

Cybersecurity integration in distance learning: an analysis of student awareness and attitudes

Adnan Ahmad Hnaif¹, Areej Mofeed Derbas², Sally Almanasra³

¹Department of Cybersecurity, College of Science and Information Technology, Al-Zaytoonah University of Jordan, Amman, Jordan

²Department of Basic Science, College of ART, Al-Zaytoonah University of Jordan, Amman, Jordan

³Department of Software Engineering, Faculty of Computer Studies, Arab Open University, Riyadh, Saudi Arabia

Article Info

Article history:

Received Sep 1, 2023

Revised Nov 20, 2023

Accepted Nov 27, 2023

Keywords:

Cybersecurity

Cybercriminals

Distance learning

E-learning

LMS

ABSTRACT

With the rapid growth of distance learning, especially since the COVID-19 pandemic, cybersecurity has become increasingly essential to protect students, instructors, and institutions from cyber threats. This paper examines the role of cybersecurity in enhancing students' security awareness during distance learning. A literature review covers critical cyber threats in distance learning and strategies to mitigate risks through cybersecurity tools, policies, training, and promoting a culture of cybersecurity. Primary research was conducted by surveying 531 university students engaged in distance learning to assess their cybersecurity awareness, attitudes, and behaviors. Results indicate relatively low awareness and adoption of secure practices. Recommendations include implementing multi-layered cybersecurity defenses, student security awareness training, and nurturing a "human firewall" through a cyber-aware campus culture. Cyber risks can be reduced through proactive partnerships between students, faculty, information technology (IT) staff, and administrators to secure distance learning environments.

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



Corresponding Author:

Adnan Hnaif

Department of Cybersecurity, College of Science and Information Technology

Al-Zaytoonah University of Jordan

P.O.Box 130 Amman 11733 Jordan

Email: adnan_hnaif@zuj.edu.jo

1. INTRODUCTION

The unprecedented expansion of distance learning, accelerated by the COVID-19 pandemic, has brought to the forefront the critical issue of cybersecurity [1]. This paradigm shifts in education exposes students, faculty, and institutions to heightened cyber risks, ranging from phishing attacks to data breaches [2], [3]. Distance learning has expanded dramatically with the advancement of online platforms, resources, and technologies [4]. While distance learning provides flexibility and accessibility, it also introduces cybersecurity risks for students, faculty, and institutions [5]. The decentralized nature of distance learning further compounds cyber vulnerabilities.

Distance learning involves exchanging large amounts of personal and academic data online, making it vulnerable to theft and exploitation by targeting students and academics with fraudulent messages. These messages aimed at stealing credential data or connecting to the internet through insecure networks that expose the data to danger or challenges related to securely storing and managing big data safely [6]. This makes universities and educational institutions potential targets for cyber attacks that can disrupt educational systems, requiring protecting the information of university students, academics, administrators, and research from unauthorized access.

Therefore, it is necessary to train users on best security practices and how to detect fraud attempts and to use and regularly update security software to protect systems, networks, control access to educational resources and sensitive data, and secure online exams [7]. The importance of cybersecurity in distance learning is that it builds students' and teachers' confidence in using technology for education and ensures the integrity of exams and academic assessments [8]. Lin *et al.* [7] "promoting information security awareness is one of the most cost-effective methods for protecting information systems and networking infrastructure".

This study uniquely contributes insights directly from students on their preparedness and behaviors related to distance learning cybersecurity. The analysis of their perceptions, experiences, and needs identifies tangible gaps that can be addressed through strategic recommendations. These include integrating security awareness into curricula, establishing robust incident response processes, strengthening data protections, and fostering an organizational culture prioritizing cybersecurity across all learning communities.

Most prior work has focused on institutional or faculty perspectives, while students themselves are an under-explored human layer in securing online education. Little investigation has been done into interventions tailored to enhance cybersecurity hygiene and vigilance among the student population. This study aims to address that gap by surveying students directly about their experiences, behaviors, and needs related to cybersecurity when engaging in distance learning. The results will identify tangible areas for improvement in policies, training, and resources to empower students to reduce risks, which have not been thoroughly elucidated in existing literature. By advancing understanding of students' specific role and needs, more strategic recommendations can be made to equip them to uphold robust cybersecurity.

The low levels of cybersecurity awareness and adoption of secure practices among students underscores the serious risks for online education. Without understanding threats and how to mitigate them, students remain highly vulnerable to cyberattacks that can disrupt learning. The gaps identified in both curricula and institutional policies/support highlight the need for a strategic realignment prioritizing cybersecurity. Ad-hoc or incomplete defenses are insufficient as threats rapidly evolve.

This study will survey students directly about their cybersecurity awareness, attitudes, and practices related to distance learning. Much prior work has focused on institutional or faculty viewpoints, while the student perspective has been relatively unexplored. The analysis of students' perceptions and self-reported preparedness will provide unique insights compared to existing work centered on administrative or staff perspectives. The conclusions will outline concrete ways to integrate cybersecurity into curricula, strengthen protections, and encourage security-conscious habits among students themselves through training and resources designed for their needs. The student-centered approach will advance understanding of their pivotal role as a human layer of defense and provide strategic recommendations to equip them to uphold robust cybersecurity hygiene, which has not been fully investigated in previous studies.

