research Article

Keywords: Adolescents, Child Protection, Cybersecurity Literacy, Digital Threats, Social Work, Jordan

Posted Date: June 26th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9579815/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: No competing interests reported.

Abstract

The rapid digitalization of adolescents' lives has introduced unprecedented child protection challenges, yet limited research has examined cybersecurity literacy among adolescents in the Global South. This explanatory sequential mixed-methods study investigated the extent of cybersecurity literacy among Jordanian adolescents aged 14 to 17, the digital threats they encounter, and potential social work intervention models. In the quantitative phase, 625 adolescents completed a validated electronic questionnaire measuring cybersecurity knowledge and behavior. In the qualitative phase, focus group discussions and semi-structured interviews were conducted with 20 participants, including students, parents, teachers, and school counselors. Quantitative findings revealed a moderate overall level of cybersecurity literacy (M = 3.63, SD = 0.726), characterized by a significant knowledge-behavior gap: knowledge was high (M = 3.79) while behavior remained moderate (M = 3.49). The most prevalent digital threats were hacking attempts (28.1%), harmful content (23.5%), and cyberbullying (16.7%). Notably, 39.4% of adolescents had received no cybersecurity training, and only 1.3% reported threats to their schools. Regression analysis identified training as the strongest predictor of both literacy and threat reporting. Qualitative findings illuminated barriers including shame culture, fear of parental punishment, and a lack of practical skills. Grounded in Bronfenbrenner's Ecological Systems Theory and Social Construction Theory, the study proposes a storytelling-based intervention model for enhancing online resilience, offering actionable implications for child protection practice and policy.

1. Introduction

The digital revolution has fundamentally transformed the developmental landscape of childhood and adolescence. Globally, young people are among the most active users of digital technologies, with the internet serving as a primary space for socialization, education, and identity formation (World Health Organization, 2019). In Jordan, this trend is particularly pronounced; a national survey by the Ministry of Digital Economy and Entrepreneurship (2022) documented extensive internet penetration among the youth population, while Save the Children Jordan (2024) reported that children aged 10 to 17 are increasingly navigating complex digital environments with limited protective guidance. This pervasive digital engagement, while offering substantial opportunities for learning and social connection, simultaneously exposes adolescents to a spectrum of online threats, including cyberbullying, hacking, exposure to harmful content, and sexual exploitation (Laczi & Póser, 2024; Martínez et al., 2020).

The concept of cybersecurity literacy has emerged as a critical protective factor in this context. Defined as the combination of knowledge, awareness, and behaviors that enable individuals to navigate the digital environment safely (Jacobson & Idziorek, 2013; Vasileiou & Furnell, 2019), cybersecurity literacy extends beyond mere technical competence to encompass the capacity to recognize, respond to, and mitigate online risks. However, a persistent challenge documented in the literature is the knowledge-behavior gap, wherein individuals possess theoretical understanding of online safety principles yet fail to translate this knowledge into consistent protective behaviors (Branley-Bell et al., 2022; Fattah et al., 2023). This gap is particularly concerning among adolescents, whose developmental characteristics, including heightened impulsivity, susceptibility to peer influence, and evolving cognitive capacities, may render them especially vulnerable to the consequences of this disconnect (Lahti et al., 2024).

In Jordan, the intersection of rapid digitalization and limited cybersecurity education creates a pressing child protection concern. Research has documented that Jordanian adolescents face significant online risks, including cyberbullying, hacking, and online harassment, often without adequate protective mechanisms (Alshareef et al., 2024; AlSobeh et al., 2023). The development of national cybersecurity strategies, including the Jordanian Cybercrime Law No. 17 of 2023, represents a positive legislative step; however, the effective translation of these

policies into educational practice remains a significant challenge (Ghandour & Woodford, 2024). From a social work perspective, the profession's core commitment to social justice, empowerment, and the person-in-environment framework positions it uniquely to address these emerging digital threats (International Federation of Social Workers, 2014). Yet, the integration of digital competency into social work practice and child protection frameworks remains underdeveloped, particularly in the Middle Eastern context.

Despite the growing body of research on adolescent cybersecurity, critical gaps persist. There is a notable scarcity of mixed-methods research that combines the breadth of quantitative assessment with the depth of qualitative inquiry to understand both the prevalence and the lived experience of cybersecurity challenges among adolescents in the Global South (Oguine et al., 2025). Furthermore, limited research has examined the specific factors that predict cybersecurity literacy and threat-reporting behaviors among adolescents, or explored culturally appropriate intervention models grounded in social work principles. This study addresses these gaps by employing an explanatory sequential mixed-methods design guided by the following research questions:

- To what extent are adolescents in Jordan literate about cybersecurity?
- What types of digital threats are adolescents exposed to?
- What is the potential model for social work intervention with cybersecurity literacy in the field of child protection?

1.1. Cybersecurity Literacy: Conceptualization and the Knowledge-Behavior Gap

Cybersecurity literacy is a multidimensional construct that encompasses the knowledge, awareness, and behavioral competencies required for safe navigation of the digital environment (Jacobson & Idziorek, 2013; Vasileiou & Furnell, 2019). It extends beyond the narrower concept of digital literacy, which primarily concerns the ability to use digital technologies effectively (Alexander et al., 2016), to include a specific focus on the identification and mitigation of online threats. The construct comprises two interrelated dimensions: cybersecurity knowledge, which refers to the theoretical understanding of security concepts such as password management, two-factor authentication, and privacy settings; and cybersecurity behavior, which involves the practical application of this knowledge through consistent protective actions (Hoang et al., 2020; Repi & Nasution, 2024).

A central challenge in the field is the persistent knowledge-behavior gap. Research consistently demonstrates that possessing cybersecurity knowledge does not automatically translate into safe online practices. Branley-Bell et al. (2022) found significant discrepancies between what individuals know about online safety and how they actually behave online, a finding corroborated by studies across diverse populations (Fattah et al., 2023; Luic et al., 2021). Among adolescents, this gap is particularly pronounced. Blažič and Blažič (2022) documented that European high-school students demonstrated adequate theoretical knowledge of cybersecurity principles but exhibited inconsistent application of protective behaviors. Similarly, Subasi et al. (2023) reported that while adolescents may understand the importance of strong passwords and privacy settings, the actual adoption of these practices remains uneven. The implications of this gap are significant: adolescents who know the rules but do not follow them remain vulnerable to the very threats they are theoretically equipped to avoid.

1.2. Digital Threats and Their Impacts on Adolescents

The digital environment exposes adolescents to a range of threats with significant psychological and social consequences. Cyberbullying remains one of the most prevalent risks, with research documenting its association

with heightened levels of stress, anxiety, depression, and suicidal ideation (Du et al., 2024; Sulaiman & Mahfar, 2024). Perwitasari and Wuryaningsih (2022) demonstrated that cyberbullied adolescents were two to three times more likely to report suicidal thoughts, while Molero et al. (2022) confirmed through meta-analysis the strong association between cybervictimization and anxiety and depression. The social consequences are equally concerning, as cyberbullying victims often experience isolation and withdrawal from social interactions (Jaskulska et al., 2022; Onditi, 2023).

Beyond cyberbullying, online sexual exploitation represents a particularly severe threat, with victims frequently suffering from fear, anxiety, depression, and post-traumatic stress disorder (Álvarez-Guerrero et al., 2024; Lee et al., 2022). The stigma associated with such exploitation often leads to social isolation and reluctance to seek support (Lin et al., 2025; Salazar et al., 2023). Privacy violations constitute another significant concern, as adolescents who experience unauthorized sharing of personal information report increased anxiety and stress, particularly when they perceive a loss of control over their data (Corcoran et al., 2024; Laird & Hawk, 2024). Furthermore, exposure to harmful online content, including material promoting self-harm and eating disorders, has been linked to increased engagement in these behaviors among adolescents (Bednarek et al., 2024; Soldatova & Ilyukhina, 2021). Phishing scams and hacking attempts also contribute to psychological distress, undermining trust in online platforms and affecting social standing (Abroshan et al., 2021; Audrin & Blaya, 2020; Stalans et al., 2023).

1.3. Child Protection and Social Work in the Digital Age

Child protection encompasses three core elements: protecting all children from all forms of violence without discrimination, providing necessary support when there are shortcomings in child protection, and ensuring the effective participation of children in decisions affecting their rights (Wekerle, 2024). The Committee on the Rights of the Child (2021) has emphasized the protection and activation of children's rights in the digital environment, recognizing that meaningful access to digital technology enables children to enjoy their civil, political, economic, and social rights. Redefining child protection to include digital safety measures has become an urgent necessity given the emergence of new threats such as privacy violations, exposure to inappropriate content, and cyberbullying (Kovács-Szépvölgyi, 2023; Paukova, 2019). Köhler-Dauner et al. (2025) have argued for a regulated, age-tiered approach to social media access, proposing differentiated strategies based on developmental stages rather than outright bans.

