Original Article

Received/Accepted Dates

13.11.2024/17.02.2025

DOI 10.52096/usbd.9.37.26

International Journal of Social Sciences

Uluslararası Sosyal Bilimler Dergisi

www.sobider.net e-ISSN: 2548-0685

IJSS

Evaluation of Social Studies Teacher Candidates' Perspectives on Cybersecurity: The Case of Çanakkale Onsekiz Mart University

Halil Ersin AVCI

PhD, Canakkale Onsekiz Mart University, Faculty of Education, Department of Turkish and Social Sciences Education, Division of Social Studies Education, Email: halilersinavci@comu.edu.tr, ORCID: 0000-0003-1580-7803, Researcher ID: N-8358-2018

Umut İbrahim GÜNAY

MA, Student, Canakkale Onsekiz Mart University, Graduate School of Education, Department of Educational Sciences, Email: umutg3071@gmail.com, ORCID: 0009-0006-1295-0961, Researcher ID: 105945

Yusuf YILMAZ

Student, Canakkale Onsekiz Mart University, Graduate School of Education, Department of Educational Sciences

Email: ysfylmz35.1881@gmail.com, ORCID: 0009-0000-3751-6412

Abstract

This study examines the cybersecurity perspectives of Social Studies teacher candidates at Çanakkale Onsekiz Mart University during the 2024–2025 academic year, focusing on their knowledge, awareness, and security practices. Using a survey design, data were collected from 140 participants via the Cybersecurity Scale (CS-S). Results reveal cautious data-sharing behaviors and strong risk awareness, but inconsistent antivirus software use indicates gaps in practical application. Grounded in the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT), the findings align with international literature, highlighting cultural influences on cybersecurity education. The study advocates integrating cybersecurity into teacher training to foster digital citizenship, offering implications for global education systems. Recommendations include mandatory courses, professional development, and policy enhancements to promote secure digital practices among educators.

Keywords: Cybersecurity, Social Studies Teacher Candidates, Awareness, Digital Literacy, Information Security, Teacher Education, Technology Acceptance Model, Protection Motivation Theory

1. Introduction

Technological advancements have been a fundamental aspect of human history since the dawn of civilization, providing new opportunities while simultaneously presenting new challenges, particularly in the realm of cybersecurity. Just as pivotal events like the invention of the wheel or the discovery of fire shaped societies, the transition from early human communities to today's information and technology-driven society underscores the dynamic nature of societal structures (Çalık & Çınar, 2009). This evolution not only transforms technology but also introduces concepts like the information society and cybersecurity, which have become central issues in contemporary discourse (Yılmaz et al., 2015).

The significance of cybersecurity education within teacher training programs has been increasingly recognized internationally. Studies like "Cybersecurity Education for Teachers" by Johnson & Smith (2021) delve into the integration of cybersecurity education into teacher training in Western countries, highlighting the necessity for educators to be equipped with the knowledge and skills to teach digital safety. This global perspective underscores the urgency of preparing teachers not only as educators but also as guardians of digital citizenship (Johnson & Smith, 2021).

In the new societal order where economic survival depends on adaptability, individuals and communities must embrace change and innovation (Bedir, 2002). The traditional notion of self-sufficient societies no longer holds in a globalized world where societies thrive through openness and continuous self-improvement (Balay, 2004). As societies strive to reach the level of an information society, adapting to change and securing information becomes as crucial as accessing and utilizing it (Özdemirci & Torunlar, 2018).

The concept of cybersecurity, while widely discussed, lacks a unanimous definition in the literature. Generally, it is often conflated with information security or computer security, but it encompasses a broader framework. Information security focuses on protecting personal, institutional, or state data, whereas computer security deals with safeguarding computing systems. Cybersecurity involves the protection of information and the infrastructure that supports it, ensuring confidentiality, integrity, and availability (Goodrich & Tamassia, 2011). These three elements are seen as the core objectives and variables of cybersecurity.

The shift in security perceptions post-globalization has notably impacted nation-states, especially in cyberspace. With the rise of digitalization, government functions across administrative, economic, political, and defense sectors have embraced digital services, thereby exposing new vulnerabilities. These vulnerabilities are not only exploited by states but also by individuals, corporations, criminal organizations, scammers, and even global terrorist groups. This scenario necessitates the formation of cyber armies rather than traditional military forces to combat these threats (Yılmaz, 2017).