The research problem focuses on cybersecurity risks threatening distance learning and the need to safeguard increasingly online-reliant education. While technical controls are crucial, prior literature has shown their limitations in fully preventing sophisticated threats. This context frames a key gap in understanding students' cybersecurity awareness and preparedness to defend against risks. The objective of the study is to investigate and analyze how cybersecurity measures can contribute to improving students' awareness of security issues while participating in distance learning programs. The study aims to explore the various ways in which cybersecurity practices, tools, and educational initiatives can effectively enhance students' understanding of potential cyber threats and their ability to protect themselves and their online activities. The paper is structured to first present a comprehensive literature review, followed by an explanation of our research methodology. The subsequent sections delve into the analysis of our survey results, discussing their implications for enhancing cybersecurity in distance learning environments. This structure demonstrates the relevance of our findings in addressing the identified gaps in student cybersecurity awareness and practices.

2. LITERATURE REVIEW

2.1. Cyber threats targeting distance learning

Cybercriminals frequently target educational institutions, which hold valuable data, including intellectual property, research, and personal information. Verizon [9] data breach investigations report found that the education sector was the second most breached industry after healthcare. From denial-of-service (DoS) attacks to ransomware, schools at all levels face cyber risks as operations move online [10].

A 2020 EDUCAUSE study identified phishing, malware, and credential theft as top threats for teaching and learning during COVID-19 [11]. Attackers often use phishing to trick users into clicking malicious links or disclosing login credentials. Brute force attacks employ automated login guessing. Insiders may abuse access privileges or fall prey to social engineering. Alawida *et al.* [11], lack of security controls and limited staff oversight in distance learning systems increase exposure to cyber risks.

Poor cyber hygiene and lack of awareness also endanger users. Students often reuse passwords across applications, store passwords insecurely, connect to unsecured networks, or fail to install software updates [12]. Unintentional insider threats stem from negligence, errors, or lack of training [13]. Most ransomware attacks initially access networks by exploiting known software vulnerabilities or stolen credentials [14].

2.2. Cybersecurity strategies and controls

Educational institutions utilize layered defenses to protect infrastructure, data, and end users. Technical controls include firewalls, multi factor authentication (MFA), endpoint protection, network segmentation, intrusion detection/prevention systems (IDS/IPS), data encryption, backup/recovery systems, vulnerability management, and access controls [15]. Distance learning systems and activities should align with institutional security policies and standards. Cloud services and collaboration platforms require vetting to assess security risks [10].

2.3. Promoting a culture of cybersecurity

Technical controls provide essential safeguards but cannot fully prevent cyber incidents. Users are a critical defense layer [8]. A strong security culture promotes cyber awareness, mindfulness of risks, and commitment to protection behaviors throughout the educational community [16]. Leadership endorsement, communication, community partnerships, and accountability nurture an organizational culture where security is valued and prioritized [17]. Training and awareness programs enhance understanding of policies, procedures, and threats. With knowledge, users can make more informed security decisions [18].

2.4. Training and awareness strategies

Suwais and Alshahrani [19] identified a list of courses offered as virtual classes (VC) and face-to-face (F2F) classes in the last two academic years (2015, 2016 and 2016, 2017). The selected courses varied in difficulty and included both practical and theoretical subjects. The sample size consisted of 200 students selected from 1,000 students who studied in the two academic years.

Abduljawad *et al.* [20] proposed acceptance framework for e-learning in Jordan incorporates various factors such as awareness of e-learning, perceived benefits, and perceived risks. Alotaibi and Alghamdi [21] surveyed faculty members at Shaqra University in Saudi Arabia about their readiness to adopt an e-learning platform. The results showed high self-efficacy in using information and communication technologies (ICT) tools but lower confidence in aspects like designing web pages and managing online forums. There were no major differences based on gender, but experience with e-learning did correlate with higher confidence and more positive attitudes. The study concludes faculty are ready to use the e-learning platform, but training should be offered to increase skills and confidence for inexperienced instructors.

Abduh *et al.* [22] analyzed Indonesian Twitter sentiments about online learning during the COVID-19 pandemic. Tweets were collected containing relevant hashtags and analyzed using lexicon analysis and POS tagging. Results showed an overwhelmingly positive sentiment, with 78% of tweets being positive. The most common topics were distance learning, education, learning support, teachers, schools, and students. This suggests Indonesians have embraced online learning but need more support. The study provides insights for education policymakers on public attitudes to guide decisions around online learning initiatives.

Ayyoub *et al.* [23] used quantitative research methods-administered a questionnaire to 2,648 students enrolled in 3 online courses at the University of Jordan. Also, they analyzed data using SPSS to find degrees of awareness about cybercrimes and legal procedures related to e-crimes in e-learning, and finally, they calculated averages, standard deviations, ratios and frequencies of responses.

