

Shaping Awareness, Competence, and Application of Digital Security in Teacher Learning: A Systematic Literature Review

Yudi Setiawan, Ade Gafar Abdullah*, Haipan Salam

Universitas Pendidikan Indonesia, Bandung, Indonesia

*Corresponding Email: ade_gaffar@upi.edu

ARTICLE INFO

Article history

Received: Apr 21, 2026

Revised: Jun 02, 2026

Accepted: Jun 04, 2026

Keywords

Digital Security

Teacher Competence

Cybersecurity Awareness

Professional Development

Systematic Review

ABSTRACT

This systematic literature review examined teachers' digital security awareness, competencies, and implementation practices in educational settings. Guided by PRISMA and the PICOCs framework, the study analyzed publications from Scopus and Google Scholar between 2012 and 2024. Of 526 identified records, 47 studies met the inclusion criteria and passed quality assessment. The findings showed that teachers generally possessed adequate awareness of basic digital security threats, such as viruses and phishing, but had limited understanding of advanced security practices. Three key competency domains were identified: technical knowledge, pedagogical skills, and professional attitudes. The implementation of digital security in teaching was often inconsistent due to inadequate training, limited resources, and insufficient institutional support. A significant gap remained between teachers' awareness and their practical application of security measures. The review highlights the importance of targeted professional development and stronger institutional support to improve digital security literacy and educational practice among teachers.

This is an open access article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Introduction

The rapid advancement of information and communication technology (ICT) has precipitated transformative changes across societal sectors, including education Lavicza et al (2022). Within this digital landscape, educators and students now access diverse online learning resources, engage in

virtual communication, and transcend geographical limitations, significantly altering the educator's role Otts et al (2021). However, this ICT integration concurrently introduces significant cybersecurity risks. As the proliferation of internet-connected devices and the volume of shared data escalate, ensuring digital security has emerged as a critical imperative for educational institutions García-Peñalvo (2021). Digital security is essential for safeguarding sensitive personal information, preserving digital asset integrity, and mitigating cyber threats.

For educators, digital security literacy encompassing requisite knowledge, competencies, and the application of best practices is paramount to protect themselves, their students, and the broader educational environment from risks including data breaches, malware, and other cyberattacks Stobert et al (2018). Understanding educators' perceptions and levels of digital security awareness is foundational for developing effective strategies to promote robust cyber hygiene practices. As primary handlers of information within educational systems, teachers' awareness and comprehension of cybersecurity principles are indispensable Bacak et al (2022). Investigating educators' perceptions regarding digital security is crucial to identify gaps and challenges hindering the adoption of optimal security practices Chou and Chou (2016). Furthermore, examining factors influencing these perceptions such as prior training, technological proficiency, and institutional support structures can inform targeted interventions to foster a culture of cyber resilience within educational frameworks Sánchez-Cruzado et al (2021).

Digital security encompasses the protection of information and digital assets against unauthorized access, use, disclosure, disruption, modification, or destruction. It comprises a comprehensive suite of practices and technologies designed to ensure the confidentiality, integrity, and availability (CIA triad) of data and digital systems Singh (2002). Establishing a robust digital security posture requires fostering a proactive and responsible culture, thereby contributing to a more accountable and trustworthy digital environment Maathuis and Chockalingam (2022). Digital security is intrinsically linked to cybersecurity, which specifically addresses the protection of internet-connected systems, networks, and devices from malicious cyber threats Schiliro (2023). Organizations must therefore adopt clearly defined strategies for effective digital security risk management, including encryption protocols, access controls, firewalls, intrusion detection and prevention systems, and comprehensive security policies (Ghauri, 2021; Gorodianska, 2021).

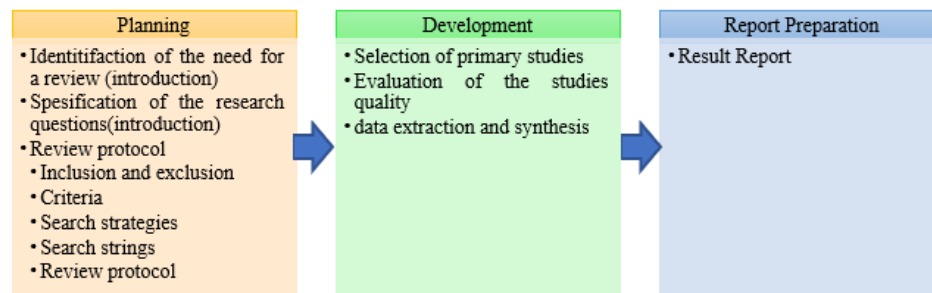
Existing research underscores the critical importance of digital security in educational settings; however, a significant gap persists in understanding educators' perceptions of digital security and the requisite competencies for addressing cybersecurity challenges within classrooms (Arsenovych,

2022; Petrov et al., 2022). Empirical findings indicate that many educators lack sufficient awareness of digital security risks and possess inadequate competencies to effectively safeguard themselves and their students against cyber threats (Guerrero et al., 2019; Pencheva et al., 2020). This competency deficit can precipitate serious consequences, including personal data breaches, disruptions to instructional continuity, and violations of privacy regulations and legal standards Sapanca and Kanbul (2022). Furthermore, despite the widespread adoption of digital technologies in curricula and instructional methodologies, the mechanisms by which educators embed digital security principles into their pedagogical practices remain poorly understood (Gallego et al., 2019; Guerrero et al., 2019; Torres-Hernández and Gallego, 2023). Educators frequently encounter barriers to effective technology integration, often attributable to insufficient professional development, limited institutional support, and resource constraints (Akram et al., 2022; Pérez-Sánchez et al., 2022).

A comprehensive systematic literature review (SLR) is required to address this gap through the synthesis of extant findings and identification of areas warranting further investigation. This SLR aims to advance understanding of educators' perceptions regarding digital security, the competencies essential for addressing cybersecurity challenges, and the integration of digital security practices within educational environments. By critically analyzing relevant empirical research, the review seeks to delineate the current landscape, identify emergent trends, and formulate evidence-based recommendations for both future scholarship and educational practice. This SLR is guided by three research questions: (1) What perceptions and conceptual understandings of digital security do educators hold? (2) Which digital security competencies are essential for educators? (3) How is digital security implemented within pedagogical processes? Addressing these questions contributes significantly to the fields of vocational education and educational technology, providing critical insights into digital security's role in education and informing the development of targeted strategies to enhance digital security awareness, competencies, and implementation practices among educators.

Method

This systematic literature review was conducted in accordance with the methodological guidelines established by (Kitchenham et al., 2009; Petersen et al., 2015; Sinoara et al., 2017). The research process comprised three sequential phases: Planning, Development, and Results Preparation, as depicted in Figure 1.

