INTERNATIONAL JOURNAL OF SOCIAL SCIENCE, INNOVATION AND EDUCATIONAL TECHNOLOGIE (ONLINE) - ISSN: 2717-7130

Vol:5 Issue: 17 pp: 77-87

JEL Codes: I2, I 29

ER, A. K., DEMİRBAĞ, A., YILDIRIM, Y., BIDAK, M. (2024). **"A Look at Security Practices in Education"**. *International Journal of Social Science, Innovation and Educational Technologies (Online)*", Vol: 5 Issue: 17 pp: 77-87

Keywords: *school, education, security, risk management*

Article Type Review Article

A Look at Security Practices in Education

Arrived Date	Accepted Date	Published Date
29.12.2023	20.01.2024	31.01.2024

Ali Kemal ER[1] Adil DEMİRBAĞ[2] Yasin YILDIRIM[3] Mehmet BIDAK[4]

Abstract

The processes of change in education form the basis for discussing the effects of globalization, which is in a different dimension from centuries ago, in the flow of ideas, goods and people at the international level. Today, technology is 'tightening' the concepts of space and time, reducing their importance. This brings about a significant change in human activities around the world and is called globalization in many respects. Globalization first emerged prominently in the field of economics. With the development of computer technology, the removal of regulations and barriers in financial markets has led to the fact that entire economies have become dependent on the increasing flow of capital. At the same time, advances in telecommunications have led the global economy to a level of production coordination that has not been seen in many countries. This global shift in education affects learning processes and knowledge sharing, enabling students and teachers to be more integrated with an international perspective. In this context, education systems are faced with the need to adapt to the dynamics brought about by globalization. Innovative teaching methods, digital learning platforms, and cultural interaction are among the cornerstones of the global transformation in education.

This global shift in education affects learning processes and knowledge sharing, enabling students and teachers to be more integrated with an international perspective. In this context, education systems are faced with the need to adapt to the dynamics brought about by globalization. Innovative teaching methods, digital learning platforms, and cultural interaction are among the cornerstones of the global transformation in education. In this study, a perspective on security practices in education will be brought and the ways to ensure the security of digital learning platforms and information sharing will be focused.

[1] alikemaler061@gmail.com, Okan University, Business Administration Master's Program, Field of Educational Management, İstanbul/ TÜRKİYE

[2] oreas11@gmail.com, Süleyman Demirel University, Health Management Education Non-Thesis Master's Degree, Isparta / TÜRKİYE

[3] yasihat@hotmail.com, Institute of Social Sciences- Çankırı Karatekin University, Educational Management, Non - Thesis Master's Program, Çankırı / TÜRKİYE

[4] bidak06@gmail.com, Ankara University, Educational Administration and Inspection Master's Program, Ankara/ TÜRKİYE

http://dx.doi.org/10.54603/iss.201

INTRODUCTION

Today, the rapid development of technology and digitalization in education processes have brought security issues in education to the forefront. In this context, educational institutions should seriously consider security measures for digital learning platforms that facilitate students' and teachers' access to information. Security practices in education play a vital role in protecting against a variety of threats, keeping student data secure, and keeping learning environments reliable. In this context, addressing security in education requires a holistic approach that includes not only technological but also pedagogical and managerial dimensions.

Modernity is defined as a 'risk society' in terms of the risks posed by the uncertainty and unpredictable nature of the modern world for individuals, organizations and societies. In this context, security practices have become very critical in order to cope with these risks in the field of education. Inequality of opportunity in education and negative outcomes in continuous learning processes are related to equal access to information resources and diversity of competencies. Therefore, safety practices play an important role in combating these challenges in education and making learning environments safer and more inclusive (Pieczywok, 2018).

In this article, a literature on the importance of security practices in education, current threats and effective solutions against these threats will be presented.

Some Security Practices in Educational Institutions

Security training must be continuously improved to effectively respond to the complex challenges of the 21st century. This training should aim not only to ensure the safety of individuals but also to create safe spaces in the community. In order to cope with the rapidly changing realities of the 21st century, safety training must be constantly revised and rethought to adapt to these changing conditions.