Karim and Ali [24] explored the use of virtual meeting applications (VM apps) in the context of e-learning during the COVID-19 pandemic. The study compared the security features and vulnerabilities of three popular VM apps: Zoom, Microsoft Teams, and Google Meet. The results indicate that Google Meet is the most secure against cyber-attacks, followed by Microsoft Teams and Zoom. The paper emphasizes the importance of considering cybersecurity issues in the use of VM apps for educational purposes and highlights privacy risks such as information disclosure, malware execution, and unauthorized access to meetings. The authors suggest that improvements in encryption and password protection can enhance the security of these applications.

On the other hand, [25] discussed the integration of blockchain technology in smart cities to enhance security and privacy. The authors explored different applications of blockchain in smart cities and how its features can improve smart city services. The paper proposed an electronic voting model using a smart contract based on the Ethereum blockchain to demonstrate the implementation of blockchain technology in smart cities, and also highlighted the importance of blockchain technology in providing security in smart cities and mentions the use of blockchain for distributed electronic health records.

Ahmed and Khorsheed [26] discussed the incorporation of IT and operations technology (OT) in the next-generation communication system, which includes the internet of things (IoT) communication and its security concerns in the 5G network. The authors mentioned the use of IoT communication and its architecture in the context of data transfer over wireless and wired networks, as well as its role in informed decision-making and different services. Table 1 (in Appendix) summarizes the literature review, providing insights into various aspects of cybersecurity integration in distance learning environments.

3. RESEARCH METHOD

Primary research was conducted through anonymous surveys to assess students' cybersecurity awareness and practices during distance learning. The sample included 531 students at a mid-sized private university in Jordan engaged in fully online or hybrid learning during the COVID-19 pandemic. Participation was voluntary.

The methodology of this study revolves around a meticulously designed survey, distributed to a diverse group of students engaged in distance learning. The survey comprises a series of Likert scale questions, developed to gauge students' awareness and attitudes towards various aspects of cybersecurity. We selected participants through a stratified sampling technique, ensuring a representative cross-section of the student population. For data analysis, statistical methods were employed to interpret the responses effectively. This comprehensive approach allows for an in-depth understanding of the cybersecurity landscape in the context of distance learning.

In addition, the survey included questions to gauge perceptions, attitudes, experiences, and behaviors related to cybersecurity during distance learning. Topics included awareness of policies, training, and support resources; self-assessed knowledge and preparedness; cyber hygiene practices; experiences with cyber threats; and openness to learning about cybersecurity. Survey results were analyzed using descriptive statistics to identify central tendencies and frequencies. Cross-tabulations examined relationships between key variables. Analysis focused on assessing students' security awareness, identifying knowledge gaps, and determining opportunities to enhance distance learning cybersecurity through training and policies.

The methodology for this research initiated by distributing the online survey link electronically among the students. Then, descriptive statistics identified response frequencies and central tendencies. As for the testing, cross-tabulations examined relationships between variables. Finally, analysis is carried out to identify gaps in awareness, preparedness, and areas to enhance cybersecurity integration based on student perceptions. The following sections describe the key stages of our methodology:

3.1. Study population

The sample population was carefully selected from Al-Zaitoonah University in Jordan, a very prestigious institution known for its academic programs. This group of students represented different academic disciplines, providing access to the study a broad view of. Participants were mainly in the undergraduate age group, with a balanced mix of males and females and ages 18 to 25. Selection was made to ensure based on specific criteria related to the study that a representative sample of the university student population would provide a comprehensive understanding.

3.2. Study sample

The study sample consisted of 531 students randomly selected from Al-Zaytoonah University of Jordan who were engaged in distance learning during the COVID-19 pandemic. Participation was voluntary. This sample size was deemed sufficient to obtain a representative distribution of perspectives across different academic levels and backgrounds.

3.3. Survey design

A questionnaire survey was designed to assess students' cybersecurity awareness, attitudes, experiences, and behaviors related to distance learning. The survey had 32 questions using 5-point Likert scale responses to gauge agreement with statements about cybersecurity risks, policies, training, practices, and openness to learning. Question topics included: awareness of policies/resources, self-assessed preparedness, experiences with threats, cyber hygiene habits, handling of private data, reporting issues, and integrating cybersecurity into curricula.

3.4. Reliability and stability testing

Cronbach's alpha is a method of evaluating reliability that compares the amount of shared variation, or covariance, among the items that comprise an instrument to the amount of overall variance. The theory states that there should be a significant amount of covariance between the items in relation to the variance if

the instrument is reliable. The internal consistency and reliability of the questionnaire scale with several Likert answer questions were assessed using the Cronbach's alpha test. The stability coefficients for the resolution axes varied from 0.731 to 0.895, suggesting high dependability, while an alpha coefficient of 0.804 was obtained, showing strong reliability.