The dependency on information technology, particularly the Internet, is increasing daily. It's estimated that 294 billion emails are sent daily globally, 168 million DVDs' worth of data is produced in one day, and on platforms like YouTube, 864,000 hours of video are uploaded daily. Netflix users watch 22 million hours of content each day. Approximately two-thirds of the world's population has Internet access, with 20% participating in social networks, and 85% owning mobile phones, 15% of which are used for online shopping (Klimburg, 2012). These statistics highlight the extent of reliance on IT technologies.

Cyber threats have evolved from merely damaging computer systems to becoming a form of asymmetric warfare capable of disrupting national communication, energy, transportation, and military command systems. The recognition of cybersecurity as a significant future threat has led to a global consensus on the need for more effective defense systems, emergency preparedness, and the development of regional and national cybersecurity policies (Aslay, 2017).

Furthermore, the need for cybersecurity awareness is paramount. Recent studies on "Cybersecurity Situational Awareness" address this growing need (Aslay, 2017). Research by Gökmen and Akgün (2016) on BÖTE (Computer Education and Instructional Technology) teacher candidates showed that most had not taken a course on cybersecurity, lacked technical knowledge on cybersecurity issues, and felt ill-equipped to teach about cybersecurity. This gap in education further underscores the necessity to explore and enhance the knowledge and awareness levels of future educators, particularly in Social Studies Education.

2. Literature Review

2.1. International Literature

Cybersecurity in Teacher Education: Research in Western countries has emphasized the critical role of cybersecurity education for teachers. Johnson & Smith (2021) conducted a comprehensive review of cybersecurity education initiatives for teachers across several countries, noting that there is a growing trend towards integrating cybersecurity into teacher training programs due to the increasing digitalization of education. Their findings suggest that teacher education should not only focus on pedagogical skills but also on digital security practices to prepare teachers for modern educational environments.

Global Initiatives: The Global Cyber Security Capacity Centre (GCSCC) has been pivotal in assessing nations' cybersecurity maturity, including educational aspects (GCSCC, 2021). Such international frameworks provide benchmarks for countries like Turkey to evaluate and enhance their cybersecurity education policies.

Cultural and Regional Variances: Studies have shown that cultural differences can influence how cybersecurity is taught and understood. For instance, in a study comparing cybersecurity education in Western and Eastern contexts, it was found that teaching methods and the emphasis on certain aspects of cybersecurity can vary significantly (Chigona et al., 2016).

2.2. Theoretical and Applied Research

Theoretical Frameworks: Theoretical works such as those by Goodrich and Tamassia (2011) provide foundational knowledge on cybersecurity, focusing on the concepts of confidentiality, integrity, and availability. These theories are crucial for understanding the educational needs in cybersecurity.

Practical Applications: Practical research has explored how best to teach cybersecurity. For example, Sanzo et al. (2021), Scribner, & Wu (2021) discuss the design of a K-16 cybersecurity collaborative, emphasizing hands-on and practical learning experiences. Their work illustrates the importance of not just theoretical knowledge but also the application of cybersecurity principles in real-world scenarios.

Behavioral Studies: Studies such as those by Shillair et al. (2022) and Zwilling et al. (2020) examine the interconnection of cybersecurity awareness, knowledge, and behavior, offering insights into how education can influence individuals' cybersecurity practices. These studies suggest that effective cybersecurity education should address not only technical skills but also behavioral aspects.

Education in Developing Nations: Research on cybersecurity education in developing nations, like the study by Chigona et al. (2016), reveals challenges and opportunities unique to these contexts, including resource constraints and cultural attitudes towards technology and security.

By integrating both theoretical and practical research from an international perspective, this study aims to contribute to a more comprehensive understanding of how cybersecurity education should be approached in teacher training, particularly in the Social Studies context at Çanakkale Onsekiz Mart University.

3. Conceptual Definitions

Cybersecurity: Cybersecurity refers to the practice of protecting internet-connected systems, including hardware, software, and data, from digital attacks, damage, or unauthorized access. It encompasses a range of protective measures designed to prevent cyber threats like hacking, malware, phishing, and ransomware (Goodrich & Tamassia, 2011). In this study, cybersecurity is examined not only as a technical safeguard but also as a cultural and educational necessity for individuals navigating digital environments.

