Journal of Posthumanism
2025
Volume: 5, No: 2, pp. 487–501
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i2.434

Implementation Security and Privacy in the Era of Industry 4.0 to Protect Digital Attacks on Health Profession Students: SOAR Analysis

Imma Rachayu[1], Yatim Riyanto[2]*, Utari Dewi[3], Fitri Maiziani[4], Ramazan[5], Suci Perwitasari[6], Ratih Wulandari[7]

Abstract

Health Profession Students are Generation Z potential targets in today's digital world. However, in the era of Industry 4.0, technological developments also impact high risks to security and privacy. Therefore, efforts to increase digital security and privacy awareness are the top priorities to protect against digital attacks as a threat to students' health. This research aims to conduct data mapping precisely where students' online activities can be explored in detail so that the threat of digital attacks can be overcome with practical strategic steps using SOAR analysis. The research uses descriptive quantitative methods with a structured questionnaire survey approach and a sample of 372 university students with a health major. The results of the study show an overview of student activities in the digital world, namely the use of passwords on systems they do not know the validity of, low knowledge about the use of software as a two-step security tool, and students behave passively when they become victims of digital crime. Strategic steps in protecting against digital attacks include strengths, opportunities, aspirations, and results. This research offers a robust strategic basis for formulating a curriculum related to security and privacy awareness policies for students in overcoming digital threats in the industry 4.0 era and designing a program plan to engage students in digital literacy as agents of change actively. Future research should analyze Security and Privacy in Industry 4.0 to protect against digital attacks, expanding the sample to various Indonesian universities and study programs.

Keywords: *Digital Attack, Health Profession Students, Privacy, Security SOAR Analysis*

Introduction

Data protection and personal information are rights protected by the government (Echevarría et al., 2015; Oliveira & Dias, 2023). Personal data has become a crucial issue in today's digital era (Bilić & Žitko, 2024; Gómez-Barroso, 2018), thereby increasing the concern of citizens to ask for high security and privacy protection against digital attacks that occur (Rafiq et al., 2022). The digital attack that occurs in the world today is in the form of Distributed Denial of Services (DDoS) (Falowo & Abdo, 2024), operational disruption in the economic sector (Riggs et al.,

[1] Universitas Negeri Surabaya, Indonesia, Email: imma.22034@mhs.unesa.ac.id .ORCID iD: https://orcid.org/0000-0001-5766-9432 .Universitas Dehasen Bengkulu, Indonesia, Email: immarachayu@unived.ac.id
ORCID iD: https://orcid.org/0000-0001-5766-9432
[2] Universitas Negeri Surabaya, Indonesia, Email: yatimriyanto@unesa.ac.id (* Correspondence author). ORCID iD: https://orcid.org/0000-0002-5011-8379
[3] Universitas Negeri Surabaya, Indonesia, Email: utaridewi@unesa.ac.id. ORCID iD: https://orcid.org/0000-0003-3369-497X
[4] Universitas Negeri Surabaya, Indonesia, Email: fitri.22020@mhs.unesa.ac.id. ORCID iD : https://orcid.org/0009-0006-2325-4806
[5] Universitas Negeri Surabaya, Indonesia, Email: ramazan.22003@mhs.unesa.ac.id
[6] Universitas Negeri Surabaya, Indonesia, Email: suci.23022@mhs.unesa.ac.id. ORCID iD: https://orcid.org/0009-0004-9102-2244
[7] Universitas Negeri Surabaya, Indonesia, Email: ratih.23027@mhs.unesa.ac.id

2023), Modern Progressive Pitfall (MPP) (Rao et al., 2023), Digital Platforms That Accelerate Post-Covid 19 (Ahmad et al., 2022).

Data protection and personal information are rights protected by the government (Echevarría et al., 2015; Oliveira & Dias, 2023). Personal data has become a crucial issue in today's digital era (Bilić & Žitko, 2024; Gómez-Barroso, 2018), thereby increasing the concern of citizens to ask for high security and privacy protection against digital attacks that occur (Rafiq et al., 2022). The digital attack that occurs in the world today is in the form of Distributed Deniel of Services (DDoS) (Falowo & Abdo, 2024), operational disruption in the economic sector (Riggs et al., 2023), Modern Progressive Pitfall (MPP) (Rao et al., 2023), Digital Platforms That Accelerate Post-Covid 19 (Ahmad et al., 2022).

The Industrial Revolution 4.0 is a life activity that is integrated with digital technology, especially for Generation Z. In this era, individual mental health is a new challenge that has never been focused on maturely, so this concern must be urgently solved (Chen et al., 2021). The challenges of digital attacks include data tampering, identity and money theft (Jia et al., 2020; Nakamura et al., 2020; Singamaneni et al., 2022), Malware and phishing attacks (Al-Khater et al., 2020; Coyac-Torres et al., 2023; Mishra, 2023). With various digital facilities available today, there are many digital platforms, social media, artificial intelligence, and online learning environments, so connectivity can continuously trigger levels of anxiety, anxiety, depression, insomnia, and anti-social face-to-face (Coyac-Torres et al., 2023). However, various research papers have not entirely focused on mapping related to security and privacy in the current era, so the low mapping in students' online activities causes the risk of academic performance disruption, so student activities are difficult to control against technology, which results in a decrease in the potential for professional performance as a superior health worker candidate and hinders the creation of early data mapping.