**Fig 1:** Three-stage systematic review research process.**Phase 1: Planning****a. Review Protocol**

To establish the scope of the systematic review, the PICOCS (Population, Intervention, Comparison, Outcomes, Context, Study Design) method proposed by Kitchenham et al (2009) was employed. Table 1 presents the PICOCS framework applied in this review.

Table 1. PICOCS Framework Applied in This Review

<i>PICOCS Component</i>	<i>Criteria</i>
Population (P)	Teachers globally
Intervention (I)	Interventions related to digital security aimed at teachers
Comparison (C)	No specific comparison; teachers' perceptions, competencies, and application of digital security were categorized and synthesized
Outcomes (O)	Perception, competence, and application of teacher digital security competence in learning
Context (C)	Digital security competency of teachers globally
Study Design (S)	Relevant studies (quantitative, qualitative, or mixed methods)

b. Inclusion and Exclusion Criteria

To select the most relevant studies for answering the research questions, explicit inclusion and exclusion criteria were established prior to the search, as outlined in Table 2.

Table 2. Inclusion and Exclusion Criteria

<i>Criterion</i>	<i>Description</i>
Time span	2012–2024
Inclusion Criteria	English-language documents; published in peer-reviewed journals, conference proceedings, or book series; observational studies; final publications; documents that address the research questions; focus on digital security for teachers
Exclusion Criteria	Documents not related to the research questions; non-English language; duplicate records; incomplete attributes; non-final versions; title and content irrelevant to digital security in teacher education

c. Search Strategy

Two academic databases were selected for the search: Scopus and Google Scholar. The search was conducted through the second week of April 2024. These databases were chosen for their relevance to the field and coverage of educational technology and cybersecurity research. Keywords were combined using the Boolean operators AND and OR, and an asterisk (*) was applied to include singular and plural forms. Customized search strings for each database are presented in Table 3. The review protocol was validated by a professor in the field of vocational technology education (the second author) to ensure transparency and rigor (Page and Moher, 2017; Perestelo, 2013). The data are displayed in Table 3 and 3a.

Table 3. Database Search Strings

Database	Search String
Scopus	(AI OR digital* OR literac* OR competence* OR ability* OR skill* AND security* OR safet* AND education* OR teacher* OR teaching* OR stud* OR voca*, online* OR AI OR digital AND competence* OR ability* OR skill* OR literac* AND security* OR safet* AND education)
Google Scholar	((("perception of teachers" OR "teacher's understanding") AND "digital security"); ("digital security competence" AND "teacher"); ("implementation of digital security" AND "learning" AND "teacher"))

Table 3a. Specific Keywords Used in Database Searches

Database	Keyword Category	Keywords Applied
Scopus	Population	teacher*, education*, stud*, voca*
	Intervention / Domain	digital*, AI, literac*, competence*, ability*, skill*, online*
	Outcome	security*, safet*
	Perception	"perception of teachers", "teacher's understanding"
Google Scholar	Competence	"digital security competence", "digital security"
	Application	"implementation of digital security", "learning", "teacher"

Boolean operators AND and OR were used to combine terms; an asterisk (*) captured variant word forms (e.g., teacher* retrieved "teacher," "teachers," "teaching").

Phase 2: Development

a. Selection of Primary Studies

Literature from the Scopus database was searched and filtered using the Watase Uake web application Wahyudi (2024), while Google Scholar records were screened manually. All retrieved documents were organized using Microsoft Excel LTSC. The selection of primary

studies followed the PRISMA flow diagram, presented in Figure 2, encompassing four stages: identification, screening, eligibility assessment, and inclusion.

At the identification stage, 526 documents were retrieved (419 from Scopus; 107 from Google Scholar). During screening, Scopus duplicates, incomplete records, and discontinued documents were removed automatically by the Watase Uake application, reducing this pool to 226 records. Google Scholar records were manually filtered using the duplicate-removal function in Excel and Mendeley. At the eligibility stage, titles, abstracts, and keywords of each document were examined against the exclusion criteria and search strings, yielding a total of 88 documents (43 from Scopus; 45 from Google Scholar). Subsequently, 41 studies were excluded because they did not answer the research questions, were not teacher-specific in context, or could not be retrieved in full text. Ultimately, 47 peer-reviewed articles were included for in-depth analysis. No conflict of interest was identified among the included studies. PRISMA Flow Diagram explained in Figure 2.

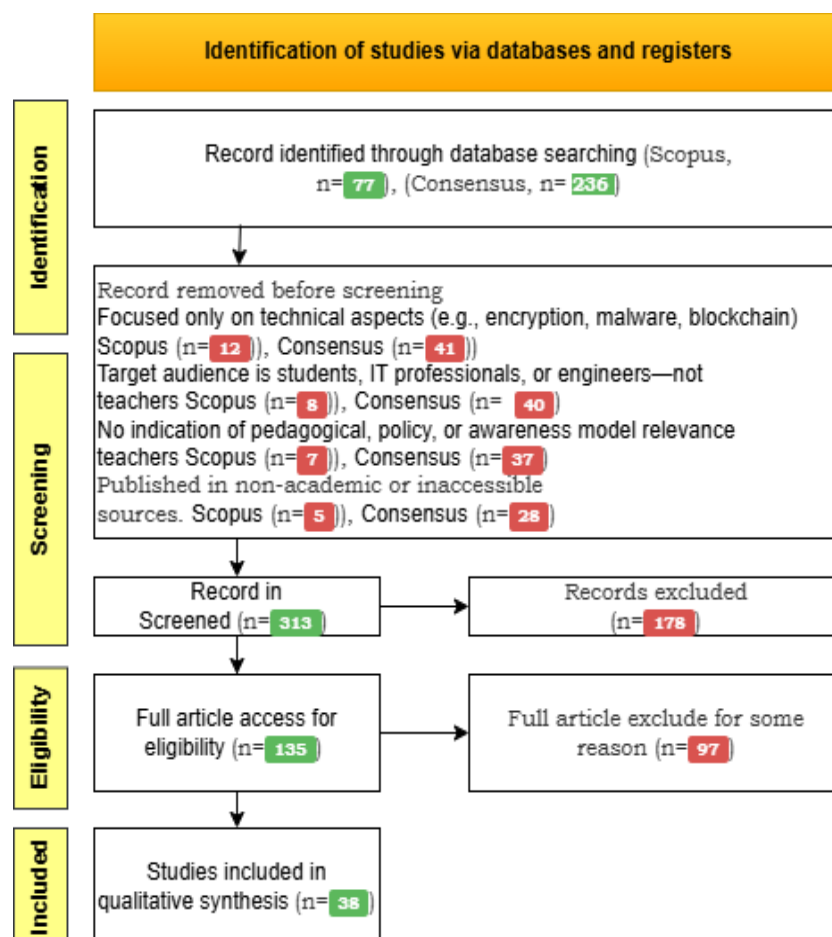


Fig 2: PRISMA Flow Diagram.