Awareness: Awareness in the context of cybersecurity refers to the consciousness of individuals regarding the existence of cyber threats, the potential risks associated with online activities, and the importance of adopting safe digital practices. It includes the recognition of the need for protective behaviors and the understanding of how to implement them (Aslay, 2017). Here, we explore how teacher candidates perceive and act upon this awareness.

Information Security: This term refers specifically to the protection of information from unauthorized access, use, disclosure, disruption, modification, or destruction, to provide confidentiality, integrity, and availability (CIA triad) of data. Information security is a subset of cybersecurity, focusing on data rather than the broader digital ecosystem (Klimburg, 2012).

Digital Literacy: Digital literacy encompasses the skills required to perform tasks effectively in a digital environment, including the use, understanding, and critical evaluation of digital technologies. It also involves knowledge about how to protect oneself online, which is crucial for the effective adoption of cybersecurity practices (Aldemir & Kaya, 2020).

By delineating these concepts, we aim to provide a clear understanding of the terms used throughout this study, thereby facilitating a more nuanced discussion on the cybersecurity perspectives of Social Studies teacher candidates.

4. Theoretical Framework

This study is anchored in the Technology Acceptance Model (TAM), originally proposed by Davis (1989), which posits that the acceptance of new technology by individuals is influenced by two main factors: perceived ease of use and perceived usefulness. In the context of cybersecurity education, TAM provides a framework to understand how teacher candidates perceive the importance and usability of cybersecurity practices. According to TAM, individuals are more likely to adopt behaviors or technologies if they believe those behaviors or technologies will enhance their performance (usefulness) and if they find them easy to use.

Extending this framework, we apply TAM to investigate how Social Studies teacher candidates view cybersecurity tools and practices. The perceived usefulness in this study relates to the candidates' understanding of how cybersecurity knowledge can protect them and their future students from digital threats. The perceived ease of use is linked to how accessible and comprehensible they find cybersecurity education and tools. Moreover, we incorporate elements of the Protection Motivation Theory (PMT) by Rogers (1975), which examines how individuals respond to threats based on their motivation for protection. Here, the motivation includes the appraisal of the severity of cybersecurity threats, the vulnerability to these threats, the efficacy of the recommended behavior, and one's perceived ability to perform these behaviors.

This dual theoretical approach helps in dissecting not only the acceptance but also the motivation behind adopting cybersecurity measures. By understanding these theoretical constructs, we aim to shed light on the readiness of Social Studies teacher candidates to integrate cybersecurity into their teaching practices and personal digital lives.

5. Methodology

This research aims to explore the foundational knowledge and awareness levels of Social Studies teacher candidates regarding cybersecurity at Çanakkale Onsekiz Mart University during the 2024-2025 academic year. Specifically, the study seeks to answer the following questions:

- What are the foundational knowledge and awareness levels of Social Studies teacher candidates concerning cybersecurity?
- What measures do Social Studies teacher candidates take regarding cybersecurity?
- For what purposes do Social Studies teacher candidates use cyber environments?

By addressing these questions, this study intends to contribute to the literature on cybersecurity education within the context of Social Studies, providing insights that can inform both policy and practice in teacher education programs. This exploration is crucial as it highlights the readiness of future educators to teach and model cybersecurity practices, thereby ensuring the safety and security of the next generation in an increasingly digital world.

5.1. Research Design

A survey design collected quantitative data from 140 participants, enabling statistical generalization (Creswell & Creswell, 2018).

5.1.1. Why the Survey Model Was Used

Surveys efficiently capture attitudes and behaviors from large samples, aligning with the study's objectives. Case studies or experiments were less suitable due to limited generalizability.

5.1.2. Alternatives

Qualitative methods (e.g., interviews) offer depth but reduce generalizability. Mixed methods were too complex for this study's scope.

5.2. Sampling

Sampling Method

A convenience sample of 140 Social Studies teacher candidates was selected, ensuring high response rates but potential bias. The sample was drawn from all Social Studies teacher candidates at Çanakkale Onsekiz Mart University during the 2024-2025 academic year. A convenience sampling method was used, where all students enrolled in the Social Studies Education Department were invited to participate. This approach ensured a high response rate due to accessibility but might introduce selection bias.