The possibilities offered by security training encompass the concept of creating safe spaces for individuals to exist. These areas should include not only physical security, but also digital, financial and social security. Especially with factors such as digitalization and globalization, security training must be able to adapt to these new realities and strengthen the capacity to protect individuals in a multifaceted way.

In this context, developing the society in such a way that it can continuously learn and apply this knowledge is one of the main goals of safety education. By broadening society's understanding of security, enabling individuals to be more aware and prepared for risks can increase the resilience of not only individuals but also society in general. At this point, security training should be designed to cover not only individuals, but also institutions and all layers of society.

In educational institutions, various security practices and measures are taken to ensure the safety of students and employees. These practices cover physical, digital, and social security in the educational environment. Some of the security practices commonly used in education include:

1. **Physical Security:** Physical security measures are taken in school buildings, classrooms and other areas. These measures may include measures such as security cameras, alarm systems, closed-circuit television (CCTV) monitoring, ID cards and door locking systems. It can also be important to have visitor registration systems and security personnel in place at school entrances.

   In his study, Aydinan (2023) evaluated the current state of campus security in selected Higher Education Institutions in Nueva Ecija. The study was carried out in selected Higher Education Institutions in Nueva Ecija. The participants of the study were administrators, faculty and students, as well as security personnel, and questionnaires were used to collect relevant data.

The findings revealed that the five selected Higher Education Institutions adhered to the highly implemented security practices and procedures, with respondents' assessment indicating that they were implemented in terms of physical security, staff security, and document security. Among the fifteen problems, the three most important are: There are a limited number of CCTV cameras in strategic locations. Offices and laboratories do not have sprinkler systems and smoke detectors; There is inconsistency in the implementation of the NO-ID NO Entry Policy, Visitor ID and logbook, and the Gate Pass policy. The findings revealed that the five selected Higher Education Institutions did not differ in their current campus security.

Among the recommendations are that selected Higher Education Institutions should continue to maintain security practices that have already been put in place; It should be considered that security cameras should be installed in strategic locations and include elements including sprinkler systems. Security guards are required to constantly enforce the school's security policies, rules and regulations. Future studies should focus on safety measures against natural or man-made disasters that may occur within the campus and create a Safety handbook for the college, adopting the recommended safety manual to improve the implementation of campus safety.

2. **Digital Security:** Educational institutions strive to protect student and staff data by implementing digital security measures. These measures can include technical measures such as strong password policies, data encryption, secure network connections, and firewalls.

   Salvador et al. (2021) first focused on security issues using Moodle, Zoom, Blackboard, and edX, as well as best practices against security threats and cyberattacks on e-learning systems from the external network. From this study, it is understood that an encryption mechanism has emerged as the best technique to protect the confidentiality, integrity, and authentication of data on e-platforms. However, this is not strong enough to mitigate cybersecurity attacks on e-learning systems. Therefore, it is proposed to combine the encryption mechanism with other techniques such as biometric authentication, firewalls, IDS, digital watermarking, and security process models."
3. **Contingency Plans:** Educational institutions should be prepared for emergencies such as fires, earthquakes, terrorist attacks, etc. Contingency plans include protecting students and staff, informed evacuations, and emergency procedures. Contingency planning is a cornerstone for the resilience of educational institutions, necessitating comprehensive strategies to address a spectrum of emergencies ranging from natural disasters like fires and earthquakes to more complex scenarios such as terrorist attacks. These plans serve as a proactive roadmap, meticulously outlining protocols and procedures to safeguard the well-being of students and staff in the face of unforeseen events. Ensuring the protection of the educational community encompasses not only the physical safety of individuals but also considerations for data security, communication channels, and the continuity of essential operations. Informed evacuations form a crucial component, requiring clear communication channels and well-defined evacuation routes. These plans should be meticulously tailored to the specific characteristics of the institution, accounting for the layout of facilities, the number of occupants, and the potential risks associated with the geographic location. Regular drills and training exercises play a pivotal role in familiarizing students and staff with emergency procedures, fostering a culture of preparedness and ensuring a swift and organized response during actual incidents. Collaboration with local emergency services and authorities further enhances the effectiveness of contingency plans, creating a seamless integration with broader community response efforts. As educational institutions increasingly rely on technology for communication and operations, contingency plans should also encompass strategies for maintaining digital infrastructure and data integrity during emergencies. In essence, a well-crafted and regularly updated contingency plan not only mitigates the immediate impact of emergencies but also instills confidence within the educational community, assuring them that

the institution is equipped to handle unexpected challenges with a comprehensive and well-executed response.