b. Study Quality Assessment

To ensure the rigor of included evidence, a comprehensive quality assessment was carried out using three complementary methods. First, a quantitative quality checklist comprising 10 items was applied to all included studies (Table 4). The checklist was formulated based on criteria recommended by (Kitchenham et al., 2009; Petticrew & Roberts, 2008; Riaz et al., 2009), and subsequently adapted to the focus of the present study. The 10 items assess the following aspects of each included study: (Q1) relevance to teacher digital security training; (Q2) clarity of methodology; (Q3) teacher-specificity of the study population; (Q4) identification of study design; (Q5) clarity of study objectives; (Q6) attention to teachers' perceptions of digital security; (Q7) explanation of required teacher competencies; (Q8) examination of how teachers integrate digital security into instruction; (Q9) presence of a model or framework for digital security competency; and (Q10) alignment of research questions with problem solutions. Each item was scored on a three-point scale: Yes = 1, Partly = 0.5, No = 0. A minimum aggregate score of 7 out of 10 was established as the inclusion threshold, ensuring that only methodologically rigorous and contextually relevant studies were retained. Studies scoring below this threshold were excluded regardless of their topical relevance.

Second, a professor in the field of vocational technology education (the second author) verified the accuracy of the extracted information and conducted an in-depth analysis of all included articles. Third, the AMSTAR checklist Shea et al (2017) was applied to evaluate the overall quality of the systematic review process. The data are displayed in Table 4.

Table 4. Study Quality Assessment Checklist

<i>Item</i>	<i>Quality Criterion</i>	<i>Yes</i>	<i>No</i>	<i>Partly</i>
Q1	Is the goal related to teacher training in digital security competence?			
Q2	Is the methodology clearly described?			
Q3	Are the study population participants teachers?			
Q4	Is the study design clearly identified?			
Q9	Does the study present a model or framework for digital security competency?			
Q10	Do the research questions lead toward solutions to the stated problem?			

Table 5. Quality Evaluation Criteria for Included Studies

<i>Evaluation Aspect</i>	<i>High Quality</i>	<i>Medium Quality</i>	<i>Low Quality</i>
Relevance	Directly addresses one or more research questions	Indirectly addresses one or more research questions	Does not address the research questions
Methodology	Uses robust methodology appropriate to study objectives	Uses adequate methodology, though not fully aligned with objectives	Uses weak methodology not appropriate to study objectives
Quality of Findings	Findings are valid and reliable	Findings are reasonably valid, with some limitations	Findings are invalid or unreliable
Contribution Value	Provides significant contribution to understanding the research topic	Provides a moderate contribution to understanding the research topic	Does not provide a significant contribution to understanding the research topic

c. Data Extraction and Synthesis

Data extraction was organized through two stages to address the three research questions. First, metadata from each primary study were extracted, including author, title, abstract, keywords, DOI, year of publication, database, document type, and language. Second, study content was categorized according to the following dimensions: study objectives, study type, teachers' perceptions of digital security, digital security competencies required of teachers, and how teachers implement digital security in learning. Study types were classified following the taxonomy described by Barros (2018), correlational studies (CS), descriptive studies (DS), descriptive and correlational studies (DCS), exploratory studies (ES), systematic review studies (SR), and non-experimental studies (NES). Study objectives were classified according to the framework proposed by Tonella et al (2007). Data synthesis is presented in the Results and Discussion section.

Table 6. Included Primary Studies (n = 47)

<i>No.</i>	<i>Title</i>	<i>Authors (Year)</i>
1	Integrating Security in the Computer Science Curriculum	Siraj A, Taylor B, Kaza S, G S (2015)
2	How to Transfer Cyber Security Skills?	Đekić M (2022)
46	Upper-Basic Schoolteachers' Beliefs about Their Students' Awareness of Digital Citizenship	Daher W, Omar A, Swaitly H, et al. (2022)
47	Development of Digital Competence in Secondary Education Teachers' Training	Fraile MN, Peñalva-Vélez A, Lacambra AM (2018)

Results and Discussion

The following section presents and interprets findings from the 47 included primary studies across the three research questions: (1) teachers' perceptions and understanding of digital security; (2) digital security competencies essential for educators; and (3) the implementation of digital security in the learning process.

a. RQ1: Teachers' Perceptions and Understanding of Digital Security

Teachers' perceptions and understanding of digital security constitute a fundamental determinant of their behavior and practice in maintaining secure educational environments. Through narrative synthesis, the included studies revealed that teachers define digital security in variable ways. Most teachers conceptualized it as the protection of data, information, and personal identity from threats arising from the use of digital technology (Chou and Chou, 2016; Daher et al., 2022; Gallego-Arrufat et al., 2019; Torres-Hernández and Gallego-Arrufat, 2022). This definition aligns broadly with accepted conceptions in the information security literature, which include the protection of data, privacy, and responsible digital practice Tomczyk (2020). Teachers emphasized awareness of threats such as malware, identity theft, and hacking, as well as the importance of preventive measures. Aspects such as online privacy, ethical behavior in cyberspace, copyright protection, prevention of cyberbullying, and financial transaction security were also highlighted (Khramova et al., 2018; Tomczyk, 2020).

However, several studies revealed that some teachers held a more limited understanding, focusing exclusively on viruses and hacking while overlooking risks such as online fraud, privacy violations, and technology misuse Tomczyk (2019a). This gap between teachers' definitions and the comprehensively accepted definition in the information security literature represents a critical concern Schiliro (2023). In contrast, a minority of teachers demonstrated more comprehensive understanding, encompassing encryption, digital identity management, and protection of sensitive data (Latorre-Medina and Tnibar-Harrus, 2023; Zakia and Yana, 2023). These findings enrich the theoretical framing of digital security in education by confirming that it cannot be reduced to technical knowledge alone; teachers' subjective perceptions and definitional boundaries substantially shape their protective behaviors Bacak et al (2022).

1. Level of Understanding and Risk Awareness

With respect to teachers' level of understanding of specific digital security risks including malware, phishing, and data theft findings were similarly heterogeneous. Several studies found that most teachers possessed adequate understanding of common threats and reported implementing practices such as password-based device protection and virus prevention

(Kumar et al., 2019; Tomczyk, 2019b). However, other studies identified limited knowledge of digital security and online data protection among teachers, particularly regarding advanced threats and technical safeguards (Chou and Chou, 2016; Elmalı et al., 2020; Khramova et al., 2018). Regarding good security practices such as using strong passwords and updating software, levels of understanding also varied considerably, with some teachers requiring more structured education (Dipak, 2023a; Gallego-Arrufat et al., 2019; Rodrigues, 2020; Torres-Hernández and Gallego-Arrufat, 2023). Additionally, noted that effective digital security awareness includes maintaining minimal personal information on social media, accepting requests only from trusted contacts, and activating security features on devices.