Social work operates as a gateway for promoting social change and empowering individuals and communities (International Federation of Social Workers, 2014), serving as a foundational pillar for child protection through community engagement (Rakaab, 2025). In the digital age, social workers play a pivotal role in promoting the ethical use of technology, advocating for digital inclusion, and navigating the complexities of the digital environment (Storer et al., 2023). They promote digital inclusion by participating in policy initiatives and programs aimed at enhancing digital literacy among marginalized communities (Kalenda & Kowaliková, 2020; Sanders & Scanlon, 2021), and work to improve users' online safety to enable them to overcome digital threats (Lee & Lee, 2022). Segal et al. (2025) explored the use of technology by social workers in Israel, finding that while technology offers new service delivery possibilities, it also presents significant ethical challenges. Behan-Devlin (2024) highlighted that the COVID-19 pandemic accelerated the adoption of digital communication tools in children's safeguarding social work, leading to a hybrid model of practice.

Community awareness and engagement are essential components of any approach to enhancing cybersecurity knowledge and behaviors (Muller & Burrell, 2022). Interactive awareness programs have been shown to be more effective than traditional approaches (Aldawood & Skinner, 2020), and training programs hold significant potential to enhance adolescents' cybersecurity literacy through innovative approaches, including intervention mapping (Pirta-

Dreimane et al., 2022), digital content and innovative teaching techniques (Xenakis et al., 2024), and cross-disciplinary education (Ahmad et al., 2022). At the policy level, investing in social cybersecurity is recognized as an urgent priority for national security and corporate asset protection (Pratap & Giri, 2025; Santhosh & Thiyagu, 2022).

1.4. Storytelling as an Educational Intervention

Storytelling has emerged as a powerful educational intervention for promoting cybersecurity literacy among adolescents. Research consistently demonstrates that narrative-based learning enhances engagement, improves understanding of complex concepts, and has the potential for better long-term knowledge retention. Akdag and Altinay (2021) demonstrated the effectiveness of digital stories for creating safe school environments, while Andriessen et al. (2025) confirmed through a systematic review that storytelling is an effective approach for cybersecurity education across different age groups. Rikkers and Sarmah (2025) showed that story-driven gamification enhances both engagement and learning outcomes, and Weijsenfeld and Sarmah (2025) found that narrative-based serious games resulted in significantly higher user engagement compared to traditional text-based learning. Kaptan and Cakir (2025) provided further evidence for the effectiveness of narrative-based approaches in developing digital competencies.

A key theme in the literature is the importance of co-designing stories with children and adolescents to ensure cultural relevance and authenticity. Quayyum (2025) demonstrated that co-designed cybersecurity stories not only resonate more deeply with young audiences but also foster a sense of ownership and agency. The reviewed literature critiques traditional educational models that focus solely on transmitting information, arguing that in the dynamic field of cybersecurity, the goal must be to move beyond simply "being secure" to "acting securely." Storytelling and other engaging methods are better suited to fostering this behavioral change, as they allow learners to emotionally connect with the material and see the real-world consequences of online behaviors (Esfandiari et al., 2025; Sağlam et al., 2023).

1.5. The Jordanian Context

In Jordan, cybersecurity among adolescents represents a complex issue with significant social and technological implications. AlSobeh et al. (2023) found a close relationship between cybersecurity awareness and adolescents' quality of life, recommending the launch of national cybersecurity programs to educate teenagers on cyberattack risks and protection strategies. Altarawneh et al. (2025) revealed that knowledge of passwords, social networking sites, and legal aspects are key factors influencing cybersecurity awareness among middle school students, highlighting the need for structured educational programs including simulations and expert-led workshops.

Research indicates that adolescent girls are particularly vulnerable to online risks in Jordan. Alshareef et al. (2024) investigated the online risks faced by adolescent girls and found exposure to various risks including electronic violence, security risks, and social risks, with protection mechanisms that were often weak. The development of national cybersecurity strategies, such as the Jordanian Cybercrime Law, represents a positive step, but effective implementation in educational settings remains challenging. Ghandour and Woodford (2024) provided guidelines for developing cybersecurity policies in Jordanian schools, emphasizing the need for a proactive approach encompassing strategy, standards, hardware and software, and training. In the broader regional context, the literature emphasizes the urgent need for culturally relevant and comprehensive cybersecurity education programs integrated into school curricula (Alharbi et al., 2022; Alansari et al., 2026).

1.6. Theoretical Framework

This study is guided by two complementary theoretical frameworks: Bronfenbrenner's Ecological Systems Theory and Social Construction Theory. Together, these theories provide a robust foundation for understanding the complex interplay of individual, social, and cultural factors that shape adolescents' experiences with cybersecurity.

Bronfenbrenner's (1979, 1994) Ecological Systems Theory offers a comprehensive framework for understanding human development as a product of interactions between individuals and their environments across multiple nested systems: the microsystem (immediate relationships with family, school, and peers), the mesosystem (interconnections between microsystems), the exosystem (external factors that indirectly influence development), the macrosystem (cultural and societal influences), and the chronosystem (the element of time and historical events) (Gonzales, 2020; Yang & Oh, 2024). In the digital age, this theory has been adapted to account for the pervasive influence of technology. Navarro and Tudge (2023) proposed a "neo-ecological theory" introducing the concept of "virtual microsystems," while Gaitis et al. (2025) extended this framework through a "technologised neo-ecological perspective" to understand risks in extended reality environments. Patel and Quan-Haase (2024) proposed a social-ecological model that integrates digital media as a central ecological system in young people's lives.

Social Construction Theory, as articulated by Berger and Luckmann (1966), posits that understanding of reality is shaped by shared perceptions, interactions, and social processes. Payne (2021) emphasized the role of social constructivism in understanding and shaping social work practices, highlighting how social norms, values, and power dynamics define and address social issues. In the context of cybersecurity, this theory helps explain how online risks and identities are socially defined and negotiated. Austen (2009) argued that young people socially construct their own understandings of risk through peer interactions and cultural contexts, while Elvira-Zorzo and Gómez (2025) examined how adolescents construct their identities both online and offline, with online identity construction potentially leading to emotional distress.

By integrating these two frameworks, this study adopts a holistic approach to understanding adolescent cybersecurity literacy, recognizing that it is shaped by a complex interplay of individual, social, and cultural factors within both physical and virtual environments. The ecological perspective provides a multi-level lens for analyzing influences on adolescent online behavior, while the social constructionist perspective highlights the importance of understanding how adolescents themselves make sense of their digital experiences. Together, these frameworks inform the development of comprehensive and contextually appropriate interventions for promoting cybersecurity literacy and protecting children in the digital age.

2. Methods

2.1. Research Design

This study employed an explanatory sequential mixed-methods design, a robust approach that integrates quantitative and qualitative data collection and analysis in two distinct, consecutive phases (Creswell & Creswell, 2018). This design was strategically chosen to first identify the broad statistical patterns of adolescent cybersecurity literacy and then to explore the underlying reasons and contexts for those patterns in depth (Edmonds & Kennedy, 2017; Toyon, 2021). The initial, dominant phase was quantitative, focusing on gathering numerical data from a large sample to answer the primary research questions regarding the extent of cybersecurity knowledge and behaviors. This was followed by a qualitative phase designed to explain and elaborate upon the initial quantitative findings (Draucker et al., 2020).

The research was philosophically grounded in a pragmatist paradigm. Pragmatism as a worldview eschews the traditional dichotomy between quantitative and qualitative research, instead focusing on the practical consequences of research and the real-world problems being investigated (Feilzer, 2023; Gillespie et al., 2024; Kaushik & Walsh, 2019). This paradigm aligns with the study's goal of not only understanding a social phenomenon but also generating actionable knowledge to inform social work practice and child protection policy. The growing importance of mixed-methods research in health and social sciences further supports this methodological choice (Wasti et al., 2022).

2.2. Participants and Sampling

The study population comprised adolescents aged 14–17, along with their parents, teachers, and school counselors in Jordan. The sampling procedures for both phases were designed to ensure a comprehensive and diverse representation of the target population.

2.2.1. Quantitative Phase

The quantitative phase involved a sample of 625 adolescents. A multi-stage stratified random sampling technique was utilized, with stratification based on two key variables: geographical area (urban, rural, desert/Badia, and refugee camp) and school type (public, private, and international). This stratification ensured that the sample reflected the diversity of the adolescent population within the country. The recruitment of participants was facilitated through the Madrasati initiative, a well-established non-governmental organization that partners with a wide network of schools across Jordan. The sample size was determined based on Krejcie and Morgan's (1970) guidelines for determining sample size for research activities.

2.2.2. Qualitative Phase

Following the quantitative phase, a purposive sampling strategy was employed to select 20 participants for the qualitative component (Campbell et al., 2020). The qualitative sample was composed of three distinct groups: a focus group with seven parents, a separate focus group with six students, and individual semi-structured interviews with seven teachers and school counselors (Krueger & Casey, 2014). Participants were selected from the same schools that participated in the quantitative phase, allowing for a direct link between the two datasets. This purposeful selection was crucial for a deep exploration of the themes that emerged from the initial quantitative analysis.