5. **Education and Awareness:** It is important to educate and raise awareness of safety to school staff and students. Awareness of security risks by students and staff can help detect security threats in advance.
   Pieczywok (2018) has a content in which security education is discussed in the context of threats to human existence. The purpose of the article is to present the operational and technical (educational) aspects of Security Training to prevent threats. The main research objective adopted by the author is: What are the main threats to humanity and how to prevent them through Security Education? The focus is on educational issues and threats to humanity. The article consists of an introduction stating the importance of the topic. The most typical threats to human safety and how Security Training can prevent them are described later.
6. **Social and Emotional Safety:** A positive and safe school climate is important for students' emotional safety. Combating social and emotional bullying and promoting tolerance and respect among students increases safety in education.
7. **Environment and Facilities:** In order to keep the school environment safe, necessary arrangements should be made in areas such as school gardens and playgrounds. In addition, safety standards must be observed in special areas such as laboratories, workshops and gyms.
8. **Cyber Security:** The education sector should pay special attention to cyber security in order to create an effective defense mechanism against cyber threats. Measures in this area play a critical role in terms of the security of student data, the continuity of educational processes and the protection of the flow of information within the institution.
9. **Advanced Threat Detection Systems:** Educational institutions should adopt advanced threat detection systems to detect and prevent cyberattacks in advance. Rapid intervention can be provided by detecting security incidents instantly. The adoption of advanced threat detection systems stands as a critical imperative for educational institutions navigating the complex landscape of cybersecurity. In an era where cyber threats are becoming increasingly sophisticated and prevalent, these institutions must proactively fortify their digital ecosystems against potential attacks. Advanced threat detection systems leverage cutting-edge technologies such as artificial intelligence, machine learning, and behavioral analytics to identify patterns indicative of malicious activities. By continuously monitoring network traffic, user behavior, and system activities, these systems can swiftly detect anomalies or potential security breaches. The real-time nature of these detection mechanisms enables educational institutions to move beyond reactive approaches, intervening promptly to mitigate the impact of cyberattacks or even thwart them before any damage occurs. This level of proactive cybersecurity is particularly crucial in educational environments where a vast array of devices and networks are interconnected, creating a broad attack surface. Additionally, advanced threat detection systems contribute to threat intelligence by analyzing global trends and emerging risks, allowing institutions to stay ahead of evolving cyber threats. As educational institutions increasingly digitize their operations and embrace online learning platforms, the implementation of advanced threat detection systems becomes paramount for ensuring the confidentiality, integrity, and availability of sensitive information and critical systems. In essence, these systems serve as indispensable guardians, fortifying the cybersecurity posture of educational institutions and providing a vigilant shield against the ever-evolving landscape of cyber threats.

10. **Trained Security Personnel:** Specialized cybersecurity teams continuously monitor network security within the organization, identifying potential weak points and responding immediately. In addition, it is important to increase the level of awareness of all personnel through cyber security training.

Firewalls and Intrusion Detection Systems: Educational institutions should integrate powerful firewalls and intrusion detection systems to enhance network security. This can detect unauthorized access, preventing serious security breaches.