2. Factors Influencing Teachers' Perceptions

Educational background and training emerged as the strongest predictors of teachers' digital security understanding. Teachers with specialized education or training in digital security demonstrated superior threat recognition and more consistent adoption of security practices (Elmalı et al., 2020; Fraile et al., 2018; Gallego-Arrufat et al., 2019; Torres-Hernández and Gallego-Arrufat, 2023), while those lacking such preparation exhibited more limited understanding Chou and Chou (2016). Experience with digital technology was also positively associated with security awareness and implementation of protective measures (Tomczyk, 2019b; Zakia and Yana, 2023). Notably, age and years of professional experience did not emerge as significant differentiating factors; younger and older teachers displayed comparable levels of digital security understanding (Elmalı et al., 2020; Khramova et al., 2018). This finding challenges the assumption that older teachers are less digitally security-literate; rather, it suggests that training and hands-on experience not chronological age drive competence development (Vila-Counago et al., 2020). Additional factors including personal motivation, access to learning resources, and institutional support were also identified as influential, indicating that the relationship between background and security understanding is non-linear (Daher et al., 2022; Roll and Ifenthaler, 2021; Tsvetkova and Kiryukhin, 2019).

b. RQ2: Digital Security Competencies Essential for Educators

Having established the landscape of teachers' perceptions, this section synthesizes findings regarding the specific competencies educators require to address digital security challenges effectively. The synthesis of included studies revealed three core domains of digital security competency that teachers should possess: (1) knowledge of digital security threats and practices, (2) technical skills in using security tools, and (3) attitudes and behaviors that support a culture of digital security. Table 7 provides a summary of these domains and their key components.

Table 7. Summary of Core Digital Security Competency Domains for Educators

Competency Domain	Key Components	Representative Studies
Knowledge (Technical)	Threat recognition (malware, phishing, ransomware, DDoS); knowledge of security tools (antivirus, VPN, encryption, firewall); password management; data backup	(Dipak, 2023a; Krašna & Bratina, 2012; Latorre-Medina & Tnibar-Harrus, 2023; Marchisio et al., 2022; Starkey, 2020)
Skills (Pedagogical-Technical)	Operation of security software and devices; incident identification and response; critical evaluation of digital content; integration of security topics into curricula	(Dipak, 2023a; Gümüş et al., 2023; Krašna & Bratina, 2012; Marchisio et al., 2022; Randelović et al., 2017; Starkey, 2020)
Attitudes & Behaviors (Professional)	Risk awareness; personal responsibility; promotion of digital security culture; student monitoring; parental collaboration; continuous professional learning	(Gallego-Arrufat et al., 2019; Torres-Hernández & Gallego-Arrufat, 2023)

1. Knowledge of Digital Security Threats and Practices

Teachers must possess comprehensive knowledge of the diverse landscape of digital security threats, including malware (viruses, trojans, worms, ransomware), phishing attacks, hacking, DDoS attacks, data theft, personal information leaks, cyberbullying, and social engineering (Dipak, 2023a; Krašna and Bratina, 2012; Latorre-Medina and Tnibar-Harrus, 2023; Marchisio et al., 2022; Starkey, 2020). These threats can cause substantial harm at both individual and organizational levels, including data loss, account compromise, and financial damage. To mitigate such threats, teachers must be knowledgeable about security software (antivirus, firewall, data encryption, VPN), the use of strong and unique passwords, regular software updates, phishing awareness, and data backup procedures (Dipak, 2023a; Gümüş et al., 2023; Krašna and Bratina, 2012; Marchisio et al., 2022; Randelović et al., 2017; Starkey, 2020). Teachers who possess this foundational knowledge are better positioned to model responsible digital security behavior for their students and to identify institutional vulnerabilities before they escalate into incidents Gallego-Arrufat et al (2019)

2. Digital Security Skills

Beyond knowledge, teachers must develop practical skills in operating security software and devices such as antivirus programs, firewalls, and data encryption tools (Kuzminykh et al., 2021; Marchisio et al., 2022; Randelović et al., 2017). Proficiency in these tools is essential for preventing malware attacks, phishing, and other cyber threats. Equally important are teachers'

skills in identifying suspicious behavior such as abnormal network activity or phishing messages and responding appropriately when security incidents occur, including blocking unauthorized access, isolating compromised systems, and reporting incidents to relevant authorities (Marchisio et al., 2022; Roll and Ifenthaler, 2021). Critical evaluation of digital content, recognition of emerging threats, and timely adoption of appropriate precautions also constitute essential skill components (Kim et al., 2017; Kuzminykh et al., 2021). The literature consistently emphasizes that these skills must be sustained through continuous professional development, as the digital threat landscape evolves rapidly (Gallego-Arrufat et al., 2019; Latorre-Medina and Tnibar-Harrus, 2023; Torres-Hernández and Gallego-Arrufat, 2022).

3. Digital Security Attitudes and Behaviors

Attitudes and behaviors represent the third and equally critical domain of digital security competency. Teachers must maintain heightened awareness of digital security risks, actively safeguard students' personal information and sensitive data, and assume responsibility for maintaining security within the learning environment (Çiftçi & Delialioğlu, 2016; Gümüş et al., 2023; Kopecký et al., 2022; Sapanca and Kanbul, 2022). This includes following recommended security practices such as using strong passwords, refraining from carelessly sharing personal information, and staying current with evolving threats as well as educating students about safe digital practices and promoting cyber-ethical behavior (Dipak, 2023b; Fraile et al., 2018; Krašna and Bratina, 2012; Starkey, 2020). Teachers should also monitor students' online activities and collaborate with parents to reinforce safe practices in both school and home environments (Gallego-Arrufat et al., 2019; Gümüş et al., 2023; Martin et al., 2023; Tomczyk, 2019b). Continuous professional training in digital security is thus identified as an urgent priority across multiple included studies (Fraile et al., 2018; Gallego-Arrufat et al., 2019; Latorre-Medina & Tnibar-Harrus, 2023; Marchisio et al., 2022; Randelović et al., 2017; Torres-Hernández and Gallego-Arrufat, 2023).

These three competency domains are consistent with the broader model of digital literacy, which situates security competence as a multidimensional construct integrating cognitive, psychomotor, and affective dimensions (Fraile et al., 2018; Gallego-Arrufat et al., 2019; Latorre-Medina and Tnibar-Harrus, 2023; Marchisio et al., 2022; Randelović et al., 2017; Torres-Hernández & Gallego-Arrufat, 2023). The pedagogical implication is that teacher preparation programs must address all three domains systematically, rather than privileging technical knowledge at the expense of attitudinal and behavioral development Marchisio et al (2022).

c. RQ3: Implementation of Digital Security in the Learning Process

The implementation of digital security in the learning process encompasses three interrelated dimensions: curricular integration, safe use of digital technology, and institutional policies and guidelines.