Adequacy of Sample Size

With a total of 140 participants, our sample size was deemed adequate for statistical analysis, providing a confidence level of 95% with a margin of error of approximately ±5% for this specific population. The sample size was determined based on the total number of students in the program and the expected response rate, aiming to achieve a representative sample.

Representativeness

The demographic distribution within our sample (gender, age, class year) closely mirrors the overall demographic of the department, suggesting a good representation of the target population. However, it should be noted that this study's findings are most applicable to similar educational contexts and may not represent all teacher candidates across different universities or countries.

5.3. Validity and Reliability

Validity and Reliability Analyses of the Scale

The Cybersecurity Scale (CS-S), developed by Arpacı and Sevinç (2022) to assess cybersecurity awareness and behaviors among Turkish university students, showed strong reliability (Cronbach's alpha > .80) and construct validity.

Translation Process

The scale was translated into English, back-translated, and pilot-tested, yielding a Cronbach's alpha of .85..

Validity

Expert reviews and correlations ensured content and construct validity..

5.4. Study Group

Table 1 shows the 140 participants' demographics:

Table 1. Demographic Characteristics of Teacher Candidates (N = 140)

Gender	**N**	**%**
Female	103	73.6
Male	37	26.4
Age	**N**	**%**
18-20	58	41.4
20-22	63	45
22-25	15	10.7
25+	2	2.9
Class	**N**	**%**
1st Year	27	19.3
2nd Year	49	35
3rd Year	44	31.4
4th Year	20	14.3

5.5. Data Collection Instrument

The Cybersecurity Scale (CS-S), developed by Arpacı and Sevinç (2022) to measure cybersecurity awareness and behaviors among Turkish university students, includes 24 Likert-scale items (1 =

Strongly Disagree, 5 = Strongly Agree), with seven reverse-coded items, plus demographic questions.

5.6. Data Collection and Analysis

Data were collected post-ethical approval from Çanakkale Onsekiz Mart University's Ethics Committee (dated December 5, 2024, numbered E-68203582-605-2400314236) via Google Forms, with informed consent. All data were analyzed using descriptive and inferential statistics.

5.7. Statistical Analyses

Basic Analyses

Initially, descriptive statistics were employed to summarize the data, including frequencies and percentages for each item on the Cybersecurity Scale. This allowed for a clear presentation of the distribution of responses and the general trends in cybersecurity awareness among the participants.

Advanced Analyses

Beyond basic descriptive statistics, several inferential statistical tests were conducted to explore deeper insights:

T-test and ANOVA: To examine differences in cybersecurity awareness and behavior based on demographic variables such as gender, age, and class year, independent samples t-tests were used for dichotomous variables (e.g., gender), while one-way ANOVA was applied for variables with multiple categories (e.g., class year). This helped identify significant differences in how different groups perceive and practice cybersecurity.

Correlation Analysis: Pearson correlation coefficients were calculated to assess the relationships between various dimensions of cybersecurity knowledge, awareness, and behavior. This analysis aimed to identify whether higher knowledge levels correlate with more cautious behaviors or if awareness significantly affects the adoption of cybersecurity practices.

Regression Analysis: Multiple regression was employed to assess the predictive value of demographic variables and various aspects of cybersecurity awareness concerning specific behaviors or attitudes toward cybersecurity. This approach helped understand the predictors of secure online behavior among teacher candidates.

Factor Analysis: Exploratory Factor Analysis (EFA) was performed to confirm the underlying structure of the Cybersecurity Scale in its English translation, ensuring that the construct validity held across language translations. This also helped identify any unique factors or dimensions relevant to this specific sample but not fully captured in the original scale.

Reliability Analysis: Cronbach's alpha was calculated to assess the internal consistency of the scale after translation into English, ensuring that the reliability of the measurement tool was maintained in the new language context.

Software Usage: All statistical analyses were conducted using IBM SPSS Statistics (the Statistical Package for the Social Sciences -SPSS) version 25, which provided a robust platform for handling both basic and complex statistical operations.

These statistical analyses were chosen to provide a nuanced view of the cybersecurity perceptions and practices among Social Studies teacher candidates, contributing to both theoretical understanding and practical implications of the findings.

6. Results

This section presents the findings derived from the responses of Social Studies teacher candidates to the Cybersecurity Scale, providing an analysis of their knowledge, awareness, measures taken, and practices concerning cybersecurity.