In the digital era, security and privacy are hot topics where personal identities are accessed online. Results of metadata show that the majority of privacy of big data applications with a content and hybrid approach model in overcoming security challenges and breaches of big data is a hot issue in today's digital era (Rafiq et al., 2022). Various aspects of life, especially education, have been significantly influenced by the rapid growth of digital technology, especially post-COVID-19 (Bozzi, 2024; van der Sanden et al., 2024). Digital devices and platforms have become increasingly popular among college students, but they have an impact on mental health and the way they access information (Aguilera, 2015; Bucci et al., 2019; Figueroa & Aguilera, 2020), so they become potential targets in digital threat attacks. Efforts to improve digital security for health students are the main topic of this study. Institutions' role in integrating the curriculum with digital citizenship courses is significant for students who behave online and responsibly (Althibyani & Al-Zahrani, 2023).

However, there is still a lack of comprehensive data to find concrete data on how to carry out effective, adequate safety precautions for health students. The limitations of research that focuses on the role of students who have the potential to become victims of online crime are caused by the form of the carelessness of students in leaking passwords on systems that are not trusted for their validity and their limitations in using software to secure data from viruses or personal data theft so that the system is complex to track the threat of cybercrime faced by students. They become passive when they become victims of the aforementioned digital crime. This research is essential because health diploma students are the most vulnerable targets of digital attacks due to

the weak ability of students in digital security literacy. This research aims to map out special strategies in protecting against digital attacks on health diploma students and increase student awareness about the importance of preventing digital attacks in the era of the Industrial Revolution 4.0. Based on this, the researcher conducted an in-depth data survey related to security threats to health vocational students and provided technical support by involving students to become agents of change against digital attacks.

Literature Review

Industry 4.0 is a series of transformations of the construction industry into the era of intelligent construction. Various digital components are integrated with advanced technology so that they can create an interconnected ecosystem between digital and physical components, including the BInternet of Things, big data, cloud computing, artificial intelligence, and Building Information Modelling (You & Feng, 2020), virtual reality, as well as a manufacturing system that is integrated commercially and industrially (Bednar & Welch, 2020). The goal is to increase productivity and efficiency by utilizing the Internet of Things (IoT) and wireless sensor networks (WSN) (Majid et al., 2022). However, these challenges bring benefits and new challenges regarding data security and privacy (N. F. Khan et al., 2023; Marko et al., 2024). The vulnerabilities that occur include hacking caused by a lack of security, data collected by IoT devices being vulnerable to being accessed without the owner's permission, and Botnet attacks, including cyberattacks. In addition to IoT devices, Big Data analysis has vulnerabilities through the misuse of sensitive or stolen personal data, resulting in privacy violations (M. A. Khan & Salah, 2018). In addition to IoT, other technologies that are developing in this era are; Social networks and crowdsourcing (Wang et al., 2019). Cyber security often occurs due to the low digital literacy skills of students, and they have very little understanding of digital ethics, cyber risks, and how to protect personal data (Firat, 2023; Martins Van Jaarsveld, 2020; Pangrazio & Selwyn, 2019). Based on the results of previous research, it is stated that there is a need for cybersecurity integration in a series of lecture curricula, workshops on cybersecurity, and qualified device security infrastructure (Firat, 2023; Saeed, 2023). Health students are more likely and focused on clinical science (RISET & TINGGI, 2020)), so they are less exposed to learning related to cybersecurity, lack awareness of violations of personal data theft, and are unaware of any sanctions against online harassers. SOAR analysis is a strategic analysis model that evaluates and develops the institution's potential. SOAR analysis consists of Strengths, Opportunities, Aspirations, and Results (Kumar et al., 2023). This analysis has positive benefits, including strategies for how to involve policymakers in the strategic planning process that focuses on positive and constructive things so that it can focus more on commitment to the future (Harding et al., 2022; C. Y. Hong et al., 2020; Vardopoulos et al., 2023).

Methods

The research design uses descriptive quantitative. Samples are recruited from several universities with majors in the field of Health, related to the Diploma (D3) Midwifery, Nursing, and Nutrition program with an age range of 18 to 23 years, as well as male and female genders. The design was chosen to explore concrete data with a structured questionnaire survey approach with concerns about security and privacy, victims of online crime, and the risk of crime in the current digital world, as well as a strategic plan using SOAR analysis. The population of this study is health vocational students in three study programs (Midwifery, Nutrition, and Nursing) and three different universities: Bengkulu State University, Bengkulu Ministry of Health Polytechnic, and

Dehasen University of Bengkulu. This study's sample consisted of 124 people in the three study programs, so the total sample involved was 372. The sampling technique uses simple random sampling, so each study program has the same opportunity to be selected as a sample in the research. The instrument uses a questionnaire using a Likert scale model (1-6) to measure students' habits about digital security. The research procedure is carried out by developing instruments, validating instruments by experts, testing instruments, distributing questionnaires, collecting data, and processing data with the results of recapitulation in the form of data visualized through graphs and tables. The data is based on this descriptive quantitative method to analyze the factors that affect digital security attacks using a survey platform with anonymous data that focuses on collecting and recapitulating results in average and percentage values without identifying individuals personally. The researcher ensured that the anonymous data collection procedures were well designed to maintain the respondents' privacy, security, and trust level so that the data collected became unbiased and representative for descriptive purposes.