1. Integration of Digital Security in the Curriculum

The development of students' digital security competencies requires deliberate and structured curricular integration. Included studies identified several strategies employed by teachers to embed digital security content within their instructional practice. Teachers developed specialized learning modules covering topics such as personal data protection, cyber threat identification, digital ethics, and safe password use (Dionysiou and Ktoridou, 2012; Dooley et al., 2016; Martínez Mayoral et al., 2017; Redmiles et al., 2016; Starkey, 2020). These modules were integrated into subjects such as ICT and, in some cases, language instruction Leary et al (2016). Activity-based approaches including collaborative projects focused on online security risk identification, data security principles instruction, and cybersecurity simulations were also reported as effective (Dooley et al., 2016; Instefjord and Munthe, 2016; Rodrigues, 2020). Applied assignments involving real-world security scenarios, cyber attack simulations, and digital security case studies provided opportunities for students to develop practical competencies (Dionysiou and Ktoridou, 2012; Wolfenden, 2019). Available resources such as the Security Knitting Kit, the Security Injections Towson modules, and cyber range platforms further enabled authentic learning experiences (Langner et al., 2022; Siraj et al., 2015). Organizing material around current practice situations and embedding practical exercises into instruction were also identified as effective strategies for ensuring the relevance and applicability of digital security learning Langner et al (2022).

2. Safe Use of Digital Technology

The safe use of digital technologies in teaching practice constitutes an essential implementation dimension. Teachers were found to select security-tested applications, ensure that software was regularly updated, and provide training to students on appropriate software use (Instefjord and Munthe, 2016; Stobert et al., 2018). In online learning contexts, teachers implemented secure connection practices (e.g., VPN use), encrypted sensitive data, protected student privacy, and conveyed the importance of digital security to students (Krašna and Bratina, 2012; Martínez Mayoral et al., 2017; Tammam and D'Alessio, 2016). Additional strategies included instructing students not to share personal information online, the use of

strong passwords, and ensuring encryption of all sensitive data transmissions during online sessions (Leary et al., 2016; Redmiles et al., 2016; Starkey, 2020). Multidisciplinary professional development including training in learning media creation, peer collaboration, and targeted capacity-building initiatives was identified as an effective approach to improving teachers' digital security competence in practice (Islami et al., 2022). Gender-based differences in perceived competence were also noted, with female pre-service teachers expressing greater need for additional training compared to their male counterparts (Latorre-Medina and Tnibar-Harrus, 2023).

3. Digital Security Policies and Guidelines in Schools

Institutional policies and guidelines are fundamental enablers of a secure educational environment. The literature consistently identified the need for clear, comprehensive digital security policies covering access restrictions to harmful websites, strong password requirements, procedures for information sharing and incident reporting, and rules governing personal device use in school (Cole and Kritzer, 2009; Krašna & Bratina, 2012; Leary et al., 2016; Starkey, 2020; Tammara and D'Alessio, 2016). Such policies must involve all relevant stakeholders, including teachers, students, parents, and school administrators (Martínez et al (2017). Incident response procedures should include immediate reporting to authorities, isolation of the affected system, forensic investigation, vulnerability remediation, and remedial training for staff and students (Dionysiou and Ktoridou, 2012; Dooley et al., 2016; Estrada et al., 2022; Instefjord and Munthe, 2016; Wolfenden, 2019). Teachers play a central role in enacting these policies, educating students about digital security, enforcing institutional guidelines, and fostering a culture of shared cyber responsibility (Dipak, 2023a; Gallego-Arrufat et al., 2019; Gümüş et al., 2023; Marchisio et al., 2022; Sapanca and Kanbul, 2022; Torres-Hernández and Gallego-Arrufat, 2022).

4. Theoretical and Practical Implications

The findings of this review carry significant theoretical implications for the conceptualization of digital security in education. Prior scholarship has largely centered on technical and institutional dimensions of cybersecurity, with insufficient attention to the teacher as a key actor Bacak et al (2022). This review extends existing theory by demonstrating that educators' digital security competence is a multidimensional construct shaped by educational background, professional training, technological experience, and psychological factors including perceptions and attitudes (Torres-Hernández and Gallego-Arrufat, 2023).

Based on these findings, a holistic model or framework for improving teacher digital security competence should incorporate context-sensitive training programs, accessible learning resources, institutional environmental support, and ongoing evaluation and feedback mechanisms (Lavicza et al., 2022; Marchisio et al., 2022).

Practically, the findings call for comprehensive and continuous professional development programs for teachers covering knowledge, skills, and attitudinal dimensions of digital security, tailored to teachers' backgrounds and institutional contexts Fraile et al (2018). These programs should be supported by digital modules, online learning platforms, and professional communities of practice to facilitate knowledge exchange Kuzminykh et al (2021). Curricular integration of digital security should proceed systematically, utilizing special learning modules, applied projects, and existing resources such as cyber ranges and security simulation kits Siraj et al (2015). At the policy level, governments should develop national guidelines for digital security in education and allocate adequate resources and funding. Institutions must establish clear security policies, incident handling procedures, and technical support infrastructure, while engaging parents and communities as partners in promoting digital security culture in both school and home environments (Krašna and Bratina, 2012; Stobert et al., 2018).

Conclusion

This systematic literature review synthesized evidence from 47 peer-reviewed studies to address three research questions regarding teachers' digital security perceptions, competencies, and implementation practices. With respect to RQ1, teachers demonstrated variable perceptions of digital security; while most defined it as the protection of data, information, and personal identity from digital threats, a significant proportion held more limited conceptualizations, overlooking risks such as online fraud and privacy violations. Perceptions were found to be shaped primarily by educational background, training, and practical technology experience, rather than by age or years of service. With respect to RQ2, three core competency domains were identified as essential for teachers: (1) knowledge of the diverse landscape of digital security threats and established protective practices; (2) technical skills in the operation of security software and tools, threat identification, and incident response; and (3) attitudes and behaviors characterized by heightened risk awareness, personal responsibility, and proactive promotion of digital security culture among students and colleagues.