11. **Security Policies and Procedures:** Cyber security in education should include up-to-date and appropriate security policies. These policies provide guidelines to all stakeholders within the organization, ensuring that safety standards are maintained. Security policies and procedures are indispensable elements of a comprehensive cybersecurity framework in the realm of education. In an era where educational institutions increasingly rely on digital technologies and data-driven processes, the need for robust and up-to-date security policies cannot be overstated. These policies serve as a guiding beacon for all stakeholders within the organization, encompassing educators, students, administrative staff, and IT professionals. By articulating clear guidelines and standards, these policies establish a collective understanding of the importance of cybersecurity and the measures required to maintain a secure educational environment. They address a spectrum of concerns, including data protection, network security, access controls, incident response, and the responsible use of technology. Regular updates to these policies are crucial to staying abreast of evolving cyber threats and technological advancements. They should reflect the dynamic nature of the digital landscape, ensuring that security measures remain relevant and effective in safeguarding sensitive information and preserving the integrity of educational processes. Furthermore, comprehensive security procedures derived from these policies provide a systematic approach for responding to security incidents, mitigating risks, and fostering a culture of proactive cybersecurity awareness. In essence, security policies and procedures form the backbone of a resilient cybersecurity posture in education, promoting a collective responsibility for maintaining safety standards and fostering a secure learning environment for all stakeholders involved.
12. **Cyber Security Intelligence Management:** Educational institutions should be prepared for cyber security incidents and determine their response processes with an effective incident management plan. This allows for a quick and organized response to possible attacks.
13. **Secure Education Platforms**: If educational technology is used, it should be ensured that these platforms comply with cyber security standards. Features such as data encryption, secure connections, and session security are important to ensure the security of student data.
14. **Information Security Awareness**: Cybersecurity in education should include making students, instructors, and other stakeholders aware of potential threats. Information security awareness can be an effective tool in preventing attacks such as social engineering.

Cybersecurity in education ensures that technology is used safely and effectively, protecting educational processes and keeping student data safe. With constantly updated security strategies, educational institutions become more resilient to cyber threats and maximize students' safety.

The research carried out by Ondrušková and Pospíšil (2023) includes an important experiment with the aim of assessing the cybersecurity awareness of children in Czech primary schools. The study was designed to test children's ability to distinguish between risks online.

Within the scope of the research, preliminary tests were conducted and children's initial cyber security awareness was revealed. Then, the children were put through a certain training process and questionnaires were filled out after the training. The retests aimed to measure how much the education children received influenced their online behavior and improved their cybersecurity skills. The results showed that in the initial tests, children had only a moderate level of cybersecurity awareness. This indicates that children have a limited level of awareness

of the potential risks they may face online. On the other hand, it has been determined that the one-time training program has only a negligible impact on online behavior.

The research highlights the need for more comprehensive and effective educational strategies to increase children's awareness of cybersecurity. At the same time, it emphasizes the importance of providing online safety trainings in a continuous and participatory manner, going beyond being one-off. These findings provide valuable information for the development of more effective educational approaches for children to act safely and consciously in the digital environment.

In his study, Fouad (2021) draws attention as a field that investigates the inadequacies in cyber security in the higher education sector and conducts policy analysis, despite the increase in cyber threats in universities and colleges around the world, especially with the effect of the Covid-19 epidemic. By focusing on the predominance of high-profile cyber incidents, unlike the common, everyday threats in cybersecurity-related policymaking and academic discourse, it addresses an issue where the risks to which institutions of higher learning are exposed to cyber threats are often neglected. Unlike some studies that focus on cyber threats to educational institutions and technologies, and how risks are transferred to target institutions, this article examines the complexities of protecting higher education against cyber threats, noting that this is more than an information technology (IT) issue, it is a national policy issue.

In this context, it emphasizes the frequency with which cyber threats are ignored in the characteristics of higher education institutions, emphasizing the necessity of national strategies and security policies. This study argues that the measures to be taken at the level of educational institutions and the state should be considered from a broader perspective in solving the problems related to cyber security.

The study by Nuñez et al. (2023) highlights that higher education institutions (HEIs) are increasingly relying on digital technology for classroom and organization management, but this puts them at a higher risk from information and communication technology (ICT) security attacks. Recent studies show that HEIs are experiencing more security breaches in the field of ICT security, both cybersecurity and information security. The paper conducted a literature review to identify ICT safety practices that have been prevalent in HEIs over the past decade. The 11 journal articles profiled and analysed reveal the threats and protective measures on the security of HEIs in terms of organisational security, technological security, physical security, and standards and frameworks. Security tools and techniques are divided into specific categories by ways to protect ICT security. HEIs also implement general security standards and guidelines, such as the ISO 27000 series and Center for Internet Security (CIS) controls. Through synthesis and analysis on ICT security tools and techniques, this critical review aims to offer research directions on IT management that academic and technical managers will further explore to secure sources of information.