Results and Discussion

The Development of Questionnaire Instruments through Validation

For six months, the research was carried out from the development of questionnaire instruments through validation carried out by two validators who were experts in psychology and the media then, a trial process was carried out with samples from the S1 Computer Education study program with several tests on one by one respondent and small group tests at low, medium and high skill levels, then the questioner was distributed as many as 384 respondents with an age range of 18-23 years who came from diploma students health, which includes; (n=124) in the D3 Midwifery study program, (n=124) in the D3 Nursing study program and (n=124) D3 Nutrition. In this study, male respondents (n=25) comprised 6,5% of the total sample, and women (n=359) comprised 93,5%.

The results of the experts' recapitulation of the instrument validation test were declared feasible, and then a questionnaire was distributed in the trial process with one-by-one respondents, as many as three students who had low, medium, and high levels of ability. The results of the recapitulation of the questionnaire trial with one-by-one respondents are as follows:

No	Level of ability	Study Program			Average (%)
		Midwifery (%)	Nursing (%)	Nutrition (%)	
1	Low	90	93	98	93,7
2	Medium	95	96	94	95,0
3	High	96	98	97	97,0
Total Average					95,2

Table 1 Results of the questionnaire trial recapitulation one by one respondent

Based on the table above, it can be seen that the questionnaire related to cyberpsychology for health students has categories related to internet addiction, impact on social relationships, privacy and security concerns, digital well-being, social comparison, and self-esteem, impact on social relationships, fear of missing and cyberbullying. This questionnaire design trial involved three

students with low, medium, and high ability levels. The results of the recapitulation stated that the average score of students with low ability levels in the three universities was an average percentage of 93.7%; in contrast, the medium ability category it had an average percentage of 95.0%, and the high category had an average percentage of 97.0%. The results of the average percentage recapitulation of the three universities show that the average percentage is 95.2%, so it is declared suitable for use without revision.

No	Level of ability	Study Program			Percentage (%)
		Midwifery (%)	Nursing (%)	Nutrition (%)	
1	Low	95	97	95	95,7
2	Medium	96	96	98	96,7
3	High	100	98	98	98,7
Total Average					97,0

Table 2 Results of the questionnaire trial recapitulation small group

The data referring to the table above, it can be seen that questionnaires related to cyber security and privacy for health students have categories related to worries about security and privacy, reporting to the authorities if they experience online harassment, being victims of online identity theft getting threats through social media, providing passwords to systems whose validity is not trusted, online crime is complex to detect by tracking systems by victims, scanning device using security software periodically. This questionnaire design trial involved nine students with low, medium, and high ability levels. The recapitulation results stated that the average score of students with low ability levels in the three universities was 95.7%, the medium ability level had an average percentage of 96.7%, and the high ability level showed an average percentage of 98.7%. Based on the average percentage recapitulation results of the three universities, the average percentage is 97.0%, so it is declared suitable for use without revision.

Table 3: Summarizes the results of student activities related to privacy and security concerns

Source: Processed recapitulation of respondent, (2024)

Category of security and privacy	Study Programs		
	Midwifery (%n=124)	Nursing (%n=124)	Nutrition (%n=124)
Worried about security and privacy	78,6	78,6	81,7
Report to the authorities if you experience online harassment	48,9	46,6	44,9
Victims of online identity theft	73,1	76,1	74,2
Getting threats through social media	69,5	64,4	68,9
Providing passwords to systems whose validity is not trusted	84,1	82,5	80,1
Online crime is difficult to detect by tracking systems by victims	80,1	74,2	78,2
Scanning devices using security software	46,5	45,1	48,2

periodically.			

Cyber of security and privacy on aspects: in the first activity, students showed that they were worried about privacy security when using online applications; midwifery students showed an average percentage of 78.6%, then nursing students had an average percentage of 78.6%, and nutrition students on the average percentage of 81.7%. In the second activity, students can report to the authorities if they experience online harassment; for midwifery students, it showed that the average percentage is 73.1%; for nursing students, the average percentage was 76.1%; and for nutrition had an average percentage of 73,1%. The third describes students about victims of online identity theft; midwifery students showed an average percentage of 76,1%, nursing students had an average percentage of 64.4%, and nutrition students had 74,2%. In the fourth activity of getting threats through social media, midwifery students showed an average percentage of 69.5%, nursing students had an average percentage of 64.4%, and nutrition students had a percentage of 68.9%. The fifth activity described students providing passwords to systems whose validity is not trusted; midwifery students showed a mean percentage of 84,1%, nursing students own an average percentage of 82,5%, and nutrition students had an average percentage of 80,1%. The sixth activity describes students doing online crimes that are difficult to detect by tracking systems by victims; midwifery students showed an average percentage of 80,1%, nursing students showed an average percentage of 74,2%, and nutrition students showed an average percentage of 78,2%. The seventh activity describes students scanning devices using security software periodically; midwifery students showed an average percentage of 46,5%, nursing students showed an average percentage of 45,1%, and nutrition students showed an average percentage of 48,2%.