3.5. Study tool

To address the study's inquiries, a survey was conducted in two sections. The first section collects information about participant demographics while the second part focuses on the role of cybersecurity in dust learning. The questionnaire was distributed electronically through a link that was sent to the students.

3.6. The validity of the study tool

To ensure the validity of the questionnaire, it was reviewed by expert academic referees in Jordanian universities with specialized knowledge in scientific research and instruction. These experts evaluated the clarity and comprehensiveness of the questionnaire items in capturing key dimensions of cybersecurity. Based on the input from the referees, revisions were made to improve the questionnaire. Their feedback helped modify, refine, and enhance the questionnaire to make it more lucid, nuanced, and aligned with best practices in cybersecurity assessment. Engaging subject matter authorities in this arbitration process was valuable for strengthening the legitimacy and rigor of the instrument through peer critique and recommendations. The information gleaned from arbitrators with expertise in the field was crucial for bolstering and fine-tuning the questionnaire prior to broader administration. This scholarly critique and guidance refined the initial instrument to better embody cybersecurity facets relevant for the target audience.

4. RESULTS, ANALYSIS AND DISCUSSION

The analysis of the information gathered from participants via a questionnaire is the goal of this section. One of the methods used for data analysis was SPSS. This section also includes the approaches' results, which are followed by a discussion of the findings addressing various topics covered in the literature.

4.1. Results

The data in Table 2 indicates that 53% of the respondents were female respondents compared to 47% of male respondents. The percentage of students from IT specialty reached 73%, and for the others specialty, the percentage reached 27%. The students were distributed according to the academic years: 18% of them were first-year students, 19% were second-year students, 25% were third-year students, 38% were fourth-year students and above. Table 3 indicates the respondents' response to the questionnaire items related to the research question, which is what is the role of cybersecurity in enhancing students' security awareness during distance learning?

Table 2. Demographics of student survey participants

Variable	level	Frequency	Percentage
Gender	Male	252	84%
	Female	279	52%
Speciality	IT	390	73%
	Others	141	27%
Academic level	First year	93	18%
	Second year	135	25%
	Third year	153	29%
	Fourth year and above	150	28%

Where the results of the response for respondents from different educational levels showed that students agree to face cybersecurity risks while participating in distance learning at a rate of 79% $((84\%+67\%+80\%+85\%)/4)$ at various educational levels. The results of the respondents from different academic levels on the effective lack of awareness of cybersecurity in distance learning curricula showed a percentage of 77%. The response of the respondents to the item students' behaviors through distance learning affect their vulnerability to cyberattacks was 79% from the different academic levels. The response of the respondents to the paragraph students needs to be aware of the risks of sharing private information during distance learning was 92% of students at different academic levels. As for the response of the respondents to the item weakness in existence of legal and ethical measures when securing student data in distance learning, it was 92% at all academic levels. As for the students' response rate to the item "students are not encouraged to report potential cybersecurity incidents during distance learning" 79% at different levels of study.

This study provides valuable insights into students' cybersecurity awareness and preparedness in distance learning, revealing important gaps that need to be addressed. The survey results show students recognize online risks but lack comprehensive understanding, training, and support to practice secure behaviors. Significant percentages highlighted inadequate security education in curricula and institutional policies.

These findings demonstrate the need for a multifaceted cybersecurity approach tailored to online education. Relying solely on technical controls is not sufficient. Students are a critical human layer of defense, but require knowledge, skills, and encouragement to develop security-conscious habits online. Educational institutions must prioritize cybersecurity by integrating training into curricula, strengthening protections, establishing robust incident response, and nurturing an organizational culture valuing awareness.

Effective partnerships between academic leadership, faculty, IT staff, and students are essential to build cyber-resilient learning communities. Cyber hygiene and readiness must become shared responsibilities. This study provides a foundation for further research into specific educational interventions and expanding the scope to faculty and administrator perspectives. Enhancing cybersecurity engagement across educational communities will lead to safer distance learning ecosystems.

The survey results reveal that students recognize cybersecurity as an issue during distance learning, but lack sufficient awareness and training. 79% of respondents across all academic levels agreed that they face cybersecurity risks while participating in distance learning. This high percentage shows students are concerned about cybersecurity but likely feel unprepared to defend against threats. 77% reported an effective lack of cybersecurity awareness being integrated into distance learning curricula. 79% felt their own behaviors through distance learning affect their vulnerability to cyberattacks. 92% agreed that students need more awareness on the risks of sharing private information online. Another 92% saw weak legal and ethical measures for securing student data in distance learning environments. Finally, 79% said students are not encouraged to report potential cybersecurity incidents while engaging in online learning.

Overall, the data indicates gaps in both curricula and institutional policies/procedures around cybersecurity in distance learning. Students do not feel empowered to report issues, suggesting poor incident response programs. Weak protections also fail to prioritize the security of student data. These findings align with literature emphasizing the growing cyber risks in online education and the need for comprehensive security strategies. The results demonstrate student cyber hygiene and developing a "human firewall" are essential but currently underserved.