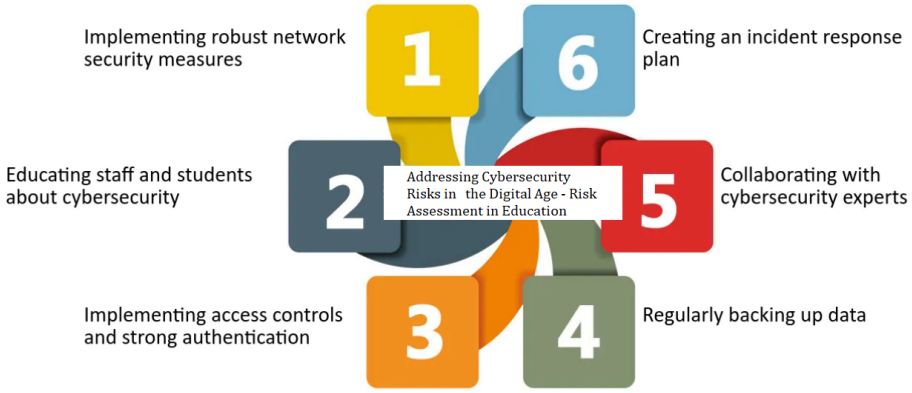

Figure 1. Addressing Cybersecurity Risks in the Digital Age- Risk Assessment in Education

Source: url-2

The emphasis on risk assessment, especially in the field of education, focusing on the cybersecurity risks brought about by the digital age, is shown in figure 2. In the context of the importance of creating safe learning environments in education, the term "Risk Assessment" refers to a process of identifying, measuring, and managing potential cybersecurity risks. In other words, the process of identifying cyber threats and developing safe learning environments to protect against these threats should be given importance. Cyber security in education should not forget the importance of ensuring that students and teachers are safe in the digital environment, focusing on maintaining education processes in a healthy and safe manner, and taking conscious precautions against cyber security risks while using the technological opportunities brought by the digital age.

15. **Data Security:** In today's digitally driven world, educational technology plays a critical role in shaping the learning experience of students. However, these major technological advances bring with them significant responsibilities, especially in terms of data security. Secure protection of sensitive student and organization data is a vital requirement for the sustainable success of educational technology.

    The benefits of educational technology include customized learning experiences for students, interactive content, and instant feedback. However, with these advanced features, an increasing amount of sensitive information is being generated and stored. Student information, test results, teacher evaluations, and other personal data must be protected so that this technology can be used effectively.

    Data security should be a priority for educational institutions and technology providers. Therefore, the adoption of strong encryption methods, secure network infrastructures, and up-to-date security protocols is of paramount importance. In addition, transparency and legal compliance should be observed in the collection, processing, and storage of student data (Francis, 2023).

    The future of edtech will not only enrich the learning experience of students, but will also improve data security standards and practices. At this point, the cooperation of all stakeholders in the sector by prioritizing student privacy and data security will contribute to the creation of a sustainable educational technology ecosystem.

    Here are some best practices for ensuring data security in education technology (Francis, 2023):