The Discuss of the Category of Concerns about Security and Privacy in the Midwifery and Nursing Study Program

The fundamental question related to the results of the questionnaire recapitulation showed that the category of concerns about security and privacy in the midwifery and nursing study program showed the same result with a percentage of 78.6%. However, the nutrition student group showed a higher percentage figure of 81.7%. The percentage results showed a high similarity value related to students' awareness of the risks of online activities that they do every day. The distribution of student activities that they do in the aspect of security and privacy as a risk includes their negligence in using passwords in the system so that they are easily detected and sometimes share passwords with friends or other parties without being filtered first, then they also ignore the notifications that appear on their devices, update the status on social media related to their whereabouts at any time along with location details, The digital devices they have are not accompanied by an antivirus that supports the device, clicking on links that suddenly appear on the device and are not recognized for their legitimacy, so it is difficult to track them if they become victims due to their limited ability to access software devices, as well as allowing new applications to be downloaded to access personal data without prior permission. This finding aligns with what was done (Huijts et al., 2023). Awareness of the risks to security and privacy is still at a low level, resulting in high concerns, in addition, attacks carried out directly can increase the difficulty of recognizing and detecting cyber-attacks. Cyber-attacks can be overcome using one of the human-computer interaction approach (HCI) strategies, where the HCI principle can empirically analyze and evaluate the framework in strengthening security against evolving digital threats (Albarrak, 2024). In line with the above research, *Cyber Threat Intelligence (CTI) protects the digital system's cyber security* (Eltayeb, 2024b). *Then, some digital twins* can explore the role

of Artificial Intelligence (AI) in maintaining platform cybersecurity and digital integration with technology (Homaei et al., 2024).

In addition, in the category of reporting online harassment to the authorities, all students showed data recapitulation results below 50% related to online harassment reporting. Nutrition students achieved the lowest results, with an average of 44.9%. This is because the surrounding social environment is not supportive, so they are used to being shy and worried about being humiliated if they become victims of crime. Sometimes the act of online harassment is considered normal, so victims are more likely to be silent and ignorant, as well as low education related to how to report the harassment to the authorities. Previous research has stated that the role of technology is like a double-edged sword, where technology can be used as a protector and also as a threat to victims of online violence (Boethius et al., 2023). However, there is a criminal law that deals with digital crimes against women that combines aspects of every digital character with gender-based violence on a more stringent legal standard (Polyzoidou, 2024). Gender-based violence directed at women shows that after covid 19 there has been an increase in online violence against women on many platforms. The violence reveals various socio-technical problems that hinder protection for victims and appropriate punishment for online criminals (Amaral et al., 2022). The highest social media platforms as a source of online harassment and digital violence include; Facebook, Twitter and Email (Burns et al., 2024).

Based on data recapitulation, victims of online identity theft show that nursing students have the highest average percentage of 76.1%, followed by nutrition students with an average rate of 74.2%, and the lowest in midwifery students with an average percentage of 73.1%. The triggering factor for the theft of student data online is due to their activities that demand to interact online through online learning that uses a system that requires students to fill in personal data and enter online groups to submit assignments or projects as well as information related to the courses they are effective at. The growth of online crime in the form of theft of personal data with unauthorized access is a problem in every country and continues to increase because it is caused by the pattern of an anonymous and difficult-to-control internet framework, making it more vulnerable to theft (Dutta, 2021; Rahim et al., 2020). The types of data leaks experienced by victims include personal data in the form of passwords, financial information, and confidential data, which can be financially detrimental and threaten the victim's life (Alzubaidi, 2021). In addition, online behavior is vulnerable to theft through social media activities, entertainment, work, and instant messaging (Gan et al., 2024) and email (Sturman et al., 2025).

Threats through social media experienced by most students are above 60%. The highest average in the midwifery student group has an incidence rate of 69.5%, which is caused by the tendency of the female midwifery students who have a level of vulnerability in commenting related to reproductive health awareness content. Meanwhile, the group of nursing and nutrition students carried out activities in the form of disseminating information related to their practice experience, promoting a healthy lifestyle through social media without realizing that there were risks they had to face related to privacy settings such as who can see posts and attach contact information. However, in addition to the threats mentioned above, there are other threats that students are not aware of, namely technology-based stalking activities and sending sexual messages or images that are not suitable for students to open (DeKeseredy et al., 2019). Victims of harassment or stalking through digital devices result in high levels of depression and anxiety in activities (Maran & Begotti, 2019), sadness, and loss of self-confidence as emotional and physical symptoms (Begotti et al., 2022; Maran & Begotti, 2022).

Giving passwords to untrusted systems is proof of students' carelessness in dealing with digital cyber-attacks in the current 4.0 era. Notably, 80% of students admit to giving passwords without knowing the risks that will occur later. The midwifery student group has the highest average rate of 84.1% due to their low ability in digital literacy so that student activities to realize that there are threats in the form of phishing, malware, or various fake platforms that are easily accessible have the purpose of stealing data and utilizing incoming information, activities faced by students are still neglected. In contrast, nursing and nutrition students are more likely to be interested in platforms that offer discounts, gifts, or free services by registering with their personal data details, of the three groups, which is still very low related to checking whether the registered platform is legal or safe. Tracking systems are online crimes that are difficult to detect. Most students believe online crimes are difficult to overcome due to limited resources and the lack of sophisticated technology to track online crimes effectively. While online crime can be hacked in seconds, tracking takes a long time. The midwifery student group has an average percentage of 80.1%, which shows that it is difficult for students to track online crimes because hackers hide their location and identity. Previous research has shown that there are a lot of high-risk vulnerabilities and warnings based on tools (*vulnerability assessment tools*) on the university web application (Jarupunphol et al., 2023). Student independence cannot directly predict aspects of vulnerability to password theft attacks and personal data information (Waqas et al., 2023). Vulnerability to such theft explores intimate partner cyberstalking (IPCS), so that it can identify gender, age, sexting, pornography consumption, and ambivalent sexism, as well as the target of the crime is women (Ejaz et al., 2023). Cybersecurity awareness is measured through cybersecurity and password security (Ahamed et al., 2024). Password can be protected by using Random Forest (RF), Decision Tree (DT), Stochastic Gradient Descent (SGD), dan Logistic Regression (LR), Integrated with stacking and bagging techniques (Aziz & Baker, 2024). In addition, Cyber Threat Intelligence (CTI) aims to identify new forms of threats and improve cyber security (Eltayeb, 2024a).