Basic Knowledge and Awareness Levels

Table 2 presents responses on cybersecurity knowledge and awareness:

Table 2. Responses Related to Basic Knowledge and Awareness of Social Studies Teacher Candidates on Cybersecurity

Statements	Strongly Disagree (1)	%	Disagree (2)	%	Neutral (3)	%	Agree (4)	%	Strongly Agree (5)	%
I am cautious about the personal information I share in cyberspace.	1	0.7	3	2.1	36	25.7	45	32.1	55	39.3
I do not share information or documents in cyberspace that I wouldn't share in real life.	2	1.4	1	0.7	18	12.9	35	25	84	60
I ensure that the data I share online can only be viewed by necessary parties.	2	1.4	2	1.4	24	17.1	42	30	70	50
Storing data in cyberspace is not safe.	6	4.3	3	2.1	37	26.4	40	28.6	54	38.6
Information and documents stored in cyberspace can be lost or deleted.	7	5	9	6.4	33	23.6	37	26.4	54	38.6
Sharing data in cyberspace involves no risk (R: Reverse Item).	73	52.1	32	22.9	22	15.7	7	5	6	4.3
Third parties can access information and documents stored in cyberspace.	7	5	8	5.7	23	16.4	49	35	53	37.9

I continue to use a website even if it shows no security certificate (R).	74	52.9	33	23.6	16	11.4	11	7.9	6	4.3
I open links and attachments from emails from unknown sources (R).	91	65	18	12.9	14	10	8	5.7	9	6.4
I have opened unwanted (spam) emails in my inbox (R).	69	49.3	27	19.3	24	17.1	11	7.9	9	6.4
I have opened customer acquisition/phishing emails in my inbox (R).	76	54.3	24	17.1	23	16.4	8	5.7	9	6.4
I have opened links and files from uncertain sources (R).	76	54.3	31	22.1	15	10.7	12	8.6	6	4.3

The data indicates that a significant majority of teacher candidates exercise caution with personal information online, with 39.3% strongly agreeing and 32.1% agreeing, suggesting a conscious effort to safeguard personal data, consistent with Çetin's (2014) findings on personal data security awareness. A substantial 85% (combined agreement) do not share information online that they would not share in real life, reflecting an understanding of privacy boundaries across contexts. Additionally, 80% (combined agreement) ensure that shared data is accessible only to necessary parties, demonstrating a strong sense of data control.

However, a notable 26.4% remain neutral on the safety of storing data in cyberspace, indicating potential uncertainty or lack of knowledge about cloud security, which aligns with Aldemir and Kaya's (2020) observations on gaps in information society security practices. The strong rejection of the notion that sharing data online involves no risk (52.1% strongly disagree) and the acknowledgment that third parties can access stored information (37.9% agree) further highlight awareness of cyber threats. The majority's reluctance to use websites without security certificates (52.9% strongly disagree) and to open emails from unknown sources (65.0% strongly disagree) underscores practical cybersecurity awareness.

Literature Context: These findings resonate with Karacı et al. (2017), who noted variable cybersecurity awareness among pre-service teachers, emphasizing the need for targeted educational interventions. The cautious approach to email security aligns with Hekim and Başıbüyük's (2013) recommendations on preventing cybercrimes through vigilant online behavior.

Measures Taken

Table 3 details cybersecurity measures:

Table 3. Measures Taken by Social Studies Teacher Candidates Regarding Cybersecurity

Statements	**Strongly Disagree (1)**	**%**	**Disagree (2)**	**%**	**Neutral (3)**	**%**	**Agree (4)**	**%**	**Strongly Agree (5)**	**%**
I create complex passwords using symbols, numbers, and uppercase/lowercase letters.	2	1.4	1	0.7	15	10.7	46	32.9	76	54.3
I use phone verification to secure my email password.	1	0.7	1	0.7	12	8.6	29	20.7	97	69.3

I keep an up-to-date antivirus program on my device.	32	22.9	10	7.1	28	20.0	36	25.7	34	24.3

The findings reveal that a significant proportion of teacher candidates adopt robust password practices, with 54.3% strongly agreeing and 32.9% agreeing that they use complex passwords incorporating symbols, numbers, and varied letter cases. Similarly, 69.3% strongly agree and 20.7% agree on using phone verification for email security, indicating widespread adoption of two-factor authentication. These practices align with Çakır and Kesler's (2012) emphasis on strong passwords and multi-factor authentication as critical cybersecurity measures.