Table 1
Participants in Qualitative Phase

Group	Methods	# of participants
Parents	Focus Group Discussion	7
Students	Focus Group Discussion	6
Teachers & Counselors	Semi-structured interviews	7
Total		20

2.3. Instruments

2.3.1. Quantitative Instrument

The primary data collection tool for the quantitative phase was a self-administered electronic questionnaire developed following an extensive review of the relevant academic literature and existing scales on cybersecurity

literacy. The questionnaire was administered using Microsoft Forms. The instrument was structured into two main sections. The first section gathered demographic data, including age, gender, geographical area, school type, and time spent online daily. The second section contained 14 items designed to address the research questions. It featured eleven items using a five-point Likert scale, ranging from 1 (Strongly Disagree) to 5 (Strongly Agree), to measure cybersecurity knowledge and behavior, one multiple-choice item to identify exposure to various online threats, and two single-choice items related to reporting behaviors and training received.

Content validity was established by having the questionnaire reviewed by a panel of academic experts in social work, cybersecurity, and education. The reliability of the instrument was assessed using Cronbach's alpha. The analysis yielded satisfactory results, with an alpha coefficient of 0.732 for the knowledge subscale, 0.709 for the behavior subscale, and 0.817 for the overall cybersecurity literacy scale, all exceeding the 0.70 threshold indicating good internal consistency (Field, 2018; Zohrabi, 2013).

Table 2
Reliability of the Questionnaire

Dimensions	Cronbach's Alpha	No. of items
Cybersecurity Knowledge	0.732	5
Cybersecurity Behavior	0.709	6
Overall Cybersecurity Literacy	0.817	11
Accordingly, the relative importance level of the items was determined according to the following formula:		

$$Relative\ importance = (Higher\ limit - lower\ limit) \,/\, (Number\ of\ Intervals) = (5-1) \,/\, (3) = 1.33$$

Table 3
Relative importance level

Relative importance level	Mean
Low	1– Lower than 2.33
Moderate	2.33 – lower than 3.66
High	3.66-5

2.3.2. Qualitative Instruments

For the qualitative phase, data were gathered through semi-structured interviews and focus group discussions (FGDs), all conducted remotely via Microsoft Teams (Ruslin et al., 2022). A semi-structured interview protocol was used for the individual interviews with teachers and school counselors, including open-ended questions designed to explore their professional experiences and perspectives on adolescent online behavior. Two separate FGD protocols were developed: one for students and another for parents. The student FGD protocol aimed to create a peer-to-peer environment where adolescents could comfortably share their experiences with online risks. The parent FGD protocol focused on understanding their concerns about their children's online safety and the strategies they use to protect them.

2.4. Data Analysis

2.4.1. Quantitative Data Analysis

The quantitative data from the 625 completed questionnaires were analyzed using IBM SPSS Statistics, Version 23. The analysis proceeded through three stages. First, descriptive statistics (frequencies, means, and standard deviations) were calculated to summarize the demographic characteristics and key variables. Second, inferential statistics, including independent samples t-tests and one-way analysis of variance (ANOVA), were employed to examine differences in cybersecurity literacy across demographic groups, with a significance level set at $\alpha = .05$. Post-hoc comparisons were conducted using Tukey's and Games-Howell tests where appropriate. Third, multiple linear regression analyses were performed to identify the predictors of cybersecurity literacy, threat exposure, and reporting behavior (Field, 2018).

2.4.2. Qualitative Data Analysis

The qualitative data from the interviews and FGDs were transcribed verbatim and analyzed using reflexive thematic analysis, following the six-phase approach developed by Braun and Clarke (2006). This method was chosen for its flexibility and its emphasis on the researcher's active role in interpreting the data to identify and analyze patterns of meaning relevant to the research questions (Byrne, 2022). The six phases included: (1) familiarization with the data, (2) generating initial codes, (3) searching for themes, (4) reviewing themes, (5) defining and naming themes, and (6) producing the report.

2.4.3. Mixed-Methods Integration

The final stage of the analysis involved the integration of the quantitative and qualitative findings at the interpretation level. The qualitative themes were used to explain, elaborate on, and provide context for the statistical results from the quantitative phase. The primary integration strategy was connecting, where the quantitative results directly informed the qualitative sampling and inquiry (Draucker et al., 2020).

2.5. Ethical Considerations

The highest ethical standards were maintained throughout all stages of this research. The study protocol received full ethical approval from the relevant institutional review board prior to the commencement of any data collection (Sadzaglishvili et al., 2021; The Society for Adolescent Health and Medicine, 2025). A two-tiered consent process was implemented for adolescent participants: written informed consent was obtained from their parents or legal guardians, and written assent was obtained from the adolescents themselves (U.S. Department of Health & Human Services, n.d.). All adult participants provided their own written informed consent. Participation was entirely voluntary, and participants were informed of their right to withdraw at any time without penalty. The quantitative data were collected anonymously, and for the qualitative data, all identifying information was removed from transcripts and replaced with pseudonyms. Audio recordings and transcripts were stored on a password-protected, encrypted hard drive accessible only to the primary researcher.

3. Results

This section presents the findings from the explanatory sequential mixed-methods study. The quantitative results from the survey (N = 625) are presented first, followed by the qualitative findings from the focus groups and interviews (N = 20).

3.1. Quantitative Findings

3.1.1. Participant Demographics

The quantitative sample consisted of 625 adolescents aged 14 to 17. The demographic profile is summarized in Table 3.

Table 3
Demographic Characteristics of Participants in the Quantitative Phase

Characteristic	Categories	Frequency	Percent %
Age	14 years	178	28.5
	15 years	199	31.8
	16 years	160	25.6
	17 years	88	14.1
	Total	625	100
Gender	Male	301	48.2
	Female	324	51.8
	Total	625	100
Area	Rural Area	155	24.8
	Urban Area	345	55.2
	Desert Area (Badia)	75	12
	Camp	50	8
	Total	625	100
School type	Public/Government	449	71.8
	Private/National	126	20.2
	International	50	8
	Total	625	100
Time spent online	Less than 1 hour	108	17.3
	About 1–3 hours	259	41.4
	About 4–6 hours	159	25.4
	More than 6 hours	99	15.8
	Total	625	100

The data on time spent online indicates a high level of digital engagement, with 82.6% of adolescents spending between one and more than six hours online daily. This high exposure underscores the centrality of the digital environment in the daily lives of these adolescents, making the study of cybersecurity literacy an urgent child protection concern.

3.1.2. Cybersecurity Literacy Levels

Overall, adolescents demonstrated a moderate level of cybersecurity literacy (M = 3.63, SD = 0.726). A notable gap emerged when literacy was disaggregated into its core components. Participants reported a high level of

cybersecurity knowledge (M = 3.79, SD = 0.750), while their self-reported cybersecurity behavior was only moderate (M = 3.49, SD = 0.846). This discrepancy highlights a significant knowledge-behavior gap.

Table 4
Means and standard deviations of cybersecurity literacy

Dimensions	M	SD	Importance level
Cybersecurity Knowledge	3.79	0.750	High
Cybersecurity Behavior	3.49	0.846	Moderate
Overall Cybersecurity literacy	3.63	0.726	Moderate

Table 5
Means and Standard Deviations of Cybersecurity Knowledge and Behavior Items

Items	M	SD	Importance level	Ranking
Dimension1: Cybersecurity Knowledge				
I am aware of the risks that may result from sharing personal information online.	4.27	1.012	High	1
I am aware of how to adjust my privacy settings on social media.	3.96	1.008	High	2
I have complete knowledge on how to create a strong password.	3.90	1.084	High	3
I can recognize phishing messages or fake websites.	3.46	1.143	Moderate	4
I am aware of the importance of two-factor authentication.	3.37	1.145	Moderate	5
Dimension 2: Cybersecurity Behavior				
I have a strong password for my accounts.	4.11	0.962	High	1
I avoid sharing my personal information online.	4.03	1.397	High	2
I avoid opening the phishing links or websites.	3.95	1.405	High	3
I avoid using one password for all my accounts.	3.21	1.417	Moderate	4
I change my passwords constantly.	2.97	1.222	Moderate	5
I added two-factor authenticator for my accounts.	2.68	1.481	Moderate	6

The analysis reveals that adolescents demonstrate strong awareness of social-relational risks (e.g., sharing personal information, M = 4.27) but lower awareness of technical-procedural security measures (e.g., two-factor authentication, M = 3.37). In the behavior dimension, the 1.43-point difference between having a strong password (M = 4.11) and implementing two-factor authentication (M = 2.68) highlights a critical vulnerability where knowledge of best practices fails to translate into protective action.

3.1.3. Demographic Differences in Cybersecurity Literacy

ANOVA and t-tests were conducted to examine differences in cybersecurity literacy across demographic groups. The results are summarized in Table 6.

Table 6
Demographic Differences in Cybersecurity Literacy

Variable	Statistic	P	Significant?
Age	F = 1.196	0.312	No
Gender	t = -1.188	0.235	No
Geographical Area	F = 3.307	0.020	Yes
School Type	F = 0.709	0.493	No
Time Spent Online	F = 3.106	0.027	Yes

No significant differences were found by age or gender. However, significant differences were found by geographical area (F = 3.307, p = .020), with urban adolescents (M = 3.70) demonstrating the highest literacy and desert/Badia adolescents the lowest (M = 3.48). Tukey's post-hoc test revealed that urban adolescents had significantly higher cybersecurity knowledge than both rural (mean difference = 0.21, p = .018) and desert/Badia (mean difference = 0.26, p = .027) adolescents. Significant differences were also found by time spent online (F = 3.106, p = .027), with the Games-Howell test revealing that adolescents spending more than 6 hours online (M = 3.74) and 4–6 hours online (M = 3.68) had significantly higher literacy than those spending less than 1 hour (M = 3.42).