Student activities to have digital security awareness are still low, based on the results of the recapitulation show that the nutrition student group is at an average of 48.2%, but for the midwifery student group, it reaches 46.5% and nursing reaches 45.1%. All student groups tend to focus more on academic and practical activities, so they pay less attention to the security aspects of their devices and lack knowledge about the various digital threats they face, such as accessing the internet through risky public wi-fi without securing their devices. Previous research shows that universities must prioritize technological aspects in building cybersecurity awareness and aligning learning curricula relevant to technological advances in the industry 4.0 era (Gonzales et al., 2022). The importance of cyber management for teenagers, thus increasing their awareness of cybersecurity (Alsobeh et al., 2023). In line with this study, teachers are the first mediators in schools who can support students' knowledge in cyber learning plans, and they participate in training to strengthen the cybersecurity education system at the school level (Childers et al., 2023). In developed countries, cybersecurity is the main focus in improving cybersecurity among students to be able to manage email and passwords correctly, so that educational institutions, parents, and students are ready to adopt security practices in using the internet in their daily activities (W. C. H. Hong et al., 2023; Saeed, 2023).

The implementation strategy of security and privacy awareness against digital attacks on health students has priorities based on SOAR analysis, as follows:

Figure 1. Summary SOAR analysis of strategy security and privacy awareness

SOAR analysis is one of the tools to focus on strengths and opportunities in strategic and dynamic planning in the era of Industry 4.0, the characteristics of SOAR analysis refer to the identification of positive aspects that are studied in designing innovative strategies to increase security awareness and privacy in today's digital world so that it can maximize the potential to be oriented to the future by considering the expected end results from the institution education in particular (Stavros et al., 2003). Previous research stated that SOAR analysis can explore resources and evaluate a program's design, function and purpose (C. Y. Hong et al., 2020; Jacobs et al., 2020). In line with the above research, SOAR Analysis is practical as a guide to making organizational changes quickly and followed by a continuous improvement process (Harding et al., 2022). The SOAR analysis process can also overcome obstacles to improve the implementation process in a program (Kumar et al., 2023; Vardopoulos et al., 2023).

Conclusion

This research has succeeded in implementing the mapping of student security and privacy strategies in the face of digital attacks in the industry 4.0 era, it finds data mapping to track the impact of threats in the form of low digital literacy students' abilities, such as; the use of passwords on systems that they do not know the validity of, low knowledge about the use of software as a two-step security device and passive behavior of students when they become victims of digital crime. This research advocates for evidence of preventing digital threats experienced by health students by taking a practical digital literacy approach in finding, evaluating, utilizing, sharing, and creating digital technology-based content with high security and privacy to prevent digital cyber-attacks in the current era. The limitations of this study are that it only includes health study programs in one city in Indonesia, so the results of the data recapitulation displayed cannot be applied in general. This research has not focused on the role of institutions and lecturers in overcoming the threat of digital attacks faced by health vocational

students.

Funding Statement

Funding is Supprot by Lembaga Pengelola Dana Pendidikan (LPDP) / Beasiswa Pendidikan Indonesia (BPI) / Pusat Pelayanan Pembiayaan dan Asesmen Pendidikan Tinggi (PPAPT) Ministry of Higher Education, Science, and Technology of Republic Indonesia.

Author Contribution

Imma Rachayu contributed to the conception, writing and review, Yatim Riyanto and Utari Dewi contributed to the conception and review. Fitri Maiziani and Ramazan contributed to data collections, Suci Perwitasari and Ratih Wulandari contributed to data processing.

Conflict of Interest

There is no conflict of interest in the article. All author responsible for the content of the article.

Acknowledgements

We want to thank our supervisors, Lembaga Pengelola Dana Pendidikan (LPDP) / Beasiswa Pendidikan Indonesia (BPI) / Pusat Pelayanan Pembiayaan dan Asesmen Pendidikan Tinggi (PPAPT) Ministry of Higher Education, Science, and Technology of Republic Indonesia, for their assistance in ensuring the proper completion of this paper and to Universitas Negeri Surabaya, especially the Educational Technology Study Program at the Faculty of Education.

References

Aguilera, A. (2015). Digital Technology and Mental Health Interventions: Opportunities and Challenges. *Arbor*, *191*(771), a210. https://doi.org/10.3989/arbor.2015.771n1012

Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Fahad, A. Al, Chowdhury, S., & Rani Dey, M. (2024). Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era: The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era. *SAGE Open*, *14*(1), 1–14. https://doi.org/10.1177/21582440241228920

Ahmad, S. U., Kashyap, S., Shetty, S. D., & Sood, N. (2022). Cybersecurity During COVID-19. In *Lecture Notes in Networks and Systems* (Vol. 191, pp. 1045–1056). https://doi.org/10.1007/978-981-16-0739-4_96

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, *8*, 137293–137311. https://doi.org/10.1109/ACCESS.2020.3011259

Albarrak, A. M. (2024). Integration of Cybersecurity, Usability, and Human-Computer Interaction for Securing Energy Management Systems. *Sustainability (Switzerland)*, *16*(18). https://doi.org/10.3390/su16188144

Alsobeh, A. M. R., Alazzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technologies*, *13*(2). https://doi.org/10.30935/ojcmt/12942

Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime. *Sustainability (Switzerland)*, *15*(15). https://doi.org/10.3390/su151511512

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

Amaral, I., Basílio-Simões, R., & Poleac, G. (2022). Technology gap and other tensions in social support and legal procedures: stakeholders' perceptions of online violence against women during the Covid-19 pandemic. *Profesional de La Informacion*, *31*(4), 1–12. https://doi.org/10.3145/epi.2022.jul.13

Aziz, E. F., & Baker, M. R. (2024). Enhancing Multi-Class Password Strength Prediction Through Machine Learning and Ensemble Techniques. *International Journal of Safety and Security Engineering*, *14*(5), 1635–1645. https://doi.org/10.18280/ijsse.140530

Bednar, P. M., & Welch, C. (2020). Socio-Technical Perspectives on Smart Working: Creating Meaningful and Sustainable Systems. *Information Systems Frontiers*, *22*(2), 281–298. https://doi.org/10.1007/s10796-019-09921-1

Begotti, T., Ghigo, M. A., & Maran, D. A. (2022). Victims of Known and Unknown Cyberstalkers: A Questionnaire Survey in an Italian Sample. *International Journal of Environmental Research and Public Health*, *19*(8). https://doi.org/10.3390/ijerph19084883

Bilić, P., & Žitko, M. (2024). Personal data as pseudo-property: Between commodification and assetisation. *European Journal of Communication*, *39*(5), 426–437. https://doi.org/10.1177/02673231241267128

Boethius, S., Åkerström, M., & Hydén, M. (2023). The double-edged sword–abused women's experiences of digital technology. *European Journal of Social Work*, *26*(3), 506–518. https://doi.org/10.1080/13691457.2022.2040437

Bozzi, A. (2024). Digital nomadism from the perspective of places and mobilities: a literature review. *European Transport Research Review*, *16*(1). https://doi.org/10.1186/s12544-024-00663-z

Bucci, S., Schwannauer, M., & Berry, N. (2019). The digital revolution and its impact on mental health care. *Psychology and Psychotherapy: Theory, Research and Practice*, *92*(2), 277–297. https://doi.org/10.1111/papt.12222

Burns, K., Halvey, O., Ó Súilleabháin, F., O'Callaghan, E., & Coelho, G. (2024). The Social Media, Online and Digital Abuse and Harassment of Social Workers, Probation Officers and Social Work Students in Ireland: A National Survey. *The British Journal of Social Work*, 3274–3294. https://doi.org/10.1093/bjsw/bcae091

Chen, Y., Li, R., & Liu, X. (2021). The relationships among relatedness frustration, affiliation motivation, and WeChat engagement, moderated by relatedness satisfaction. *Cyberpsychology*, *15*(4). https://doi.org/10.5817/CP2021-4-7

Childers, G., Linsky, C. L., Payne, B., Byers, J., & Baker, D. (2023). K-12 educators' self-confidence in designing and implementing cybersecurity lessons. *Computers and Education Open*, *4*(October 2022), 100119. https://doi.org/10.1016/j.caeo.2022.100119

Coyac-Torres, J. E., Sidorov, G., Aguirre-Anaya, E., & Hernández-Oregón, G. (2023). Cyberattack Detection in Social Network Messages Based on Convolutional Neural Networks and NLP Techniques. *Machine Learning and Knowledge Extraction*, *5*(3), 1132–1148. https://doi.org/10.3390/make5030058

DeKeseredy, W. S., Schwartz, M. D., Harris, B., Woodlock, D., Nolan, J., & Hall-Sanchez, A. (2019). Technology-Facilitated Stalking and Unwanted Sexual Messages/Images in a College Campus Community: The Role of Negative Peer Support. *SAGE Open*, *9*(1). https://doi.org/10.1177/2158244019828231

Dutta, A. K. (2021). Detecting phishing websites using machine learning technique. *PLoS ONE*, *16*(10 October), 1–17. https://doi.org/10.1371/journal.pone.0258361

Echevarría, A., Morales, D., & González, L. (2015). Monitoring and enforcing data protection

laws within an e-government interoperability platform. *Proceedings - 2015 41st Latin American Computing Conference, CLEI 2015*. https://doi.org/10.1109/CLEI.2015.7360028

Ejaz, A., Mian, A. N., & Manzoor, S. (2023). Life-long phishing attack detection using continual learning. *Scientific Reports*, *13*(1), 1–14. https://doi.org/10.1038/s41598-023-37552-9

Eltayeb, O. E. O. (2024a). Cyber Defense Using Cyber Threat Intelligence to Anticipate and Avoid Future Cyber Attacks. *Pakistan Journal of Life and Social Sciences*, *22*(2), 1883–1904. https://doi.org/10.57239/PJLSS-2024-22.2.00132

Eltayeb, O. E. O. (2024b). The Crucial Significance of Cyber Threat Intelligence in Mitigating Cyber Attacks. *Pakistan Journal of Life and Social Sciences*, *22*(2), 1760–1772. https://doi.org/10.57239/PJLSS-2024-22.2.00123

Falowo, O. I., & Abdo, J. B. (2024). 2019-2023 in Review: Projecting DDoS Threats With ARIMA and ETS Forecasting Techniques. *IEEE Access*, *12*, 26759–26772. https://doi.org/10.1109/ACCESS.2024.3367240

Figueroa, C. A., & Aguilera, A. (2020). The Need for a Mental Health Technology Revolution in the COVID-19 Pandemic. *Frontiers in Psychiatry*, *11*(June), 1–5. https://doi.org/10.3389/fpsyt.2020.00523