Table 3. Distance learning cybersecurity awareness survey results

Paragraph	Academic level	Frequency	Average
Students agree to face cybersecurity risks while participating in distance learning	First	78	84%
	second	90	67%
	third	123	80%
	Fourth and above	128	85%
Effective lack of awareness of cybersecurity in distance learning curricula	First	75	81%
	Second	81	60%
	Third	120	78%
	Fourth and above	130	87%
Students' behaviors through distance learning affect their vulnerability to cyberattacks	First	77	83%
	Second	99	73%
	Third	118	77%
	Fourth and above	124	83%
Students need to be aware of the risks of sharing private information during distance learning	First	84	90%
	Second	127	95%
	Third	138	91%
	Fourth and above	136	92%
Weak legal and ethical measures when securing student data in distance learning	First	84	90%
	Second	126	93%
	Third	136	89%
	Fourth and above	143	95%
Students are not encouraged to report potential cybersecurity incidents during distance learning	First	78	84%
	Second	95	70%
	Third	113	74%
	Fourth and above	129	86%

4.2. Analysis

The high percentage agreeing they face risks shows students are concerned but likely feel unprepared. Most see a need for better education on securely handling private data. The data reveals gaps in both curricula and policies/procedures around cybersecurity in distance learning. Students do not feel

encouraged to report issues, suggesting poor incident response programs. Weak ethical and legal protections also fail to prioritize student data security. These findings align with the literature emphasizing the growing cyber risks in online education and need for comprehensive security strategies. Student cyber hygiene and developing a “human firewall” are essential but underserved currently.

Research such as [12], [13] also highlight the need of cybersecurity knowledge in learning environments, which is consistent with your findings on students’ lack of awareness. Our conclusions regarding the necessity of all-encompassing cybersecurity plans are consistent with those found in [15] and [16], which address the significance of a robust security culture and layered defenses.

According to results, students are aware of the risks associated with cybersecurity, but they lack the necessary support and training to manage these risks effectively. This implies a mismatch between knowledge and useful cybersecurity abilities. The results also suggest that the particular cybersecurity issues associated with distant learning may not be sufficiently addressed by the institutional policies and practices in place. These findings align with a broader literature underscoring the need for robust cybersecurity protections and awareness in education. As online learning expands, sound security policies and training are crucial to safeguard institutions and students.

The present results highlight the value of integrating cybersecurity into academic curricula. Incorporating security education can help cultivate a proactive culture around technology safety among students. It equips them with essential competencies to navigate the digital landscape securely as they learn and interact online. By making cybersecurity literacy a priority, schools and universities can empower students to make informed decisions and approach threats vigilantly. Comprehensive training is key to promoting mindsets and behaviors that prioritize vigilance. As cyber risks permeate the learning process, building students’ knowledge, skills and precautionary habits is vital.

4.3. Discussion

This study reveals critical gaps in student cybersecurity readiness for distance learning. While students demonstrate baseline awareness of threats, they lack comprehensive understanding, skills, and supports to proactively navigate risks. A strategic, multidimensional approach is imperative for institutions.

To create a cyber campus and improve student behaviors and readiness it is recommended to incorporate security awareness into programs train students, on potential threats and best practices establish effective incident reporting and response mechanisms enhance data protection measures and foster an organizational culture that values cybersecurity. Achieving these goals necessitates an effort involving students, faculty members, IT staff and leadership. Prioritizing cybersecurity is crucial, in ensuring the security of distance learning environments. The research reveals that students who engage in learning often have deficiencies, in their understanding and application of cybersecurity principles. This is especially troubling considering the increased hazards connected to online learning.

The results show that comprehensive approaches that combine technological and human-centered methods are required to raise cybersecurity awareness. It is imperative that educational establishments give cybersecurity top priority while developing their curricula. The study emphasises the value of teaching students to be cautious and aware of cyberthreats as a “human firewall”.

5. CONCLUSION AND RECOMMENDATION

This study reveals important insights into the current state of students’ cybersecurity awareness and behaviors in distance learning environments. The survey results indicate that while students recognize cyber risks, they lack comprehensive understanding, training, and support to actively defend against online threats. Significant percentages of students highlighted gaps in security awareness education and policies within distance learning programs and curricula.

These findings confirm the need for a strategic, multilayered approach to enhance cybersecurity in online education as emphasized in the literature. Solely relying on technical controls is insufficient. Students are a critical human layer of defense, but they cannot develop security-conscious online habits without proper knowledge, skills, and encouragement. Educational institutions must make cybersecurity a priority by integrating training into curricula, establishing robust incident response programs, strengthening data protections, and promoting an organizational culture that values cyber awareness and vigilance. Equipping students to make secure decisions and act as a “human firewall” requires proactive partnerships between academic leadership, faculty, IT teams, and students. Cyber hygiene and readiness must become a shared responsibility. This study provides a foundation for further research into specific interventions that can empower students to reduce cyber risks. Additional work can also expand the scope to faculty and administrator perspectives and preparedness. Enhancing cybersecurity awareness and engagement across educational communities will lead to safer, more resilient online learning ecosystems.