3.1.4. Online Threat Exposure

Participants were asked about their exposure to various online threats. As shown in Table 7, the most commonly encountered threats were hacking attempts (28.10%), exposure to harmful content (23.53%), and cyberbullying (16.73%).

Table 7
Online Threats in Descending Order

Threat Type	Frequency	Percentage (%)
Hacking attempts	215	28.10
Harmful content	180	23.53
Cyberbullying	128	16.73
Other threats	116	15.16
Personal data misuse	47	6.14
Phishing scam	24	3.14
Economic exploitation	23	3.01
Harassment	21	2.75
Sexual exploitation	11	1.44
Total	765	100

Further analysis revealed a consistent concentration of online threat exposure among adolescents attending public schools in urban areas. The extremely low reporting of sexual exploitation (1.44%) and harassment (2.75%) is a critical anomaly, strongly suggesting significant underreporting due to social stigma and fear of blame.

3.1.5. Reporting Behaviors

When faced with online threats, the most common reporting pattern was reporting to parents (43.2%). However, a concerning 29.12% of participants chose not to report because they did not believe the threat was serious or critical. The reporting rate to schools was only 1.28%.

Table 8
Reporting Behaviors Following Threat Exposure

Reporting Action	Frequency	Percentage (%)
Reported to parents	270	43.20
Did not report (not perceived as serious)	182	29.12
Reported to authorities	71	11.36
Did not report (did not know how)	38	6.08
Reported to relatives	31	4.96
Did not report (fear of punishment)	25	4.00
Reported to school	8	1.28

3.1.6. Training and Regression Analysis

A substantial 39.36% of adolescents reported having received no formal or informal training on cybersecurity and online safety. Among those who received training, schools were the primary source (31.52%), followed by parents (11.68%) and self-learning (8.80%). Social workers (2.08%), NGOs (1.60%), and government programs (1.60%) accounted for minimal training provision.

To identify key predictors, a series of regression analyses were performed. The results are presented in Table 9.

Table 9
Regression Analyses for Cybersecurity Literacy, Threat Exposure, and Reporting

Dependent Variable	Independent Variable	Coefficients		
		B	Beta (β)	P- value
Cybersecurity Literacy	Area	0.005	0.006	0.874
	Time spent online	0.113	0.148	0.000188
	Received Training	0.297	0.199	0.0000006
Exposure to threats	Time spent online	0.044	0.061	0.135
	Cybersecurity literacy	-0.127	-0.135	0.001
	Received Training	0.046	0.033	0.426
Reporting	Time spent online	-0.138	0.871	0.126
	Cybersecurity literacy	-0.058	0.944	0.633
	Exposure to threats	-0.210	0.811	0.094
	Received Training	0.820	2.270	0.000003

Training was the strongest predictor of cybersecurity literacy (B = 0.297, p < .001), indicating that adolescents who received training scored 0.297 points higher. Time spent online was also a significant predictor (B = 0.113, p < .001). Cybersecurity literacy was the only significant predictor of threat exposure (B = -0.127, p = .001), demonstrating its protective effect. Training was the sole significant predictor of threat reporting (B = 0.820, p < .001), meaning adolescents who received training were 2.27 times more likely to report threats.

3.2. Qualitative Findings

The qualitative findings are derived from thematic analysis of focus group discussions with students and parents, and semi-structured interviews with teachers and counselors. The themes are organized around the three research questions.

3.2.1. Barriers to Applying Cybersecurity Knowledge

Four primary themes emerged that explain the knowledge-behavior gap.

Theme 1: Knowledge-Behavior Gap. Participants highlighted that adolescents often fail to remember or apply what they have learned about online safety. A teacher observed: “Adolescents do not remember everything they learned about online safety when they engage in their daily online activities.” A parent added: “Children lack sufficient digital skills and have not received practical cybersecurity training to enable them to use the digital space safely.”

Theme 2: Lack of Family and Community Support. Parents often do not engage in meaningful conversations about digital safety with their children, and peer influence can encourage risky behavior. A parent noted: “Parents don’t talk seriously about these topics with their children at home.” A counselor confirmed: “Peers often have a significant influence on risky behavior.”

Theme 3: Personal and Behavioral Impediments. Adolescents’ developmental characteristics, such as heightened curiosity and impulsive decision-making, lead them to engage in risky online behaviors despite knowing the potential consequences. A student shared: “Curiosity drives us to open some strange links to explore its content.”

Theme 4: Resource and Technology Limitations. Participants noted that adolescents sometimes struggle with the technical aspects of digital platforms. A parent explained: “Our children have difficulty using or navigating certain applications and websites, which makes them vulnerable to some online risks.”

3.2.2. Digital Threats and Reporting

Three themes were identified regarding threat types and reporting factors.

Theme 1: Types of Other Online Threats. Participants highlighted that adolescents encounter online disinformation and intellectual manipulation. A student stated: “We encounter misinformation online that sometimes influences the way we think.”

Theme 2: Enablers for Reporting. Key enablers included ensuring safety and security, preventing recurrence, and positive relationships with family and friends. A student explained: “I report the online threats I am exposed to so that they do not happen again to me and others.” Another added: “The support of my family and friends encourages me to report the threats I face.”

Theme 3: Barriers to Reporting. Barriers included fear of bullying, parental punishment, and retribution; shame culture; low trust in parent-child relationships; and lack of a clear reporting system in schools. A student disclosed:

“Sometimes we do not report the threats we are exposed to for fear of bullying or shame or because of a lack of trust between us and our parents.”

3.2.3. Preferred Intervention Approaches

Four themes emerged regarding optimal intervention strategies.

Theme 1: Preferred Methods for Capacity Building. Story-based learning, case-based learning, and interactive learning (video, games) were identified as the most effective methods. A teacher noted: “Students love storytelling and engage with it greatly, which increases their awareness.” A student confirmed: “What makes the training memorable is the use of videos, games, and real-life cases.”

Theme 2: Family Participation and Involvement. Participants emphasized open discussions between parents and children, parental modeling of safe online behavior, and awareness sessions for parents.

Theme 3: The Collaborative Role of Schools and Social Workers. Participants emphasized school-based prevention programs in collaboration with specialists and experts, as well as adequate support to families and students by social workers.

Theme 4: Ideal Reporting Mechanisms. Parents, schools, and authorities were identified as the key entities to which adolescents should be able to report online threats, with all three systems needing to be strengthened and coordinated.

4. Discussion

This section synthesizes and interprets the findings, contextualizing them within the broader academic literature and the study's theoretical underpinnings. The discussion is organized around the three research questions and concludes with a proposed intervention model, implications for practice and policy, and limitations.

4.1. The Knowledge-Behavior Gap: Cybersecurity Literacy Among Jordanian Adolescents

The first major finding revealed that while adolescents in Jordan possess a high level of theoretical cybersecurity knowledge (M = 3.79), their application of this knowledge in practice remains moderate (M = 3.49). This significant knowledge-behavior gap is consistent with findings in other contexts (AlSobeh et al., 2023; Branley-Bell et al., 2022) and represents a central challenge for cybersecurity education. The qualitative data provided rich insights into the multifaceted barriers that prevent the translation of knowledge into protective action, which can be understood across various ecological levels.

From the perspective of Bronfenbrenner's (1979, 1994) Ecological Systems Theory, these barriers are products of a complex, interconnected system. At the microsystem level, individual factors such as curiosity and impulsiveness drive risky behaviors, compounded by a lack of parental supervision and the powerful influence of peer norms. When peers do not prioritize safe online practices, it creates a social environment where risky behavior is normalized, a finding that resonates with research on peer influence in adolescent behavior (Lahti et al., 2024). The mesosystem, representing the connection between different microsystems, is also critical. The findings indicate a disconnect between home and school, with parents expressing a desire for more school involvement and teachers highlighting the need for family reinforcement. This gap results in inconsistent messaging and a fragmented approach to

cybersecurity education. At the exosystem level, the complexity of application interfaces and the lack of user-friendly security features create technological hurdles that directly impact adolescents' ability to implement safe practices.

At the broadest level, the macrosystem shapes perceptions of cybersecurity. The qualitative findings suggest that cybersecurity is often viewed as a technical, abstract subject rather than an essential life skill. Social Construction Theory (Berger & Luckmann, 1966; Payne, 2021) helps explain this phenomenon: if the community does not collectively define cybersecurity as a priority, individuals are less likely to internalize and act upon its principles.

The finding that no significant differences in overall literacy existed by age or gender aligns with some recent research (Aljohni et al., 2021) but contrasts with studies that found age and gender to be significant factors (Branley-Bell et al., 2022). However, the significant differences by geographical area, with urban adolescents demonstrating higher knowledge than their rural and desert-dwelling counterparts, point to a digital divide that extends beyond mere access to technology, reflecting disparities in educational resources, infrastructure, and exposure to digital safety campaigns (Sanders & Scanlon, 2021). The finding that adolescents who spend more time online demonstrate higher literacy is consistent with the notion that increased digital engagement enhances understanding and skills, though Subasi et al. (2023) have cautioned that greater time online may also increase vulnerability to threats.