Firat, M. (2023). What ChatGPT means for universities: Perceptions of scholars and students. *Journal of Applied Learning and Teaching*, *6*(1), 57–63. https://doi.org/10.37074/jalt.2023.6.1.22

Gan, C. L., Lee, Y. Y., & Liew, T. W. (2024). Fishing for phishy messages: predicting phishing susceptibility through the lens of cyber-routine activities theory and heuristic-systematic model. *Humanities and Social Sciences Communications*, *11*(1). https://doi.org/10.1057/s41599-024-04083-1

Gómez-Barroso, J.-L. (2018). Use and value of personal information: An evolving scenario. *Profesional de La Informacion*, *27*(1), 5–18. https://doi.org/10.3145/epi.2018.ene.01

Gonzales, R., Almacen, R. M., Gonzales, G., Costan, F., Suladay, D., Enriquez, L., Costan, E., Atibing, N. M., Aro, J. L., Evangelista, S. S., Maturan, F., Selerio, E., & Ocampo, L. (2022). Priority Roles of Stakeholders for Overcoming the Barriers to Implementing Education 4.0: An Integrated Fermatean Fuzzy Entropy-Based CRITIC-CODAS-SORT Approach. *Complexity*, *2022*. https://doi.org/10.1155/2022/7436256

Harding, S. L., Eyllon, M., Twigden, A., Hogan, A., Barry, D., Mirsky, J. E., Barnes, B., & Nordberg, S. (2022). Power on: The rapid transition of a large interdisciplinary behavioral health department to telemental health during the COVID-19 pandemic. *Journal of Interprofessional Education and Practice*, *27*(December 2021), 100506. https://doi.org/10.1016/j.xjep.2022.100506

Homaei, M., Mogollón-Gutiérrez, Ó., Sancho, J. C., Ávila, M., & Caro, A. (2024). A review of digital twins and their application in cybersecurity based on artificial intelligence. In *Artificial Intelligence Review* (Vol. 57, Issue 8). https://doi.org/10.1007/s10462-024-10805-3

Hong, C. Y., Yoon, R., Hwang, J. D., & Jwa, M. S. (2020). Exploring community symbiotic tourism programs for the utilization and conservation of ecology in lava stony forest (Gotjawal) of Jeju Island, Korea. *Sustainability (Switzerland)*, *12*(20), 1–18. https://doi.org/10.3390/su12208371

Hong, W. C. H., Chi, C. Y., Liu, J., Zhang, Y. F., Lei, V. N. L., & Xu, X. S. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. In *Education and Information Technologies* (Vol.

28, Issue 1). Springer US. https://doi.org/10.1007/s10639-022-11121-5

Huijts, N. M. A., Haans, A., Budimir, S., Fontaine, J. R. J., Loukas, G., Bezemskij, A., Oostveen, A., Filippoupolitis, A., Ras, I., IJsselsteijn, W. A., & Roesch, E. B. (2023). User experiences with simulated cyber-physical attacks on smart home IoT. *Personal and Ubiquitous Computing*, *27*(6), 2243–2266. https://doi.org/10.1007/s00779-023-01774-5

Jacobs, L., Du Preez, E. A., & Fairer-Wessels, F. (2020). To wish upon a star: Exploring Astro Tourism as vehicle for sustainable rural development. *Development Southern Africa*, *37*(1), 87–104. https://doi.org/10.1080/0376835X.2019.1609908

Jarupunphol, P., Seatun, S., & Buathong, W. (2023). Measuring Vulnerability Assessment Tools' Performance on the University Web Application. *Pertanika Journal of Science and Technology*, *31*(6), 2973–2993. https://doi.org/10.47836/pjst.31.6.19

Jia, X., Hu, N., Su, S., Yin, S., Zhao, Y., Cheng, X., & Zhang, C. (2020). *IRBA : An Identity-Based Cross-Domain*.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2023). Cyber-security and risky behaviors in a developing country context: a Pakistani perspective. In *Security Journal* (Vol. 36, Issue 2). Palgrave Macmillan UK. https://doi.org/10.1057/s41284-022-00343-4

Kumar, A. P., Omprakash, A., Mani, P. K. C., Kuppusamy, M., Wael, D., Sathiyasekaran, B. W. C., Vijayaraghavan, P. V., & Ramasamy, P. (2023). E-learning and E-modules in medical education—A SOAR analysis using perception of undergraduate students. *PLoS ONE*, *18*(5 May), 1–14. https://doi.org/10.1371/journal.pone.0284882

Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin, J. C. W. (2022). Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. *Sensors*, *22*(6), 1–36. https://doi.org/10.3390/s22062087

Maran, D. A., & Begotti, T. (2019). Prevalence of cyberstalking and previous offline victimization in a sample of Italian university students. *Social Sciences*, *8*(1). https://doi.org/10.3390/socsci8010030

Maran, D. A., & Begotti, T. (2022). Cyberstalking and Previous Offline Victimization in Italian Young Adults: The Role of Coping Strategies. *Social Sciences*, *11*(12). https://doi.org/10.3390/socsci11120549

Marko, S., Tsaruk, Y., Skhidnytska, H., Kryshtanovych, M., & Nikonenko, U. (2024). Ensuring Cybersecurity in the Modern World: Challenges from Artificial Intelligence-Based Fraud Posing a Threat to the Environment. *Journal of Ecohumanism*, *3*(4), 1436–1442. https://doi.org/10.62754/joe.v3i4.3673