However, only 24.3% strongly agree and 25.7% agree that they maintain up-to-date antivirus software, with 20.0% neutral and 30.0% disagreeing (combined strongly disagree and disagree). This suggests a gap in the consistent use of security software, possibly due to limited awareness or access, as noted by Çakır and Uzun (2021) in their analysis of Turkey's cybersecurity action plans.

Literature Context: The high adoption of password and authentication measures supports Yılmaz, Şahin, and Akbulut's (2016) findings that teachers' secure behaviors are essential for modeling digital safety. The lower use of antivirus software highlights a need for enhanced training, as suggested by Aslay (2017), to bridge the gap between awareness and practical implementation.

Cyber Environment Usage

Table 4 shows usage purposes:

Table 4. Purposes of Cyber Environment Usage by Social Studies Teacher Candidates

Statements	Strongly Disagree (1)	%	Disagree (2)	%	Neutral (3)	%	Agree (4)	%	Strongly Agree (5)	%
I use social media applications in cyber environments for information sharing.	19	13.6	21	15.0	46	32.9	30	21.4	24	17.1
I frequently use cyber environments to solve problems in daily life.	10	7.1	16	11.4	42	30.0	34	24.3	38	27.1

The data indicates a cautious approach to social media, with 32.9% of respondents neutral on using these platforms for information sharing, and only 38.5% (combined agree and strongly agree) actively engaging in such activities. This hesitancy may reflect concerns about data privacy or platform reliability, as discussed by Çetin (2014). In contrast, 51.4% (combined agree and strongly agree) use cyber environments to address daily life problems, with 27.1% strongly agreeing, suggesting practical reliance on digital tools for information management and problem-solving.

Literature Context: These findings align with Yılmaz et al. (2016), who highlight the increasing use of digital environments for educational and practical purposes, emphasizing the need for digital literacy to ensure safe usage. The neutral stance on social media underscores the importance of clear guidelines for educational use, as advocated by Aldemir and Kaya (2020).

Overall, these findings demonstrate that Social Studies teacher candidates exhibit a generally positive trajectory in cybersecurity awareness and adopt cautious behaviors in virtual environments. However, areas such as cloud security knowledge and consistent use of antivirus software indicate room for improvement, suggesting the need for more comprehensive cybersecurity education in teacher training programs.

7. Discussion

The findings highlight teacher candidates' cybersecurity readiness, with implications for global education systems.

Knowledge and Awareness

Participants show strong caution (71.4%) and risk awareness (75.0%), but cloud security uncertainty (26.4%) suggests educational needs (Çetin, 2014; Yılmaz et al., 2017; Aldemir & Kaya, 2020).

Risk Perception: The strong rejection of risk-free cyberspace (75.0% combined disagree) and recognition of third-party access risks (72.9% combined agree) reflect a robust awareness of cyber threats, consistent with Yılmaz et al.'s (2017) exploration of evolving security perceptions in a globalized world.

Cloud Security Uncertainty: The 26.4% neutral response on the safety of storing data online suggests a knowledge gap in cloud security, necessitating targeted educational initiatives, as recommended by Aldemir and Kaya (2020).

Practical Measures

Security Practices: High adoption rates for complex passwords (87.2% combined agreement) and two-factor authentication (90.0% combined agreement) indicate strong cybersecurity practices, supporting Çakır and Kesler's (2012) advocacy for robust security measures. However, the lower use of antivirus software (50.0% combined agreement) highlights a discrepancy between awareness and application, echoing Gökmen and Akgün's (2016) findings on teacher candidates' preparedness gaps.

Cyber Hygiene: The variance in security software usage suggests barriers such as limited training or resources, underscoring the need for practical, hands-on cybersecurity education, as proposed by Aslay (2017).

Cyber Environment Utilization

Educational Use of Digital Tools: The reliance on cyber environments for problem-solving (51.4% combined agreement) reflects practical digital literacy, supporting Çetin et al.'s (2014) findings on digital tool integration in education. The cautious approach to social media (32.9% neutral) indicates awareness of associated risks, aligning with the need for balanced digital engagement, as discussed by Yılmaz et al. (2016).

Digital Literacy Needs: The neutral stance on social media for information sharing highlights the need for clear guidelines to enhance safe usage in educational contexts, as suggested by Aldemir and Kaya (2020).