This research recommends the urgent need to improve cybersecurity education for distant learners is suggested by this research. bringing attention to the discrepancy between students' knowledge and their ability to use cybersecurity in real-world situations, which shows that educational institutions must create thorough cybersecurity policies and training initiatives. Future studies and policy development can use this research as a foundation, with an emphasis on how crucial it is to adjust to changing cyberthreats and encourage a cooperative, human-centered approach to cybersecurity.

ACKNOWLEDGEMENTS

The authors would like to thank the Arab Open University, Saudi Arabia, and Al-Zaytoonah University of Jordan, Jordan, for providing the necessary scientific research supplies to implement this research. The authors extend their appreciation to the Arab Open University, Saudi Arabia for funding this work through Arab Open University (AOU) research fund No. AOURG-2023-009.

APPENDIX

Table 1. Overview of cybersecurity research in distance learning

Author (s)	What they did	What they found	Limitations
Verizon [9]	Analyzed data breaches in various sectors, including education.	Education sector was the second most breached industry after healthcare, indicating significant cyber risks in this sector.	The report is broad and not specifically focused on distance learning, limiting its applicability to this specific context.
Bandara <i>et al.</i> [10]	Examined cybersecurity threats and challenges for open universities during COVID-19.	Highlighted the importance of cybersecurity in distance learning and the need for robust strategies to mitigate risks.	The focus was more on general cybersecurity challenges rather than specific strategies or tools effective in an educational context.
Alawida <i>et al.</i> [11]	Identified top threats for teaching and learning during COVID-19.	Phishing, malware, and credential theft were the top threats, with lack of security controls and limited staff oversight as key issues.	The study was limited to the COVID-19 context and may not reflect the broader range of cybersecurity challenges in distance learning.
Kioskli <i>et al.</i> [12]	Investigated the relationship between cybersecurity awareness education and trained professionals.	Found insufficient cybersecurity awareness education leads to inadequately trained professionals.	The scope was limited to cybersecurity awareness and did not delve into specific technological solutions or policies in educational settings.
Homoliak <i>et al.</i> [13]	Analyzed insider threats in cybersecurity.	Highlighted the role of negligence, errors, or lack of training as unintentional insider threats.	The study's focus on insider threats means it may not fully address external cybersecurity threats relevant to distance learning.
Alshaikh <i>et al.</i> [14]	proposed a technique called ShieldFS that copies files when they are altered, saving the copy in a preserved area.	Ransomware attacks are on the rise and are expected to continue increasing due to the availability of ransomware codes and development kits.	The paper does not provide specific solutions for preventing or detecting ransomware infections.
French <i>et al.</i> [15]	Examined the current status and issues of BYOD (bring your own device) in organizations.	Discussed the cybersecurity implications of BYOD policies.	The study was not focused on distance learning or educational contexts, limiting its direct applicability to this field.
Veiga and Martins [16]	Developed an instrument to assess information security culture.	Emphasized the importance of a strong information security culture in organizations.	The study's focus on organizational culture may not directly translate to educational settings, particularly for students.
Chen <i>et al.</i> [17]	Explored organizations' information security policy compliance.	Discussed the effectiveness of stick or carrot approaches in policy compliance.	The study's corporate focus limits its direct applicability to educational settings, particularly in the context of distance learning.
Ki-Aries and Faily [18]	Proposed persona-centered information security awareness.	Suggested the effectiveness of personalized approaches to information security awareness.	The conceptual nature of the paper may not provide concrete strategies or evidence-based findings specific to distance learning.
Suwais and Alshahrani [19]	Examined the impact of VC on the academic performance of students at the AOU in Saudi Arabia.	found that the drop rates of students in VC-based courses were lower compared to F2F courses, indicating higher efficiency of the VC teaching method.	The sample size of the study was relatively small, with 200 students, which may limit the statistical power and representativeness of the results.

Table 1. Overview of cybersecurity research in distance learning (*Continued*)