With respect to RQ3, implementation of digital security in the learning process was found to be inconsistent and constrained by insufficient professional training, limited institutional support, and resource gaps. Effective implementation strategies included the integration of structured digital security modules within existing curricula, the use of realistic, activity-based learning approaches, the adoption of security-tested platforms and tools, and the establishment of clear institutional policies and incident response procedures. Collaboration among teachers, students, parents, and school administrators was identified as a critical enabling condition for sustainable digital security culture in educational settings.

a. Policy Recommendations

At the national level, governments should develop clear, binding guidelines for digital security education and allocate dedicated resources and funding to support teacher professional development in this domain. Ministries of education are encouraged to embed digital security competencies into national teacher certification frameworks, ensuring baseline standards are met across all educational levels. At the institutional level, schools should establish comprehensive digital security policies covering access restrictions, password requirements, incident reporting procedures, and rules governing personal device use, with regular review and updating in response to the evolving threat landscape.

b. Recommendations for Vocational Education Institutions

Vocational and technical education institutions face unique challenges in digital security, given the applied, technology-intensive nature of their programs and their close industry linkages. To build effective institutional support frameworks, vocational institutions are specifically recommended to: (1) establish dedicated digital security coordinator or champion roles within faculties to provide ongoing peer support and guidance; (2) develop partnerships with industry and cybersecurity organizations to provide teachers with access to up-to-date resources, cyber range platforms, and simulation tools; (3) integrate digital security training modules directly into vocational teacher preparation and in-service development programs, with a focus on workplace-relevant threats and scenarios; and (4) create communities of practice among vocational educators to facilitate knowledge exchange and collaborative problem-solving on digital security issues. These measures will ensure that institutional support frameworks are not merely aspirational, but operationally grounded in the vocational education context.

These findings collectively underscore the urgent need for systematic, evidence-based professional development programs and robust institutional frameworks to build comprehensive

digital security literacy among educators. Future research should employ empirical methods including surveys, interviews, and case studies to obtain contextually nuanced understandings of teachers' digital security practices and to evaluate the effectiveness of training interventions. Longitudinal studies and cross-national comparative analyses would further strengthen the evidence base for policy and practice in this critical domain.

This review is subject to several limitations. The study relied exclusively on published literature and did not collect primary data from teachers directly, which may introduce interpretation bias and limit contextual specificity. Additionally, the scope of the review may not be exhaustive, as studies in non-English languages or less widely indexed publications may have been excluded, potentially creating gaps in understanding digital security across diverse vocational and technological education contexts.

References

- Akram, H., Abdelrady, A. H., Al-Adwan, A. S., & Ramzan, M. (2022). Teachers' perceptions of technology integration in teaching-learning practices: A systematic review. *Frontiers in Psychology, 13*, Article 920317. <https://doi.org/10.3389/fpsyg.2022.920317>
- Arsenovych, L. (2022). Tools of improving the digital competence level of cyber security professionals in the educational process. *Cybersecurity: Education, Science, Technique, 3*(15), 93–109. <https://doi.org/10.28925/2663-4023.2022.15.93109>
- Bacak, J., Martin, F., Ahlgrim-Delzell, L., Polly, D., & Wang, W. C. (2022). Elementary educator perceptions of student digital safety based on technology use in the classroom. *Computers in the Schools, 39*(2), 186–202. <https://doi.org/10.1080/07380569.2022.2071233>
- Barros, Á. A. M. M. S. X. V. M. F. A. C. M. R. Q. (2018). Evaluation of the use of applied techniques in research. *Scientific Research Magazine Updating the World of Sciences, 2*(3), 722–738. [https://doi.org/10.26820/reciamuc/2.\(3\).september.2018.722-738](https://doi.org/10.26820/reciamuc/2.(3).september.2018.722-738)
- Chou, H. L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior, 65*, 334–345. <https://doi.org/10.1016/j.chb.2016.08.034>
- Çiftçi, N. P., & Delialioğlu, Ö. (2016). Supporting students' knowledge and skills in information technology security through a security portal. *Information Development, 32*(5), 1417–1427. <https://doi.org/10.1177/0266666915601463>
- Cole, J. E., & Kritzer, J. B. (2009). Strategies for success: Teaching an online course. *Rural Special Education Quarterly, 28*(4), 36–40. <https://doi.org/10.1177/875687050902800406>
- Daher, W., Omar, A., Swait, H., Allan, B., Dar Issa, S., Amer, Z., & Halabi, A. (2022). Upper-basic schoolteachers'

- beliefs about their students' awareness of digital citizenship. *Sustainability*, 14(19), Article 12865. <https://doi.org/10.3390/su141912865>
- Dionysiou, I., & Ktoridou, D. (2012). Enhancing dynamic-content courses with student-oriented learning strategies. *International Journal of Cyber Ethics in Education*, 2(2), 24–33. <https://doi.org/10.4018/ijcee.2012040103>
- Dipak, M. H. (2023). Cyber smart teacher: A conceptual study. *International Journal for Multidisciplinary Research*, 5(6), 1–6. <https://doi.org/10.36948/ijfmr.2023.v05i06.10253>
- Dooley, C. M. M., Lewis Ellison, T., Welch, M. M., Allen, M., & Bauer, D. (2016). Digital participatory pedagogy: Digital participation as a method for technology integration in curriculum. *Journal of Digital Learning in Teacher Education*, 32(2), 52–62. <https://doi.org/10.1080/21532974.2016.1138912>
- Elmalı, D. F., Tekin, D. A., & Polat, E. (2020). A study on digital citizenship: Preschool teacher candidates vs. computer education and instructional technology teacher candidates. *Turkish Online Journal of Distance Education*, 21(4), 251–269. <https://doi.org/10.17718/TOJDE.803423>
- Estrada, F. J. R., George-Reyes, C. E., & Glasserman-Morales, L. D. (2022). Security as an emerging dimension of digital literacy for education: A systematic literature review. *Journal of E-Learning and Knowledge Society*, 18(2), 22–33. <https://doi.org/10.20368/1971-8829/1135440>
- Fraile, M. N., Peñalva-Vélez, A., & Lacambra, A. M. M. (2018). Development of digital competence in secondary education teachers' training. *Education Sciences*, 8(3), Article 104. <https://doi.org/10.3390/educsci8030104>
- Gallego-Arrufat, M. J., Torres-Hernández, N., & Pessoa, T. (2019). Competence of future teachers in the digital security area. *Comunicar*, 27(61), 53–62. <https://doi.org/10.3916/C61-2019-05>
- García-Peñalvo, F. J. (2021). Avoiding the dark side of digital transformation in teaching: An institutional reference framework for eLearning in higher education. *Sustainability*, 13(4), Article 2023. <https://doi.org/10.3390/su13042023>
- Ghauri, F. A. (2021). Digital security versus private information. *International Journal of Computer Science and Information Security*, 19(7), 10–20. <https://doi.org/10.5281/zenodo.5164002>
- Gorodianska, L. (2021). Information security of small businesses in the context of digitalization. *Collection of Scientific Works of the Military Institute of Kyiv National Taras Shevchenko University*, 105–114. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe
- Guerrero, L. Á., García, D. M. A., Pérez, M. A. C., Lira, S. E. T., & Ornelas, E. de J. L. (2019). Learn&safe: Digital security to reduce digital gap in educational community. *Proceedings of the IX Latin American Conference on Human Computer Interaction*, Article 22. <https://doi.org/10.1145/3358961.3358996>
- Gümüş, M. M., Çakır, R., & Korkmaz, Ö. (2023). Investigation of pre-service teachers' sensitivity to cyberbullying, perceptions of digital ethics and awareness of digital data security. *Education and Information Technologies*, 28(11), 14399–14421. <https://doi.org/10.1007/s10639-023-11785-7>