4.2. A Landscape of Digital Threats and the Culture of Silence

The second research question revealed a concerning picture of the digital threats confronting Jordanian adolescents. Hacking attempts (28.1%), exposure to harmful content (23.5%), and cyberbullying (16.7%) emerged as the most prevalent risks, broadly consistent with global trends (AlSobeh et al., 2023). The qualitative data further enriched this understanding by identifying more nuanced threats such as online disinformation and intellectual manipulation, which have corrosive effects on critical thinking and social cohesion (Lahti et al., 2024).

The extremely low reporting of sexual exploitation (1.4%) warrants careful interpretation. Rather than indicating a low prevalence, this figure likely reflects the profound influence of macrosystem factors, particularly the cultural stigma and shame associated with sexual victimization in the Jordanian context. This interpretation is supported by the qualitative finding that shame culture and fear of punishment are significant barriers to reporting. From a Social Construction perspective, the act of reporting a digital threat is not a neutral event but is socially defined, and in this context, it appears to be constructed as a risky and potentially shameful act. This social definition discourages disclosure and fosters what can be characterized as a culture of silence.

The finding that 29.1% of adolescents did not report a threat because they deemed it "not serious" suggests a normalization of certain online harms, a social construction that minimizes their potential impact and further entrenches underreporting. The low rate of reporting to schools (1.3%) is a particularly stark finding, pointing to a significant weakness in the mesosystem. Schools are ideally positioned to be a central hub for support and intervention, yet they appear to be underutilized, likely due to a lack of clear, accessible, and trusted reporting systems (Wachs et al., 2019). Without effective institutional pathways for help-seeking, adolescents are left to navigate these challenges alone or rely solely on their immediate family, which, as the data revealed, can also be a source of fear and judgment.

The concentration of threat exposure among urban, public school adolescents suggests a critical intersection of high digital exposure and potentially lower protective capacity within the public school system. Ecological Systems Theory provides a valuable framework for understanding these patterns: the extensive use of digital platforms places adolescents at the center of a digital microsystem teeming with both opportunities and risks, while the macrosystem

context of rapid digitalization in Jordanian society (Ministry of Digital Economy and Entrepreneurship, 2022) creates an environment where exposure to diverse threats is almost inevitable.

4.3. Training as the Cornerstone of Protection: Toward an Evidence-Based Intervention

The third research question explored a potential model for social work intervention. The quantitative data provided a clear directive: training is the single most powerful predictor of both increased cybersecurity literacy ($B = 0.297$, $p < .001$) and the likelihood of reporting threats ($B = 0.820$, $p < .001$). This empirically validates the central role of education and capacity-building in any effective intervention strategy. Furthermore, the finding that higher literacy is a significant negative predictor of threat exposure ($B = -0.127$, $p = .001$) provides compelling evidence that empowering adolescents with knowledge and skills is a direct form of protection.

However, the qualitative findings crucially illuminated that the method of training is as important as the training itself. Adolescents and educators alike expressed a strong preference for methods that are engaging, relatable, and practical, with story-based learning, case-based learning, and interactive learning identified as the most favored approaches. This points away from traditional, didactic instruction and toward pedagogical approaches that resonate with adolescents' lived experiences and learning styles. Digital storytelling, in particular, has been shown to be an effective tool for enhancing digital literacy and promoting critical skills (Akdag & Altinay, 2021; Kaptan & Cakir, 2025).

The finding that 39.4% of adolescents have received no formal cybersecurity training reveals a critical protective gap that demands immediate attention. Among those who received training, schools were the primary source (31.5%), while training from social workers (2.1%), NGOs (1.6%), and government programs (1.6%) was minimal. This distribution underscores the need for a coordinated, multi-stakeholder approach to cybersecurity education that leverages the resources of all ecological systems.

4.4. Proposed Intervention: A Storytelling-Based Model for Online Resilience

Based on the study's empirical findings and theoretical analysis, this research proposes a multi-level, storytelling-based intervention model designed to enhance cybersecurity literacy and promote online resilience among adolescents in Jordan. The model is predicated on the demonstrated power of training and the expressed preference for narrative-based learning. Its core rationale is to bridge the knowledge-behavior gap by moving beyond information delivery to foster critical thinking, empathy, and behavioral change through relatable and culturally resonant stories.

The model's goal is to enhance cybersecurity literacy, promote safe online behaviors, and build a supportive ecosystem for child protection in the digital age among adolescents aged 14 to 17 in Jordanian schools. Key stakeholders include adolescents as co-designers and primary audience; parents and teachers as facilitators of dialogue and reinforcement; social workers as key personnel for training, leading support groups, and advocating for policy change; the Ministry of Education and the Ministry of Digital Economy and Entrepreneurship for policy-level integration; and NGOs and the private sector as partners in content creation and public awareness.

The model comprises three core components. First, co-designed digital stories would be developed through brainstorming sessions involving students, parents, teachers, social workers, and cybersecurity experts, ensuring that narratives are authentic, address the most salient risks identified in the research, and reflect the cultural context of Jordanian adolescents (Quayyum, 2025). Second, facilitated dialogue and critical thinking sessions would follow

each story viewing, enabling adolescents to process the narrative content and develop analytical skills. Third, multi-level implementation would follow an ecological approach: at the microsystem level through in-class sessions; at the mesosystem level through parent-teacher workshops that address the identified gap between home and school; at the exosystem level through collaboration with the Ministry of Education to integrate the curriculum nationally and partnerships with NGOs and telecommunication companies; and at the macrosystem level through a national media campaign promoting a cultural shift toward viewing digital citizenship as a shared responsibility.

From a Social Construction perspective, storytelling is a powerful mechanism for shaping shared meaning and social norms. By presenting relatable narratives of online challenges and successful resolutions, the intervention can help socially reconstruct the meaning of cybersecurity, transforming it from an abstract, technical topic into a set of practical, pro-social behaviors. It can also reframe the act of reporting from a shameful confession into a brave and responsible action, creating new, positive social scripts for adolescents to follow (Andriessen et al., 2025; Weijsenfeld & Sarmah, 2025).

4.5. Implications for Social Work Practice and Policy

The findings carry profound implications for the social work profession and public policy. For social work practice, the digital environment represents a new and critical context that demands the development of specialized competencies. Social workers must integrate questions about online life into routine assessments with children and families, including inquiries about social media use, online friendships, experiences with online risks, and digital well-being (Copson et al., 2022). The ecological assessment, a hallmark of social work, must now include the digital environment as a critical system influencing development and well-being. Social workers should also champion narrative-based approaches, leading the development and implementation of evidence-based storytelling interventions within schools and community centers (Storer et al., 2023).

For policy and advocacy, the findings highlight several critical areas. First, child protection policies and frameworks must be updated to explicitly include online risks, defining digital abuse and exploitation in legal and policy terms and establishing clear mandates for child welfare agencies to investigate and respond to online harms (Committee on the Rights of the Child, 2021). Second, the findings provide strong evidence for advocating the mandatory inclusion of comprehensive, age-appropriate, and behavior-focused cybersecurity education in the national school curriculum, based on the principles of interactive and narrative-based learning identified in this study (Pirta-Dreimane et al., 2022). Third, social workers can be a powerful voice in advocating for technology companies to adopt a "safety by design" approach, building safety features into their products from the outset rather than treating safety as an afterthought (Köhler-Dauner et al., 2025).

4.6. Limitations and Future Directions

While this study provides valuable insights, several limitations must be acknowledged. First, the cross-sectional design captures a single moment in time and limits the ability to draw causal inferences between variables. For example, while the study found a correlation between time spent online and higher literacy, it cannot determine the direction of this relationship. Second, the reliance on self-reported data introduces the possibility of social desirability bias, where participants may have provided answers they perceived as more favorable. Third, while the sample was geographically diverse, it was not a true random sample of the entire Jordanian adolescent population, with the sample predominantly drawn from urban areas and public schools, which may limit generalizability. Fourth, the qualitative sample size (N = 20), while sufficient for generating thematic insights, was relatively small and may not have captured the full range of experiences and perspectives.

Future research should address these limitations by employing longitudinal designs to track changes in cybersecurity literacy, behaviors, and threat exposure over time. More research is needed on the specific online risks and vulnerabilities of marginalized adolescent groups, including those with disabilities, refugees, and those in remote rural areas. Rigorous evaluations, including randomized controlled trials, should be conducted to assess the effectiveness of different social work and educational intervention models, particularly the storytelling-based approach proposed in this study. Finally, more research is needed on the integration of digital risks into child protection frameworks and the role of social work in addressing online threats across the Global South.