Author(s)	What they did	What they found	Limitations
Abduljawad <i>et al.</i> [20]	proposed acceptance framework for e-learning in Jordan incorporates various factors such as awareness of e-learning, perceived benefits, and perceived risks.	The reliability analysis of the survey instrument shows that the constructs used in the study have high internal consistency, with alpha coefficients ranging from 0.71 to 0.90.	The paper does not provide specific numerical results or statistical significance values for the effects of perceived benefits, awareness, and perceived risks on e-learning usage.
Alotaibi and Alghamdi [21]	Studied faculty members' readiness to use an e-learning platform in Saudi Arabia.	Found high self-efficacy in using ICT tools but lower confidence in specific online teaching aspects.	Focused on faculty members, so it doesn't directly address student perspectives or specific cybersecurity issues.
Abduh <i>et al.</i> [22]	Analyzed Indonesian Twitter sentiments about online learning during the COVID-19 pandemic.	Revealed overwhelmingly positive sentiment towards online learning in Indonesia.	Limited to Indonesian context and public opinions on social media, which may not reflect broader or more nuanced perspectives.
Ayyoub <i>et al.</i> [23]	Analyzed data using SPSS to find degrees of awareness about cybercrimes and legal procedures related to e-crimes in e-learning.	Students had high awareness about general meaning of cybercrimes, and Female students were more aware than male students;	Only included students from one university in Jordan, so results cannot be generalized to all universities in Jordan.
Karim and Ali [24]	Compared the security features of virtual meeting applications in e-learning.	Found Google Meet to be most secure against cyber-attacks, followed by Microsoft Teams and Zoom.	Focused on specific virtual meeting applications, which may not encompass the full range of cybersecurity concerns in distance learning.
Chentouf and Bouchkaren [25]	Discussed the integration of blockchain technology in smart cities to enhance security and privacy.	Proposed an electronic voting model using blockchain to demonstrate its implementation in smart cities.	The focus on smart cities and blockchain technology limits its direct relevance to cybersecurity in distance learning environments.
Ahmed and Khorsheed [26]	Explored IT and OT integration in next-generation communication systems, including IoT in 5G networks.	Discussed the use of IoT communication and its architecture in data transfer and decision-making services.	The technical focus on IoT and 5G networks may not directly address specific cybersecurity concerns in distance learning environments.




REFERENCES

- [1] A. Derbas, N. Al-Ramahi, A. Hnaif, T. A. Alrawashdeh, and R. A. Mubaideen, "The effectiveness of e-learning system on students' of Al-Zaytoonah university of Jordan: a case study," in *2023 International Conference on Information Technology: Cybersecurity Challenges for Sustainable Cities, ICIT 2023 - Proceeding*, Aug. 2023, pp. 459–463, doi: 10.1109/ICIT58056.2023.10226073.
- [2] A. Alshahrani, "Readiness of higher education institutions for e-learning: a case study of saudi universities during the COVID-19 Pandemic," *International Journal of Advances in Soft Computing and its Applications*, vol. 13, no. 1, pp. 149–161, 2021.
- [3] A. Althunibat, F. Altarawneh, R. Dawood, and M. A. Almaiah, "Propose a new quality model for m-learning application in light of COVID-19," *Mobile Information Systems*, vol. 2022, pp. 1–12, Mar. 2022, doi: 10.1155/2022/3174692.
- [4] E. L. Amalia, V. A. Lestari, V. N. Wijayaningrum, and A. A. Ridla, "Automatic essay assessment in e-learning using winnowing algorithm," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 29, no. 1, pp. 572–582, Jan. 2023, doi: 10.11591/ijeecs.v29.i1.pp572-582.
- [5] A. Mughaid, S. AlZu'bi, A. Hnaif, S. Taamneh, A. Alnajjar, and E. A. Elsoud, "An intelligent cyber security phishing detection system using deep learning techniques," *Cluster Computing*, vol. 25, no. 6, pp. 3819–3828, May 2022, doi: 10.1007/s10586-022-03604-4.
- [6] H. Al-Masalha, A. A. Hnaif, and T. Kanan, "Cyber-crime effect on Jordanian Society," *International Journal of Advances in Soft Computing and its Applications*, vol. 12, no. 3, pp. 123–139, 2020.
- [7] C. Lin, D. Wu, and P. Li, "Developing a campus information security awareness program for college students," *Contemporary Issues in Education Research*, vol. 4, no. 5, pp. 5–15, 2011.
- [8] R. L. Mitchell, "Cybersecurity culture: counteracting cyber threats with positive security practices in education," Northwest Nazarene University, 2020.
- [9] Verizon "2021 Data breach investigations report," Vertizone, Jan. 2021.
- [10] I. Bandara, C. Balakrishna, F. Ioras, "The need for cyber threat intelligence for distance learning providers and online learning systems," *INTED2021 Proceedings*, 2021, pp. 9312-9321 doi: 10.21125/inted.2021.1947.
- [11] M. Alawida, A. E. Omolara, O. I. Abiodun, M. Al-Rajab, "A deeper look into cybersecurity issues in the wake of Covid-19: a survey," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8176-8206, 2022, doi: 10.1016/j.jksuci.2022.08.003.
- [12] K. Kioskli, T. Fotis, S. Nifakos, H. Mouratidis, "The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0," *Applied Sciences*, vol. 13, no. 6: 3410, 2023, doi: 10.3390/app13063410.
- [13] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight Into insiders and IT: a survey of insider threat taxonomies, analysis, modeling, and countermeasures," *ACM Computing Surveys*, vol. 52, no. 2, pp. 1–40, Apr. 2019, doi: 10.1145/3303771.
- [14] H. Alshaikh, N. Ramadan, H. A. Hefny, "Ransomware prevention and mitigation techniques," *International Journal of Computer Applications*, vol. 177, no. 40, pp. 31-39, 2020, doi: 10.5120/ijca2020919899 .
- [15] A. M. French, C. J. Guo, and J. P. Shim, "Current status, issues, and future of bring your own device (BYOD)," *Communications of the Association for Information Systems*, vol. 35, pp. 191–197, 2014, doi: 10.17705/1cais.03510.