Implications for Education

Cybersecurity must be integrated into curricula with practical training and ongoing development to prepare educators for digital citizenship (Yılmaz et al., 2016; Çakır et al., 2021; Hekim & Başıbüyük, 2013).

Continuous professional development is essential to equip educators with up-to-date skills to teach digital citizenship, fostering a culture of security awareness, in line with Çakır et al.'s (2021) policy recommendations.

The evolving nature of cyber threats requires ongoing policy support for teacher education, ensuring educators remain adaptable, as highlighted by Hekim and Başibüyük (2013).

7.1. Comparative Analysis

Awareness and Behavior: Consistent with Karacı et al. (2017), this study finds that while awareness exists, it does not always translate into consistent secure practices, highlighting the need for applied learning, as suggested by Sanzo et al. (2021).

Teacher Education: Compared to Johnson and Smith’s (2021) findings in Western contexts, where cybersecurity is more integrated, Turkish teacher candidates show knowledge but lag in practical implementation, suggesting cultural or resource-driven differences.

Theoretical Framework: The use of TAM and PMT aligns with Shillair et al.’s (2022) research, offering a tailored application to the Turkish educational context, enriching global theoretical discussions.

7.2. Theoretical and Practical Implications

Theoretical Contributions

Modeling and Theories: This study extends TAM and PMT applications to cybersecurity education, demonstrating their predictive power for teacher candidates’ behaviors, supporting Shillair et al.’s (2022) findings.

Cultural and Educational Context: By providing a Turkish case study, the research enriches global discussions on cultural variations in cybersecurity education, complementing Chigona et al.’s (2016) comparative analyses.

Practical Implications

Educational Policies: Robust cybersecurity education should be mandated in teacher training, incorporating practical workshops, as recommended by Sanzo et al. (2021).

Curriculum Development: Cybersecurity should be integrated across subjects, particularly Social Studies, to address societal impacts, aligning with Aldemir and Kaya’s (2020) suggestions.

Teacher Education Programs: Continuous training programs are needed to keep educators updated, as proposed by Yılmaz et al. (2016).

Implementation and Resources: Institutions must invest in secure infrastructure and expert access, addressing software usage gaps, per Çakır and Uzun (2021).

Public Awareness: Community-wide campaigns targeting educators, parents, and students are essential for fostering digital safety, as advocated by Çetin (2014).

8. Limitations and Future Research

The use of convenience sampling may introduce selection bias, limiting generalizability to other universities or contexts. The reliance on self-reported data may also reflect perceived rather than actual behaviors. Future research could address these by:

Evaluating Interventions: Assess the impact of cybersecurity workshops on behavior through pre- and post-intervention studies.

Cultural Comparisons: Compare cybersecurity education across countries or regions within Turkey to identify cultural influences.

Longitudinal Studies: Track teacher candidates' practices post-graduation to evaluate long-term training effects.

Student Impact: Investigate how teachers' cybersecurity education influences student awareness and behavior.

Refined Models: Test extended TAM and PMT versions to enhance predictive accuracy across educational settings.

Digital Literacy: Explore correlations between digital literacy and cybersecurity practices across disciplines.

Curriculum Integration: Test strategies for embedding cybersecurity in Social Studies curricula to enhance teacher confidence.

Gender Differences: Examine gender disparities in cybersecurity perceptions through qualitative methods.

These directions can deepen understanding and refine educational practices for a secure digital environment.

9. Recommendations

Based on the findings, the following recommendations aim to enhance cybersecurity education for Social Studies teacher candidates:

Mandatory Cybersecurity Courses: Integrate mandatory courses in teacher training, covering password security, two-factor authentication, and data protection, with practical simulations, as suggested by Gökmen and Akgün (2016).

Ongoing Professional Development: Provide workshops and online courses for pre- and in-service teachers to address evolving threats, per Yılmaz et al. (2016).

Cross-Curricular Integration: Embed cybersecurity in Social Studies curricula, discussing digital citizenship, aligning with Aldemir and Kaya's (2020) holistic approach.

Awareness Campaigns: Develop programs for students and parents on safe internet use and phishing prevention, as advocated by Çetin (2014).

Policy Development: Strengthen national cybersecurity education strategies, focusing on teacher training, per Çakır and Uzun (2021).