Martins Van Jaarsveld, G. (2020). The Effects of COVID-19 Among the Elderly Population: A Case for Closing the Digital Divide. *Frontiers in Psychiatry*, *11*(November), 1–7. https://doi.org/10.3389/fpsyt.2020.577427

Mishra, S. (2023). Blockchain and Machine Learning-Based Hybrid IDS to Protect Smart Networks and Preserve Privacy. *Electronics (Switzerland)*, *12*(16). https://doi.org/10.3390/electronics12163524

Nakamura, Y., Zhang, Y., Sasabe, M., & Kasahara, S. (2020). Exploiting smart contracts for capability-based access control in the internet of things. *Sensors (Switzerland)*, *20*(6). https://doi.org/10.3390/s20061793

Oliveira, M., & Dias, G. P. (2023). The role of the data protection officer in local governments: an exploratory study. *Iberian Conference on Information Systems and Technologies, CISTI*, *2023-June*. https://doi.org/10.23919/CISTI58278.2023.10211727

Pangrazio, L., & Selwyn, N. (2019). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media and Society*, *21*(2), 419–437. https://doi.org/10.1177/1461444818799523

Polyzoidou, V. (2024). Digital Violence Against Women: Is There a Real Need for Special Criminalization? *International Journal for the Semiotics of Law*, *37*(6), 1777–1797. https://doi.org/10.1007/s11196-024-10179-3

Rafiq, F., Awan, M. J., Yasin, A., Nobanee, H., Zain, A. M., & Bahaj, S. A. (2022). Privacy Prevention of Big Data Applications: A Systematic Literature Review. *SAGE Open*, *12*(2). https://doi.org/10.1177/21582440221096445

Rahim, R., Murugan, S., Mostafa, R. R., Dubey, A. K., Regin, R., Kulkarni, V., & Dhanalakshmi, K. S. (2020). Detecting the Phishing Attack Using Collaborative Approach and Secure Login through Dynamic Virtual Passwords. *Webology*, *17*(2), 524–535. https://doi.org/10.14704/WEB/V17I2/WEB17049

Rao, G. R. K., Battu, V. V, Anupama, V., Allada, A., Krishna, S. V. R., & Hema, C. (2023). Modern Progressive Pitfalls of Cyber Attacks on the Digital World. *Proceedings of the 2nd International Conference on Edge Computing and Applications, ICECAA 2023*, 244–248. https://doi.org/10.1109/ICECAA58104.2023.10212303

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V, & Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors*, *23*(8). https://doi.org/10.3390/s23084060

RISET, K., & TINGGI, T. (2020). Panduan Penyusunan Kurikulum Pendidikan Vokasi. *Academia.Edu*. http://www.academia.edu/download/61283233/Panduan-Penyusunan-Kurikulum-Pendidikan-Vokasi-201620191120-43633-12k5uv5.pdf

Saeed, S. (2023). Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia. *Sustainability (Switzerland)*, *15*(12). https://doi.org/10.3390/su15129426

Singamaneni, K. K., Dhiman, G., Juneja, S., Muhammad, G., Alqahtani, S. A., & Zaki, J. (2022). *Computational Knacks*.

Stavros, J., Cooperrider, D., & Kelley, D. L. (2003). Strategic Inquiry - Appreciative Intent: Inspiration to SOAR. *AI Practitioner*, *November*(November 2014), 1–21. https://design.umn.edu/about/intranet/documents/Strategic_Inquiry_Appreciative_Intent.pdf

Sturman, D., Auton, J. C., & Morrison, B. W. (2025). Security awareness, decision style, knowledge, and phishing email detection: Moderated mediation analyses. *Computers and Security*, *148*(September 2024), 104129. https://doi.org/10.1016/j.cose.2024.104129

van der Sanden, R., Wilkins, C., & Rychert, M. (2024). "I straight up criminalized myself on messenger": law enforcement risk management among people who buy and sell drugs on social media. *Drugs: Education, Prevention and Policy*, *31*(3), 378–390. https://doi.org/10.1080/09687637.2023.2224497

Vardopoulos, I., Giannopoulos, K., Papaefthymiou, E., Temponera, E., Chatzithanasis, G., Goussia-Rizou, M., Karymbalis, E., Michalakelis, C., Tsartas, P., & Sdrali, D. (2023). Urban buildings sustainable adaptive reuse into tourism accommodation establishments: a SOAR analysis. *Discover Sustainability*, *4*(1). https://doi.org/10.1007/s43621-023-00166-2

Wang, S., Tuor, T., Salonidis, T., Leung, K. K., Makaya, C., He, T., & Chan, K. (2019). Adaptive Federated Learning in Resource Constrained Edge Computing Systems. *IEEE Journal on Selected Areas in Communications*, *37*(6), 1205–1221. https://doi.org/10.1109/JSAC.2019.2904348

Waqas, M., Hania, A., Yahya, F., & Malik, I. (2023). Enhancing Cybersecurity: The Crucial Role of Self-Regulation, Information Processing, and Financial Knowledge in Combating Phishing Attacks. *SAGE Open*, *13*(4), 1–14. https://doi.org/10.1177/21582440231217720

You, Z., & Feng, L. (2020). Integration of Industry 4.0 Related Technologies in Construction Industry: A Framework of Cyber-Physical System. *IEEE Access*, *8*, 122908–122922. https://doi.org/10.1109/ACCESS.2020.3007206