- [16] A. Da Veiga and N. Martins, "Information security culture and information protection culture: a validated assessment instrument," *Computer Law and Security Review*, vol. 31, no. 2, pp. 243–256, Apr. 2015, doi: 10.1016/j.clsr.2015.01.005.
- [17] Y. Chen, K. Ramamurthy, and K. W. Wen, "Organizations' information security policy compliance: Stick or carrot approach?," *Journal of Management Information Systems*, vol. 29, no. 3, pp. 157–188, Dec. 2012, doi: 10.2753/MIS0742-1222290305.
- [18] D. Ki-Aries and S. Faily, "Persona-centred information security awareness," *Computers and Security*, vol. 70, pp. 663–674, Sep. 2017, doi: 10.1016/j.cose.2017.08.001.
- [19] K. Suwais and A. Alshahrani, "The impact of virtual classes on students' performance in open learning environments: the case of Arab Open University, Saudi Arabia," *Journal of Computer Science*, vol. 14, no. 1, pp. 14–22, Jan. 2018, doi: 10.3844/jcscsp.2018.14.22.
- [20] M. Abduljawad, A. Ahmad, K. M. Jaber, A. Al Thunaibat, E. A. Maria, A. Khasawneh, H. Hijazi, "Evaluating and adopting E-learning systems in Al-zaytoonah university of Jordan," *International Journal of Advances in Soft Computing and its Applications*, vol. 12, no. 3, pp.82-99, 2020.
- [21] R. Alotaibi and A. Alghamdi, "Studying faculty members' readiness to use Shaqra University e-learning platform," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 22, no. 3, pp. 1556–1564, Jun. 2021, doi: 10.11591/ijeecs.v22.i3.pp1556-1564.
- [22] M. Abduh, M. Hamka, T. Taniredja, A. Zainuddin, and W. N. Habiby, "Indonesian perceptions on online learning amidst COVID-19: a Twitter sentiment analysis," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 30, no. 1, pp. 567–576, Apr. 2023, doi: 10.11591/ijeecs.v30.i1.pp567-576.
- [23] H. Y. Ayyoub *et al.*, "Awareness of electronic crimes related to E-learning among students at the University of Jordan," *Heliyon*, vol. 8, no. 10, pp. 1-11, 2022, <https://doi.org/10.1016/j.heliyon.2022.e10897>.
- [24] N. A. Karim and A. H. Ali, "E-learning virtual meeting applications: A comparative study from a cybersecurity perspective," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 24, no. 2, pp. 1121–1129, Nov. 2021, doi: 10.11591/ijeecs.v24.i2.pp1121-1129.
- [25] F. Z. Chentouf and S. Bouchkaren, "Security and privacy in smart city: a secure e-voting system based on blockchain," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, pp. 1848–1857, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1848-1857.
- [26] A. K. Ahmed and A. A. Khorshed, "Open network structure and smart network to sharing cybersecurity within the 5G network," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 27, no. 1, pp. 573–582, Jul. 2022, doi: 10.11591/ijeecs.v27.i1.pp573-582.

BIOGRAPHIES OF AUTHORS






Adnan Ahmad Hnaif    is a full Professor at the Cybersecurity Department, Faculty of Science and information Technology, Al-Zaytoonah University of Jordan. He received his Ph.D. degree in Network Security from University Sains Malaysia–National Advanced IPv6 Centre and Excellence (NAV6) in 2010. He received his M.Sc. degree of Computer Science from Department of Computer Science in 2003, and obtained his Bachelor degree of Computer Science from the Department of Computer Science, in 1999/2000. His researches focus on the network security, network monitoring and documentation, computer networks and communications, wireless networks, and parallel processing techniques. He can be contacted at email: adnan_hnaif@zuj.edu.jo.



Areej Mofeed Derbas    is Assistant Professor at the Basic Sciences-Faculty of Arts, Al-Zaytoonah University of Jordan, she obtained her Ph.D. from the University of Jordan in 2020 in Sociology. She received her M.Sc. degree in 2002 Department of Sociology and her Bachelor's degree from Yarmouk University, Jordan in 1999. Her research focuses on development, social problems, family and childhood problems. She can be contacted at email: a.derbas@zuj.edu.jo.



Sally Almanasra    is an Associate Professor at the Faculty of Computer Studies, Arab Open University, Saudi Arabia. She received her Ph.D. in AI and Software Engineering from Universiti Sains Malaysia in 2014. Her main teaching and research interests include AI, information security, and game theory. She can be contacted at email: s.almanasra@arabou.edu.sa.