5. Conclusion

This study has illuminated the complex digital landscape inhabited by adolescents in Jordan, revealing a critical paradox: while quantitative findings demonstrate a high level of cybersecurity knowledge (M = 3.79), this does not translate into consistent protective behaviors (M = 3.49), indicating a significant knowledge-behavior gap. This gap is not a simple matter of individual choice but is deeply embedded within a multi-layered ecological context. Barriers at the microsystem level, such as adolescent curiosity and peer norms, are compounded by a disconnect between home and school at the mesosystem, the complexities of digital interfaces at the exosystem, and pervasive cultural norms at the macrosystem that frame cybersecurity as a purely technical concern. Consequently, a substantial number of young people are exposed to significant risks, including hacking attempts (28.1%), harmful content (23.5%), and cyberbullying (16.7%), alongside more insidious threats of disinformation and intellectual manipulation identified through qualitative inquiry. The study further exposes a concerning culture of silence surrounding the reporting of digital threats: while 43.2% of adolescents turn to their parents, a mere 1.3% report incidents to schools, hindered by fear, shame, and a lack of trust in formal systems. Critically, the finding that targeted training is the strongest predictor of both cybersecurity literacy (B = 0.297) and reporting behavior (B = 0.820) underscores the transformative potential of education. The proposed storytelling-based intervention model offers a promising, evidence-based pathway forward, leveraging the power of narrative to foster critical thinking, enhance digital competencies, and promote pro-social behaviors across multiple ecological levels. Ultimately, protecting children in the digital age is a fundamental challenge of social justice that requires the dedicated and collaborative efforts of social workers, educators, policymakers, and communities to create a world where all individuals can thrive in safety and dignity, both online and off.

Declarations

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contribution

M.G. conceptualized the study, conducted data curation and formal analysis, led the investigation, and developed the methodology. M.G. wrote the original draft and contributed to writing – review & editing. S.A.M. contributed to methodology, provided resources and supervision, and contributed to writing – review & editing. M.G. and S.A.M. reviewed and approved the final manuscript.

Data Availability

The data that support the findings of this study are not publicly available due to ethical restrictions. Requests for access to the data may be directed to the corresponding author.

References

1. Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic. *IEEE Access*, *9*, 121916–121929. https://doi.org/10.1109/ACCESS.2021.3109091
2. Ahmad, N., Laplante, P. A., DeFranco, J. F., & Kassab, M. (2022). A Cybersecurity Educated Community. *IEEE Transactions on Emerging Topics in Computing*, *10*(3), 1456–1463. https://doi.org/10.1109/TETC.2021.3093444
3. Akdag, S., & Altinay, Z. (2021). Learning Through Digital Stories for Safe School Environment. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/fpsyg.2021.738954
4. Alansari, A. N., Alwawi, A., Salim, A., Tarawah, N., Ksia, A., & Zaazouee, M. S. (2026). A systematic review of social media impact on psychological well-being among children, adolescents, and young adults in arab countries. *Asian Journal of Psychiatry*, *115*, 104793. https://doi.org/10.1016/j.ajp.2025.104793
5. Aldawood, H., & Skinner, G. (2020). Evaluating Contemporary Digital Awareness Programs for Future Application within the Cyber Security Social Engineering Domain. *International Journal of Computer Applications*, *177*(31), 57–61. https://doi.org/10.5120/ijca2020919793
6. Alexander, B., Adams Becker, S., & Cummins, M. (2016). *Digital Literacy*: *An NMC Horizon Project Strategic Brief*. *Volume 3.3*. New Media Consortium. https://eric.ed.gov/?id=ED593900
7. Alharbi, N., Samra, H., Li, A., & Soh, B. (2025). Empowering Saudi youth: The ISAS framework for promoting online safety and cybersecurity awareness. *International Journal of Advanced and Applied Sciences*, *12*(3), 131–142. https://doi.org/10.21833/ijaas.2025.03.014
8. Aljohni, W., Elfadil, N., Jarajreh, M., & Gasmelsied, M. (2021). Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *12*(3). https://doi.org/10.14569/IJACSA.2021.0120334
9. Alshareef, B. E., Abumariam, A., Mali, I. B., & Bader, O. G. (2024). The Risks to which Adolescent Girls are Exposed Via the Internet in Jordan and the Protection Mechanisms used from the Perspective of Adolescent Girls and their Caregivers. *International Journal of Religion*, *5*(11), 1214–1224. https://doi.org/10.61707/sfc29214
10. AlSobeh, A. M. R., AlAzzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technologies*, *13*(2), e202312. https://doi.org/10.30935/ojcmt/12942
11. Altarawneh, M. H. M., Althunibat, A., Almajali, M. H., Alzriqat, N., & Alazzam, S. (2025). Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps. *International Journal of Innovative Research and Scientific Studies*, *8*(1), 1516–1529. https://doi.org/10.53894/ijirss.v8i1.4696
12. Álvarez-Guerrero, G., Fry, D., Lu, M., & Gaitis, K. K. (2024). Online Child Sexual Exploitation and Abuse of Children and Adolescents with Disabilities: A Systematic Review. *Disabilities*, *4*(2), 264–276. https://doi.org/10.3390/disabilities4020017
13. Andriessen, J., Citro, T., Palmieri, G., & Pardijs, M. (2025). Spreading Awareness Cybersecurity via Storytelling: A Systematic Literature Review. *Methodologies and Intelligent Systems for Technology Enhanced Learning,*

Workshops - 14th International Conference, Lecture Notes in Networks and Systems, *1308*, 179–191. https://doi.org/10.1007/978-3-031-85561-0_15

14. Anna Laczi, S., & Póser, V. (2024). Navigating Children's Cybersecurity Landscape: Understanding the impact of cyberbullying, online harrasment and identity theft on children. *2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 1–6. https://doi.org/10.1109/SACI60582.2024.10619762
15. Audrin, C., & Blaya, C. (2020). Psychological Well-Being in a Connected World: The Impact of Cybervictimization in Children's and Young People's Life in France. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.01427
16. Bednarek, S., Górski, M., Załęska, A., Bychowski, M., Kwaśna, J., Kaźmierczyk, I., Lenart, K., Homza, M., Zakrzewska, N., & Kulicka, J. (2024). The Psychological Effects of Social Media Use: Insights from Combined Research on Adolescents' Mental Health. *Quality in Sport*, *35*, 56340–56340. https://doi.org/10.12775/QS.2024.35.56340
17. Behan-Devlin, J. (2024). Digital Technology in Children's Safeguarding Social Work Practice in the 21st Century: A Scoping Review. *The British Journal of Social Work*, *54*(7), 2957–2976. https://doi.org/10.1093/bjsw/bcae071
18. Berger, P. L., & Luckmann, T. (1966). *The social construction of reality: A treatise in the sociology of knowledge* (1st ed.). Anchor Books.
19. Blažič, B. J., & Blažič, A. J. (2022). Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity. *Sustainability*, *14*(8). https://doi.org/10.3390/su14084763
20. Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring Age and Gender Differences in ICT Cybersecurity Behaviour. *Human Behavior and Emerging Technologies*, *2022*(1), 2693080. https://doi.org/10.1155/2022/2693080
21. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
22. Bronfenbrenner, U. (1979). *The Ecology of Human Development: Experiments by Nature and Design*. Harvard University Press. https://doi.org/10.2307/j.ctv26071r6
23. Bronfenbrenner, U. (1994). Ecological models of human development. In *International Encyclopedia of Education* (2nd ed., pp. 37–43). Elsevier.
24. Byrne, D. (2022). A worked example of Braun and Clarke's approach to reflexive thematic analysis. *Quality & Quantity*, *56*(3), 1391–1412. https://doi.org/10.1007/s11135-021-01182-y
25. Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: Complex or simple? Research case examples. *Journal of Research in Nursing*, *25*(8), 652–661. https://doi.org/10.1177/1744987120927206
26. Committee on the Rights of the Child (Ed.). (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. UN. https://digitallibrary.un.org/record/3906061
27. Copson, R., Murphy, A. M., Cook, L., Neil, E., & Sorensen, P. (2022). Relationship-based practice and digital technology in child and family social work: Learning from practice during the COVID-19 pandemic. *Developmental Child Welfare*, *4*(1), 3–19. https://doi.org/10.1177/25161032221079325
28. Corcoran, E., Clement, A., & Gabrielli, J. (2024). A measurement model of online privacy cognitions in a sample of U.S. adolescents. *Behaviour & Information Technology*, *43*(16), 4150–4171. https://doi.org/10.1080/0144929X.2024.2305286

29. Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). SAGE Publications.
30. Draucker, C. B., Rawl, S. M., Vode, E., & Carter-Harris, L. (2020). Integration Through Connecting in Explanatory Sequential Mixed Method Studies. *Western Journal of Nursing Research*, *42*(12), 1137–1147. https://doi.org/10.1177/0193945920914647
31. Du, K., Huo, W., & Yang, Z. (2024). The Impact of Cyberbullying on Adolescents' Real Lives. *Journal of Education, Humanities and Social Sciences*, *45*, 453–460. https://doi.org/10.54097/hjh6e709
32. Edmonds, W. A., & Kennedy, T. D. (2017). Explanatory-Sequential Approach. In *An Applied Guide to Research Designs: Quantitative, Qualitative, and Mixed Methods* (2nd ed., pp. 196–200). SAGE Publications, Inc. https://doi.org/10.4135/9781071802779
33. Elvira-Zorzo, M. N., & Gómez, P. B. (2025). Identity Construction and Digital Vulnerability in Adolescents: Psychosocial Implications and Implications for Social Work. *Youth*, *5*(4). https://doi.org/10.3390/youth5040119
34. Esfandiari, M., Sciacca, B., Feijóo, S., Laffan, D. A., Milosevic, T., O'Toole, C., & O'Higgins Norman, J. (2025). Trends in digital technologies to address children's online safety education: A systematic scoping review. *International Journal of Educational Research Open*, *9*, 100462. https://doi.org/10.1016/j.ijedro.2025.100462
35. Fattah, A., Wagimin, & Nurlia. (2023). Enhancing Cybersecurity Awareness among University Students: A Study on the Relationship between Knowledge, Attitude, Behavior, and Training. *JSI: Jurnal Sistem Informasi (E-Journal)*, *15*(1), 3139–3149. https://doi.org/10.18495/jsi.v15i1.115
36. Feilzer, M. Y. (2023). A Pragmatist Approach to Mixed Methods Research. In *Philosophical Foundations of Mixed Methods Research*. Routledge.
37. Field, A. (2018). *Discovering Statistics Using IBM SPSS Statistics* (5th ed.). SAGE Publications Ltd.
38. Gaitis, K. K., Vermeulen, I., Stevenson, J. G., & Fry, D. (2025). Extended reality environments and child safety: Examining the emerging risks for child sexual exploitation and abuse and discussing prevention and response through a technologised neo-ecological perspective. *International Journal of Law, Crime and Justice*, *83*, 100786. https://doi.org/10.1016/j.ijlcj.2025.100786
39. Ghandour, A., & Woodford, B. J. (2024). Guidelines to Develop a Cybersecurity Policy in Schools, Perspectives Informed from Jordanian Cybercrime Law. *2024 25th International Arab Conference on Information Technology (ACIT)*, 1–6. https://doi.org/10.1109/ACIT62805.2024.10876919
40. Gillespie, A., Glăveanu, V., & de Saint Laurent, C. (2024). *Pragmatism and Methodology: Doing Research That Matters with Mixed Methods*. Cambridge University Press. https://doi.org/10.1017/9781009031066
41. Gonzales, M. (2020). The Bronfenbrenner Micro- and Meso- Systems. In M. Gonzales (Ed.), *Systems Thinking for Supporting Students with Special Needs and Disabilities: A Handbook for Classroom Teachers* (pp. 81–92). Springer. https://doi.org/10.1007/978-981-33-4558-4_6
42. Hoang T. B, M., Dang-Pham, D., Hoang, A.-P., Le Gia, B., & Nkhoma, M. (2020). Network Analytics for Improving Students' Cybersecurity Awareness in Online Learning Systems. *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, 1–7. https://doi.org/10.1109/RIVF48685.2020.9140781
43. International Federation of Social Workers. (2014). *Global Definition of Social Work – International Federation of Social Workers*. International Federation of Social Workers. https://www.ifsw.org/what-is-social-work/global-definition-of-social-work/
44. Jacobson, D., & Idziorek, J. (2013). *Computer Security Literacy: Staying Safe in a Digital World*. Chapman and Hall/CRC. https://doi.org/10.1201/b13707

45. Jaskulska, S., Jankowiak, B., Pérez-Martínez, V., Pyżalski, J., Sanz-Barbero, B., Bowes, N., Claire, K. D., Neves, S., Topa, J., Silva, E., Mocanu, V., Dascalu, C. G., & Vives-Cases, C. (2022). Bullying and Cyberbullying Victimization and Associated Factors among Adolescents in Six European Countries. *Sustainability*, *14*(21). https://doi.org/10.3390/su142114063
46. Kalenda, S., & Kowaliková, I. (2020). The Digital Exclusion of Vulnerable Children: Challenge for Sustainability Issues in Czech Social Work Practice. *Sustainability*, *12*(23). https://doi.org/10.3390/su12239961
47. Kaptan, E., & Cakir, R. (2025). The effect of digital storytelling on digital literacy, 21st century skills and achievement. *Education and Information Technologies*, *30*(8), 11047–11071. https://doi.org/10.1007/s10639-024-13287-6
48. Kaushik, V., & Walsh, C. A. (2019). Pragmatism as a Research Paradigm and Its Implications for Social Work Research. *Social Sciences*, *8*(9). https://doi.org/10.3390/socsci8090255
49. Köhler-Dauner, F., Peter, L., Sitarski, E., Chauviré-Geib, K., Haag, A.-C., & Fegert, J. M. (2025). Digital child protection in social networks: Age verification and age-tiered regulation in Europe. *Child and Adolescent Psychiatry and Mental Health*, *19*(1), 143. https://doi.org/10.1186/s13034-025-01016-x
50. Kovács-Szépvölgyi E. (2023). *Digital Child Protection in the Light of Sustainability*. (World). 1st Conference on Sustainability (COS '23). https://cos.sze.hu/digital-child-protection-in-the-light-of-sustainability
51. Krejcie, R. V., & Morgan, D. W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*, *30*(3), 607–610. https://doi.org/10.1177/001316447003000308
52. Krueger, R. A., & Casey, M. A. (2014). *Focus Groups A Practical Guide for Applied Research* (5th ed.). SAGE Publications, Inc. https://uk.sagepub.com/en-gb/eur/focus-groups/book243860
53. Lahti, H., Kokkonen, M., Hietajärvi, L., Lyyra, N., & Paakkari, L. (2024). Social media threats and health among adolescents: Evidence from the health behaviour in school-aged children study. *Child and Adolescent Psychiatry and Mental Health*, *18*(1), 62. https://doi.org/10.1186/s13034-024-00754-8
54. Laird, R. D., & Hawk, S. T. (2024). Adolescents' perceptions of privacy violations by parents, siblings, and friends. *Journal of Research on Adolescence*, *34*(4), 1378–1390. https://doi.org/10.1111/jora.13000
55. Lee, H.-J., Kim, S., & Park, J.-A. (2022). A Narrative Inquiry on Adolescents' Experiences of Digital Sexual Violence. *Journal of Korean Women's Studies*, *38*(3), 73–108. https://doi.org/10.30719/JKWS.2022.09.38.3.73
56. Lee, W., & Lee, E. (2022). Social Workers as Information Navigators: Insights into the Use of the Web for Serving Clients. *Social Work*, *67*(4), 351–361. https://doi.org/10.1093/sw/swac028
57. Lin, K., Cheng, V. S., Li, J. C. M., Jia, C. X., Jiang, X., & Mlyakado, B. P. (2025). Online Sexual Exploitation Among Adolescents in Tanzania: Exploring the Stigmas of Victimization and Help-Seeking. *Child & Family Social Work*, *31*(1), 225–236. https://doi.org/10.1111/cfs.13266
58. Luic, L., Svelec-Juricic, D., & Misevic, P. (2021). The Impact of Knowledge of the Issue of Identification and Authentication on the Information Security of Adolescents in the Virtual Space. *WSEAS TRANSACTIONS ON SYSTEMS AND CONTROL*, *16*, 527–533. https://doi.org/10.37394/23203.2021.16.49
59. Martínez, G., Garmendia, M., & Garitaonandia, C. (2020). Children and adolescents and Information and Communication Technologies (ICTs): Opportunities, risks and harm. *ZER. Revista de Estudios de Comunicación*, *25*(48). https://doi.org/10.1387/zer.21116
60. Ministry of Digital Economy and Entrepreneurship. (2022). *Survey on ICT access and use in Households and by Individuals 2022*. Ministry of Digital Economy and Entrepreneurship.
61. Molero, M. M., Martos, Á., Barragán, A. B., Pérez-Fuentes, M. C., & Gázquez, J. J. (2022). Anxiety and Depression from Cybervictimization in Adolescents: A Metaanalysis and Meta-regression Study. *European Journal of*

Psychology Applied to Legal Context, *14*(1), 42–50. https://doi.org/10.5093/ejpalc2022a5