- Instefjord, E., & Munthe, E. (2016). Preparing pre-service teachers to integrate technology: An analysis of the emphasis on digital competence in teacher education curricula. *European Journal of Teacher Education*, 39(1), 77–93. <https://doi.org/10.1080/02619768.2015.1100602>
- Islami, B., Arifin, Z., & Puspitorini, P. (2022). Strategy to strengthen teachers' digital competence. *Advances in Social Science, Education and Humanities Research*, 39–43. <https://doi.org/10.2991/assehr.k.220129.007>
- Khramova, M. V., Bukina, T. V., & Kurkin, S. A. (2018). The attitude of computer science teachers to the nuances of teaching computer security for junior schoolchildren. *Proceedings of the 2018 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)*, 659–662. <https://doi.org/10.1109/ITMQIS.2018.8525059>
- Kim, M. K., Xie, K., & Cheng, S. L. (2017). Building teacher competency for digital content evaluation. *Teaching and Teacher Education*, 66, 309–324. <https://doi.org/10.1016/j.tate.2017.05.006>
- Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering - A systematic literature review. *Information and Software Technology*, 51(1), 7–15. <https://doi.org/10.1016/j.infsof.2008.09.009>
- Kopecký, K., Szotkowski, R., Krejčí, V., & Gómez-García, G. (2022). Digital safety and its importance in teacher education: Analysis of children's online behaviour in the Czech and Polish context. *Revista Interuniversitaria de Formación del Profesorado*, 98(36.2), 79–92. <https://doi.org/10.47553/rifop.v98i36.2.94062>
- Krašna, M., & Bratina, T. (2012). Designing digital security course in educational sciences. *International Journal of Knowledge Engineering and Soft Data Paradigms*, 3(3/4), 280–292. <https://doi.org/10.1504/ijkesdp.2012.050723>
- Kumar, P. C., Chetty, M., Clegg, T. L., & Vitak, J. (2019). Privacy and security considerations for digital technology use in elementary schools. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13. <https://doi.org/10.1145/3290605.3300537>
- Kuzminykh, I., Yevdokymenko, M., Yeremenko, O., & Lemeshko, O. (2021). Increasing teacher competence in cybersecurity using the EU security frameworks. *International Journal of Modern Education and Computer Science*, 13(6), 60–68. <https://doi.org/10.5815/ijmeecs.2021.06.06>
- Langner, G., Skopik, F., Furnell, S., & Quirchmayr, G. (2022). A tailored model for cyber security education utilizing a cyber range. *Proceedings of the 8th International Conference on Information Systems Security and Privacy*, 365–377. <https://doi.org/10.5220/0010834000003120>
- Latorre-Medina, M. J., & Tnibar-Harrus, N. (2023). Digital security in educational training programs: A study based on future teachers' perceptions. *Information Technologies and Learning Tools*, 95(3), 109–125. <https://doi.org/10.33407/itlt.v95i3.5204>
- Lavicza, Z., Weinhandl, R., Prodromou, T., Andić, B., Lieban, D., Hohenwarter, M., Fenyvesi, K., Brownell, C., & Diego-Mantecón, J. M. (2022). Developing and evaluating educational innovations for STEAM education in

- rapidly changing digital technology environments. *Sustainability*, 14(12), Article 7237. <https://doi.org/10.3390/su14127237>
- Leary, H., Severance, S., Penuel, W. R., Quigley, D., Sumner, T., & Devaul, H. (2016). Designing a deeply digital science curriculum: Supporting teacher learning and implementation with organizing technologies. *Journal of Science Teacher Education*, 27(1), 61–77. <https://doi.org/10.1007/s10972-016-9452-9>
- Maathuis, C., & Chockalingam, S. (2022). Responsible digital security behaviour: Definition and assessment model. *Proceedings of the 21st European Conference on Information Warfare and Security*, 178–187. <https://doi.org/10.34190/eccws.21.1.203>
- Marchisio, M., Roman, F., Sacchet, M., Spinello, E., Nikolov, L., Grzelak, M., Rykala, M., & Moldoveanu, C. E. (2022). Teachers' digital competences before and during the Covid-19 pandemic for the improvement of security and defence higher education. *Proceedings of the International Conference on E-Learning 2022*, 68–75. https://doi.org/10.33965/el2022_202203l009
- Martin, F., Bacak, J., Polly, D., Wang, W., & Ahlgrim-Delzell, L. (2023). Teacher and school concerns and actions on elementary school children digital safety. *TechTrends*, 67(3), 561–571. <https://doi.org/10.1007/s11528-022-00803-z>
- Martínez Mayoral, M. A., Morales, J., Calvo, R., & Molina, J. (2017). Evaluation of digital teaching skills. *EDULEARN17 Proceedings*, 1, 9786–9792. <https://doi.org/10.21125/edulearn.2017.0852>
- Ott, E. V., Panova, E. P., Lobanova, Y. V., Bocharnikova, N. V., Panfilova, V. M., & Panfilov, A. N. (2021). Modification of the role of a teacher under the conditions of distance learning. *International Journal of Emerging Technologies in Learning*, 16(21), 219–225. <https://doi.org/10.3991/ijet.v16i21.25675>
- Page, M. J., & Moher, D. (2017). Evaluations of the uptake and impact of the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) Statement and extensions: A scoping review. *Systematic Reviews*, 6(1), Article 263. <https://doi.org/10.1186/s13643-017-0663-8>
- Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, 18(2), 68–74. <https://doi.org/10.1109/MSEC.2020.2969409>
- Perestelo-Perez, L. (2013). Standards on how to develop and report systematic reviews in psychology and health. *International Journal of Clinical and Health Psychology*, 13(1), 49–57. [https://doi.org/10.1016/s1697-2600\(13\)70007-3](https://doi.org/10.1016/s1697-2600(13)70007-3)
- Pérez-Sánchez, L., Lavandera-Ponce, S., Mora-Jaureguialde, B., & Martín-Cuadrado, A. M. (2022). Training plan for the continuity of non-presential education in six Peruvian universities during COVID-19. *International Journal of Environmental Research and Public Health*, 19(3), Article 1562. <https://doi.org/10.3390/ijerph19031562>
- Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, 64, 1–18. <https://doi.org/10.1016/j.infsof.2015.03.007>