1. **Regulatory Compliance:** Full compliance with key data protection laws, such as GDPR, is critical to ensuring the trustworthiness of digital education platforms and the privacy of student data. Understanding regional legal requirements and ensuring full compliance with these regulations enables educational institutions to fulfill their responsibilities.
2. **Encryption and Authentication:** Adopting strong encryption methods for the security of data creates an important layer of defense during transmission and storage. Multi-factor authentication offers an additional level of security by empowering users to secure access.
3. **Regular Security Audits:** In order to identify the strong and weak points in the system, regular security audits detect potential risks in advance and provide timely intervention. This allows for the continuous strengthening of educational technology.
4. **Employee Training and Awareness:** Regularly training all staff on data security protocols and best practices to minimize human error creates a preventative strategy to prevent security breaches.
5. **Data Minimization:** Collecting only the data necessary for the educational process and limiting access to authorized personnel maximizes the security of student information and reduces potential risks.
6. **Secure Cloud Storage:** The cloud storage provider's compliance with industry security standards should be reviewed regularly, and security measures should be updated on an ongoing basis.
7. **Regular Backups:** Automatic backup processes are an important step in ensuring the security of critical training data and being ready for possible data loss. Regular backups play a pivotal role in safeguarding critical training data and establishing a robust defense against potential data loss. The automation of backup processes stands as a cornerstone in this endeavor, eliminating the reliance on manual interventions that are susceptible to errors and oversights. By instituting automated systems, data protection is fortified, ensuring resilience in the face of accidental deletions, hardware failures, software bugs, or other unforeseen circumstances. The frequency of backups should be meticulously calibrated to the dynamic nature of the training data, with considerations for daily or even more frequent backups for highly volatile datasets. Versioning in backups becomes imperative for training data, enabling a historical trail of changes and facilitating the precise identification of specific versions when needed. Geographical diversification of backups, encompassing offsite storage and redundancy, provides an additional layer of security against disasters or infrastructure failures. Encryption of backed-up data safeguards it from unauthorized access, a critical concern especially when dealing with sensitive information. Regular testing of the restoration process validates the efficacy of the backup strategy, ensuring that data can be successfully recovered when required. Thorough documentation of the backup process, coupled with the establishment of monitoring systems and alerts, contributes to the overall reliability and maintainability of the backup infrastructure. Periodic policy reviews guarantee that backup strategies remain aligned with evolving data requirements and business objectives. In essence, the meticulous implementation of regular, automated backups is paramount for sustaining the security, integrity, and accessibility of critical training data, forming an integral component of a comprehensive data management strategy.
8. **Incident Response Plan:** A comprehensive incident response plan for rapid response minimizes and aims to contain potential security breaches.
9. **Cooperation with Reputable Vendors:** When choosing technology vendors, it is important to choose those with reliable backgrounds in terms of data security. Third-party services should be thoroughly reviewed and evaluated beforehand.

10. **Transparent Privacy Policies:** Sharing privacy policies openly with stakeholders builds trust by increasing transparency and ensures that everyone is aware of data processing processes.

11. **Regular Updates and Patch Management:** Regular updates and patch management to software and applications are important to address security vulnerabilities and prevent potential exploitation.

12. **Network Security:** Firewalls, intrusion detection systems, and regular network monitoring to secure networks are an important component to prevent unauthorized access.

By adopting these best practices, educational institutions and technology providers can ensure the security of student data and promote the effective use of technology by creating a trustworthy educational environment.

In the midst of the challenges of the digital age, data security is more critical than ever today. According to Statista's estimates, the worldwide data security market is expected to reach $10.78 billion by 2028; This symbolizes a significant increase from the $5.98 billion value in 2023. However, in 2023, only 13% of people worldwide will have their data secure. Therefore, there could not be a more critical time to implement data security right now. This requires the adoption of best practices that apply in every industry.

The higher education sector should also be taken into account in this context. If you're dealing with student and institute data, it's even more critical to have clear policies and processes in place, implement them effectively, and update them regularly. Here are 10 best practices for higher education data security:

1. **Stay Informed:** Understanding data protection regulations and aligning them with existing processes can be challenging. That's why it's important to ensure that your team understands these regulations and shares up-to-date information.
2. **Know What You Have:** Maintaining a data inventory and monitoring its usage will help you develop a comprehensive plan for protecting data categories.
3. **Educate Staff and Users:** Review policies, educate staff, and discuss different scenarios to raise awareness about security.
4. **Evaluate Third-Party Vendors:** Assessing the trustworthiness of your business partners is important for your data security.
5. **Spread the word:** Clearly sharing your data usage, policies, and reasons can increase stakeholder support.
6. **Implement Multi-Factor Authentication:** Multi-factor authentication enhances security measures across systems and accounts.
7. **Update and Patch Systems Regularly:** Up-to-date software and applications reduce known vulnerabilities and strengthen your data security.
8. **Encrypt Sensitive Data:** Encryption prevents unauthorized access by converting data into an unreadable format.
9. **Conduct Regular Security Assessments:** Regular security assessments are helpful in identifying vulnerabilities and assessing the effectiveness of control processes.
10. **Create an Incident Response Plan:** An incident response plan strengthens your ability to respond quickly and effectively to security incidents.