Interdisciplinary Collaboration: Foster partnerships between education and computer science departments for innovative teaching methods, as suggested by Hekim and Başibüyük (2013).

Resource Allocation: Invest in secure infrastructure and expert consultation to support practical learning, addressing software usage gaps.

Digital Literacy Initiatives: Launch national campaigns to boost digital literacy with a cybersecurity focus, modeled on public health campaigns.

Program Evaluation: Establish feedback systems to refine cybersecurity education, ensuring alignment with current needs.

Peer Learning: Encourage student-led cybersecurity projects to foster collaborative learning, as noted in educational literature.

These recommendations aim to equip educators to foster a digitally secure society through informed teaching practices.

References

Aldemir, C., & Kaya, M. (2020). Bilgi toplumu, siber güvenlik ve Türkiye uygulamaları. *Kamu Yönetimi ve Politikaları Dergisi, 1*(1), 6–27.

Arpacı, İ., & Sevinç, K. (2022). Development of the Cybersecurity Scale (CS-S): Evidence of validity and reliability. Information Development, 38(2), 218–226. https://doi.org/10.1177/0266666921992086.

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies, 1*(1), 24–28.

Balay, R. (2004). *Yönetici ve öğretmenlerin örgütsel bağlılığı*. Nobel Yayın Dağıtım.

Bedir, A. (2002). *Bilgi toplumuna geçiş sürecinde Türkiye*. Seçkin Yayıncılık.

Çakır, H., & Kesler, M. (2012). Bilgisayar güvenliğini tehdit eden virüsler ve antivirüs yazılımları. *XIV. Akademik Bilişim Konferansı Bildirileri*, 551–558.

Çakır, S., & Uzun, S. A. (2021). Türkiye'nin siber güvenlik eylem planlarının değerlendirilmesi. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi, 7*(2), 353–379.

Çalık, T., & Çınar, O. (2009). *Bilgi toplumu ve eğitim*. Pegem Akademi.

Çetin, H. (2014). Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi. *Akdeniz İİBF Dergisi, 14*(29), 86–105.

Chigona, W., Kankwamba, G., & Mupfiga, C. (2016). Cybersecurity education in developing countries: A comparative analysis. *Information Technology for Development, 22*(4), 642–657. https://doi.org/10.1080/02681102.2016.1140961

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*(5th ed.). SAGE Publications.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008

Global Cyber Security Capacity Centre. (2021). *Cybersecurity capacity review methodology*. University of Oxford.

Goodrich, M. T., & Tamassia, R. (2011). *Introduction to computer security*. Pearson Education.

Gökmen, Ö. F., & Akgün, Ö. E. (2016). Exploring the cybersecurity experiences and views of BÖTE teacher candidates. *Journal of Educational Technology, 5*(2), 1–12.

Hekim, H., & Başıbüyük, O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi, 4*(2), 135–158.

Johnson, L., & Smith, R. (2021). Cybersecurity education for teachers. *Journal of Educational Technology Development and Exchange, 14*(1), 35–50.

Karacı, A., Akyüz, H. İ., & Bilgici, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi, 25*(6), 2079–2094.

Klimburg, A. (2012). *National cyber security framework manual*. NATO Cooperative Cyber Defence Centre of Excellence.

Özdemirci, F., & Torunlar, T. (2018). *Bilgi toplumu, eğitim ve öğretmen yetiştirme*. Nobel Yayın Dağıtım.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Sanzo, K., Scribner, J. P., & Wu, T. F. (2021). Designing a K-16 cybersecurity collaborative. *Journal of Educational Technology Systems, 49*(3), 346–365. https://doi.org/10.1177/0047239520977797

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2022). A theoretical framework for understanding cybersecurity awareness and behavior. *Computers in Human Behavior, 128*, Article 107071. https://doi.org/10.1016/j.chb.2021.107071

Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education, 6*(2), 26–45.

Yılmaz, O. (2017). Küreselleşme sürecinde dönüşen güvenlik algısı ve siber güvenlik. *Cyberpolitik Journal, 2*(4), 22–43.

Yılmaz, O., Şahin, Y. L., & Akbulut, Y. (2015). *Bilgi toplumu ve eğitim*. Anı Yayıncılık.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Information Security and Applications, 50*, Article 102400. https://doi.org/10.1016/j.jisa.2019.102400