Email : joves@mpv.uad.ac.id

Website : <http://journal2.uad.ac.id/index.php/joves>

- Petrov, P., Kuyumdzhev, I., Malkawi, R., Dimitrov, G., & Jordanov, J. (2022). Digitalization of educational services with regard to policy for information security. *TEM Journal*, 11(3), 1093–1102. <https://doi.org/10.18421/TEM113-14>
- Petticrew, M., & Roberts, H. (2008). *Systematic reviews in the social sciences: A practical guide*. Wiley-Blackwell. <https://doi.org/10.1002/9780470754887>
- Randelović, M., Papić, M., & Blagojević, M. (2017). Safety issues related to the adoption of the digital dialogue in teaching. *Studies in Informatics and Control*, 26(2), 229–238. <https://doi.org/10.24846/v26i2y201711>
- Redmiles, E. M., Malone, A. R., & Mazurek, M. L. (2016). I think they're trying to tell me something: Advice sources and selection for digital security. *Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP)*, 272–288. <https://doi.org/10.1109/SP.2016.24>
- Riaz, M., Mendes, E., & Tempero, E. (2009). A systematic review of software maintainability prediction and metrics. *Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement*, 367–377. <https://doi.org/10.1109/ESEM.2009.5314233>
- Rodrigues, A. L. (2020). Digital technologies integration in teacher education: The active teacher training model. *Journal of E-Learning and Knowledge Society*, 16(3), 24–33. <https://doi.org/10.20368/1971-8829/1135273>
- Roll, M., & Ifenthaler, D. (2021). Multidisciplinary digital competencies of pre-service vocational teachers. *Empirical Research in Vocational Education and Training*, 13, Article 7. <https://doi.org/10.1186/s40461-021-00112-4>
- Sánchez-Cruzado, C., Santiago Campión, R., & Sánchez-Compañía, M. T. (2021). Teacher digital literacy: The indisputable challenge after COVID-19. *Sustainability*, 13(4), Article 1858. <https://doi.org/10.3390/su13041858>
- Sapanca, H. F., & Kanbul, S. (2022). Risk management in digitalized educational environments: Teachers' information security awareness levels. *Frontiers in Psychology*, 13, Article 986561. <https://doi.org/10.3389/fpsyg.2022.986561>
- Schiliro, F. (2023). *Towards a contemporary definition of cybersecurity* [Research report]. ResearchGate. <https://www.researchgate.net/publication/368304689>
- Shea, B. J., Reeves, B. C., Wells, G., Thuku, M., Hamel, C., Moran, J., Moher, D., Tugwell, P., Welch, V., Kristjansson, E., & Henry, D. A. (2017). AMSTAR 2: A critical appraisal tool for systematic reviews that include randomised or non-randomised studies of healthcare interventions, or both. *BMJ*, 358, Article j4008. <https://doi.org/10.1136/bmj.j4008>
- Singh, N. (2002). Digital protection. *Fashion Business International*, (Aug/Sept), 73–76. <https://doi.org/10.56726/irjmet31589>
- Sinoara, R. A., Antunes, J., & Rezende, S. O. (2017). Text mining and semantics: A systematic mapping study. *Journal of the Brazilian Computer Society*, 23(1), Article 9. <https://doi.org/10.1186/s13173-017-0058-7>

Email : joves@mpv.uad.ac.id

Website : <http://journal2.uad.ac.id/index.php/joves>

- Siraj, A., Taylor, B., Kaza, S., & G, S. (2015). Integrating security in the computer science curriculum. *Proceedings of the 2015 IEEE Frontiers in Education Conference (FIE)*, 1–5. <https://doi.org/10.1109/FIE.2015.7344233>
- Starkey, L. (2020). A review of research exploring teacher preparation for the digital age. *Cambridge Journal of Education*, 50(1), 37–56. <https://doi.org/10.1080/0305764X.2019.1625867>
- Stobert, E., Cavar, E., Malisa, L., & Sommer, D. (2018). Teaching authentication as a life skill. *IEEE Security & Privacy*, 16(5), 82–85. <https://doi.org/10.1109/MSP.2018.3761712>
- Tammaro, R., & D'Alessio, A. (2016). Teacher training and digital competence. *International Journal of Digital Literacy and Digital Competence*, 7(2), 1–10. <https://doi.org/10.4018/ijdlcd.2016040101>
- Tomczyk, Ł. (2019). What do teachers know about digital safety?. *Computers in the Schools*, 36(3), 167–187. <https://doi.org/10.1080/07380569.2019.1642728>
- Tomczyk, Ł. (2020). Skills in the area of digital safety as a key component of digital literacy among teachers. *Education and Information Technologies*, 25(1), 471–486. <https://doi.org/10.1007/s10639-019-09980-6>
- Tonella, P., Torchiano, M., Du Bois, B., & Systä, T. (2007). Empirical studies in reverse engineering: State of the art and future trends. *Empirical Software Engineering*, 12(5), 551–571. <https://doi.org/10.1007/s10664-007-9037-5>
- Torres-Hernández, N., & Gallego-Arrufat, M. J. (2022). Indicators to assess preservice teachers' digital competence in security: A systematic review. *Education and Information Technologies*, 27(6), 8583–8602. <https://doi.org/10.1007/s10639-022-10978-w>
- Torres-Hernández, N., & Gallego-Arrufat, M. J. (2023). Pre-service teachers' perceptions of data protection in primary education. *Contemporary Educational Technology*, 15(1), Article ep401. <https://doi.org/10.30935/cedtech/12658>
- Tsvetkova, M. S., & Kiryukhin, V. M. (2019). Advanced digital competence of the teacher. In *Teacher Education in the 21st Century* (pp. 1–12). IntechOpen. <https://doi.org/10.5772/intechopen.83788>
- Vila-Counago, E., Regueira, U., & Pernas-Morado, E. (2020). The safety area of digital competence: A mixed method study in Galician primary education students. *IEEE Revista Iberoamericana de Tecnologías del Aprendizaje*, 15(4), 389–398. <https://doi.org/10.1109/RITA.2020.3033218>
- Wahyudi, L. (2024). *Research collaboration, systematic literature review, meta analysis*. Watase Uake. <https://www.watase.web.id/home/index.php>
- Wolfenden, B. (2019). Gamification as a winning cyber security strategy. *Computer Fraud & Security*, 2019(5), 9–12. [https://doi.org/10.1016/S1361-3723\(19\)30052-1](https://doi.org/10.1016/S1361-3723(19)30052-1)
- Zakia, R., & Yana, D. (2023). English teachers' perception of security in digital literacy competence. *Journal on Education*, 5(3), 9946–9953. <https://doi.org/10.31004/joe.v5i3.1685>