Adopting these best practices can provide a strong defense for higher education institutions against potential data breaches and cyber threats. However, this process requires continuity and cooperation (url-1)

Results

Safety practices in education aim to create not only physical safety but also a positive learning environment by ensuring the safety of students and staff. A safe educational environment has the potential to increase students' achievement, as it makes students feel safer, which positively impacts their learning process. At the same time, it increases the efficiency of educators, allowing them to guide students more effectively. Security practices can also significantly improve the quality of education. In an environment where students and staff feel safe, learning becomes more effective and sustainable. This can increase students' engagement in class, strengthen their interactions, and positively impact the overall educational experience.

As a result, safety practices in education are of vital importance. These practices not only provide a safe physical environment, but also increase the achievement of students, increase the effectiveness of educators, and improve the quality of education in general. Therefore, creating and maintaining a safe educational environment is one of the essential elements of a successful education system.

In addition to ensuring the physical safety of students and staff, security practices in education should also cover another dimension that is gaining importance in today's digital age: cybersecurity. Integrating cybersecurity in education is a critical step in ensuring the overall information security of digital learning platforms, student information, and educational institutions. This includes taking advanced security measures to ensure that students' personal data is protected and that their online learning process is secure. Educational institutions should guide students and staff on how to protect against digital threats by organizing cybersecurity training programs and awareness campaigns. In addition, emphasis should be placed on basic cybersecurity practices such as the use of strong passwords, secure internet browsers, up-to-date software, and anti-virus programs.

In this way, expanding the scope of security practices in education to include cybersecurity will enable students to learn and share information safely in a digital environment, while also making educational institutions more resilient to cyber threats.

Acknowledgment: The authors have not received financial support from the University or any other institution/organization. The authors are grateful to the journal's anonymous reviewers for their extremely helpful suggestions to improve the quality of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

Aydinan, J. J. (2023). Higher Education Institutions' Security Capability the Leads to the Creation of Standardized Campus Security System. *Journal For Educators, Teachers and Trainers. 14*(2), 356-369. https://doi.org/10.47750/jett.2023.14.02.034

Fouad, N. S. (2021) Securing higher education against cyberthreats: from an institutional risk to a national policy challenge, *Journal of Cyber Policy, 6*(2), 137-154, DOI: 10.1080/23738871.2021.1973526

Francis, D. (October 11, 2023). Ensuring Data Security in Education Technology: Best Practices. https://www.linkedin.com/pulse/ensuring-data-security-education-technology-best-delton-francis/

Nuñez, M., Palmer, X.-L., Potter, L., Aliac, C. J., & Velasco, L. C. (2023). ICT Security Tools and Techniques among Higher Education Institutions: A Critical Review. *International Journal of Emerging Technologies in Learning (IJET)*, *18*(15), pp. 4–22. https://doi.org/10.3991/ijet.v18i15.40673

Ondrušková, D., & Pospíšil, R. (2023). The good practices for implementation of cyber security education for school children. *Contemporary Educational Technology, 15*(3), ep435. https://doi.org/10.30935/cedtech/13253

Pieczywok, A. (2018). Security Education in dangerous times. *Security and Defence Quarterly, 21*(4), 7-22. https://doi.org/10.5604/01.3001.0012.6497

Salvador, L. C. R., Llerena, C. L. A., Nguyen, H. P. D. (2021). Digital Education: Security Challenges and Best Practices. *Security Science Journal*, 2,65-76 https://doi.org/10.37458/ssj.2.2.4

url-1: https://www.watermarkinsights.com/resources/blog/5-best-practices-for-data-security-in-higher-education

url-2: https://fastercapital.com/content/Risk-Assessment-in-Education--Creating-Secure-Learning-Environments.html