62. Muller, S. R., & Burrell, D. N. (2022). Social Cybersecurity and Human Behavior. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)*, *6*(1), 1–13. https://doi.org/10.4018/IJHIoT.305228
63. Navarro, J. L., & Tudge, J. R. H. (2023). Technologizing Bronfenbrenner: Neo-ecological Theory. *Current Psychology*, *42*(22), 19338–19354. https://doi.org/10.1007/s12144-022-02738-3
64. Oguine, O. C., Anuyah, O., Agha, Z., Melgarez, I., Alvarado Garcia, A., & Badillo-Urquiola, K. (2025). Online Safety for All: Sociocultural Insights from a Systematic Review of Youth Online Safety in the Global South. *Proc. ACM Hum.-Comput. Interact.*, *9*(7), CSCW458:1-CSCW458:30. https://doi.org/10.1145/3757639
65. Onditi, H. Z. (2023). Adolescents and Retaliation Coping with Cyberbullying: Do Individual and Social Factors Matter? *Papers in Education and Development*, *41*(2). https://journals.udsm.ac.tz/index.php/ped/article/view/6199
66. Patel, M.-G., & Quan-Haase, A. (2024). The social-ecological model of cyberbullying: Digital media as a predominant ecology in the everyday lives of youth. *New Media & Society*, *26*(9), 5507–5528. https://doi.org/10.1177/14614448221136508
67. Paukova, A. (2019). Online risks and information protection of children on the pages of pedagogical press of the USA. *Zhytomyr Ivan Franko State University Journal. Pedagogical Sciences*, *3*, 69–77. https://doi.org/10.35433/pedagogy.3(98).2019.69-77
68. Payne, M. (2021). *Modern Social Work Theory*. Red Globe Press.
69. Perwitasari, D. R., & Wuryaningsih, E. W. (2022). Why Did You Do That to Me?: A Systematic Review of Cyberbullying Impact on Mental Health and Suicide Among Adolescents. *NurseLine Journal*, *7*(1), 35–47. https://doi.org/10.19184/nlj.v7i1.27311
70. Pirta-Dreimane, R., Brilingaitė, A., Majore, G., Knox, B. J., Lapin, K., Parish, K., Sütterlin, S., & Lugo, R. G. (2022). Application of intervention mapping in cybersecurity education design. *Frontiers in Education*, *7*. https://doi.org/10.3389/feduc.2022.998335
71. Pratap, A., & Giri, G. (2025). Cybersecurity in the Age of Social Engineering: Implementing Effective Defense Strategies. In *Effective Strategies for Combatting Social Engineering in* Cybersecurity (pp. 77–90). IGI Global Scientific Publishing. (cybersecurity-in-the-age-of-social-engineering). https://doi.org/10.4018/979-8-3693-6665-3.ch004
72. Quayyum, F. (2025). Co-designing cybersecurity-related stories with children: Perceptions on cybersecurity risks and parental involvement. *Entertainment Computing*, *52*, 100753. https://doi.org/10.1016/j.entcom.2024.100753
73. Rakaab, M. N. (2025). Role of social workers on child protection response in Hargeisa Somaliland. *International Journal of Advanced Multidisciplinary Research*, *12*(1–2025), 8–17. https://doi.org/http://dx.doi.org/10.22192/ijamr.2025.12.01.002
74. Repi, P. A., & Nasution, M. I. P. (2024). Menguasai Literasi Teknologi untuk Mengatasi Risiko Keamanan Cyber. *El-Mujtama: Jurnal Pengabdian Masyarakat*, *4*(4), 2038–2049. https://doi.org/10.47467/elmujtama.v4i4.3583
75. Rikkers, V., & Sarmah, D. K. (2025). A story-driven gamified education on USB-based attack. *Journal of Computing in Higher Education*, *37*(1), 248–272. https://doi.org/10.1007/s12528-023-09392-z
76. Ruslin, Mashuri, S., Abdul Rasak, M. S., Alhabsyi, F., & Syam, H. (2022). Semi-structured Interview: A Methodological Reflection on the Development of a Qualitative Research Instrument in Educational Studies. *IOSR Journal of Research & Method in Education (IOSR-JRME), Ser. V*, *12*(1), 22–29.
77. Sadzaglishvili, S., Gotsiridze, T., & Lekeshvili, K. (2021). Ethical Considerations for Social Work Research With Vulnerable Children and Their Families. *Research on Social Work Practice*, *31*(4), 351–359.

https://doi.org/10.1177/1049731521996457

78. Sağlam, 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. https://doi.org/10.1109/TE.2022.3231019
79. Salazar, M., Raj, A., Silverman, J. G., Rusch, M. L. A., & Reed, E. (2023). Cyber Sexual Harassment among Adolescent Girls: A Qualitative Analysis. *Adolescents*, *3*(1), 84–91. https://doi.org/10.3390/adolescents3010007
80. Sanders, C. K., & Scanlon, E. (2021). The Digital Divide Is a Human Rights Issue: Advancing Social Inclusion Through Social Work Advocacy. *Journal of Human Rights and Social Work*, *6*(2), 130–143. https://doi.org/10.1007/s41134-020-00147-9
81. Santhosh, T., & Thiyagu, K. (2022). *Cyber Safety and Security Awareness Initiatives in India—A Systematic Review*. *19*(1), 42–50. https://doi.org/https://doi.org/10.26634/jet.19.1.18596
82. Save the Children Jordan. (2024). *Behind the Screens: Safety in Digital Spaces for Children aged 10-17 in Jordan*. Save the Children Jordan. https://api.savethechildren.org.jo/uploads/Behind_the_Screens_online_6c1f9129b8_346067571f.pdf
83. Segal, M., Lens, O., & Gur, A. (2025). Perspectives on Social Work in the Digital Age. *Ethics and Social Welfare*, *19*(4), 380–398. https://doi.org/10.1080/17496535.2025.2517104
84. Soldatova, G. U., & Ilyukhina, S. N. (2021). Self-Destructive Online Content: Features of Attitude and Response of Adolescents and Youth. *Counseling Psychology and Psychotherapy*, *29*(1), 66–91. https://doi.org/10.17759/cpp.2021290105
85. Stalans, L., Chan-Tin, E., Hart, A., Moran, M., & Kennison, S. (2023). Predicting Phishing Victimization: Comparing Prior Victimization, Cognitive, and Emotional Styles, and Vulnerable or Protective E-mail Strategies. *Victims & Offenders*, *18*(7), 1216–1235. https://doi.org/10.1080/15564886.2023.2218369
86. Storer, H. L., Scott, C. F., Eggleston, M., Shulruff, T., & Rodriguez, M. Y. (2023). Reimagining Social Work's Digital Future: The Critical Role of Interdisciplinary Tech Partnerships. *Journal of Social Work Education*, *59*(sup1), S105–S120. https://doi.org/10.1080/10437797.2023.2186994
87. Subasi, S., Korkmaz, O., & Cakir, R. (2023). Cyberbullying, Digital Footprint, and Cyber Security Awareness Levels of Secondary School Students. *International Journal of Technology in Education and Science*, *7*(2), 129–151. https://doi.org/10.46328/ijtes.471
88. Sulaiman, N., & Mahfar, M. (2024). Cyberbullying and its Relationship to Mental Health Issues among Adolescents. *International Journal of Academic Research in Progressive Education and Development*, *13*(4), Article 4. https://doi.org/10.6007/IJARPED/v13-i4/23722
89. The Society for Adolescent Health and Medicine. (2025). Guidelines on the Inclusion and Protection of Adolescent Minors and Young Adults in Health Research: A Position Statement of the Society for Adolescent Health and Medicine. *Journal of Adolescent Health*, *76*(5), 944–953. https://doi.org/10.1016/j.jadohealth.2025.02.007
90. Toyon, M. A. S. (2021). Explanatory sequential design of mixed methods research: Phases and challenges. *International Journal of Research in Business and Social Science (2147- 4478)*, *10*(5), 253–260. https://doi.org/10.20525/ijrbs.v10i5.1262
91. U.S. Department of Health & Human Services. Office for Human Research Protections (OHRP). (n.d.). *Informed Consent FAQs*. U.S. Department of Health & Human Services. HHS.Gov. Retrieved February 1, 2026, from https://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/informed-consent/index.html
92. Vasileiou, I., & Furnell, S. (2019). A Holistic View of Cybersecurity Education Requirements: In *Cybersecurity Education for Awareness and Compliance* (pp. 1–18). IGI Global. https://doi.org/10.4018/978-1-5225-7847-

5.ch001

93. Wachs, S., Bilz, L., Niproschke, S., & Schubarth, W. (2019). Bullying Intervention in Schools: A Multilevel Analysis of Teachers' Success in Handling Bullying From the Students' Perspective. *The Journal of Early Adolescence*, *39*(5), 642–668. https://doi.org/10.1177/0272431618780423
94. Wasti, S. P., Simkhada, P., Teijlingen, E. van, Sathian, B., & Banerjee, I. (2022). The Growing Importance of Mixed-Methods Research in Health. *Nepal Journal of Epidemiology*, *12*(1), 1175–1178. https://doi.org/10.3126/nje.v12i1.43633
95. Weijsenfeld, F. G. J., & Sarmah, D. K. (2025). Gamifying cybersecurity: A narrative-driven approach to teaching steganography. *Computers and Education Open*, *9*, 100288. https://doi.org/10.1016/j.caeo.2025.100288
96. Wekerle, C. (2024). Considerations for child protection and practice: What is child protection now? *Child Protection and Practice*, *1*, 100025. https://doi.org/10.1016/j.chipro.2024.100025
97. World Health Organization. (2019). Adolescent Health – the Missing Population in Universal Health Coverage. World Health Organization. https://cdn.who.int/media/docs/default-source/mca-documents/adolescents/adolescents-and-youth/adolescent-health-uhc-report_final-may-2019.pdf
98. Xenakis, A., Vlachos, V., Roig, P. J., & Alcaraz, S. (2024). Addressing the necessity of cybersecurity literacy: The case of ETTCS CyberTeach project. *Information and Computer Security*, *33*(3), 427–451. https://doi.org/10.1108/ICS-04-2024-0095
99. Yang, S., & Oh, E. (2024). Analysis of Children's Development Pathways based on Bronfenbrenner's Ecological Systems Theory. *International Journal of Education and Humanities*, *16*(3), 250–258. https://doi.org/10.54097/vaap3p97
100. Zohrabi, M. (2013). Mixed Method Research: Instruments, Validity, Reliability and Reporting Findings. *Theory and Practice in Language Studies*, *3*(2), 254–262. https://doi.org/10.4304/tpls.3.2.254-262