JSI : Jurnal Sistem Informasi *(E-Journal), Vol.15, No.1, 2023*
ISSN Print : 2085-1588 / ISSN Online :2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsifasilkom@unsri.ac.id

Enhancing Cybersecurity Awareness among University Students: A Study on the Relationship between Knowledge, Attitude, Behavior, and Training

Anwar Fattah[1*], Wagimin[2], Nurlia[3]
[1]Electical Engineering, Balikpapan University, Indonesia

[2]Industrial Engineering, Balikpapan University, Indonesia

[3]Management, Balikpapan University, Balikpapan

*Corresponding Author**

Email: anwar.fattah@uniba-bpn.ac.id[1*], wagimin66.leo@gmail.com[2], nurlia@uniba-bpn.ac.id[3].

Abstract

The purpose of this research is to explore and measure the level of cybersecurity awareness among university students. Specifically, we aim to examine the relationships between knowledge, attitude, behavior, and training in shaping cybersecurity awareness. By understanding these factors and their interplay, we can identify potential areas of improvement and develop targeted interventions to enhance cybersecurity awareness among university students. The quantitative data analyzed by the smallest partial quadratic structural equation method (PLS-SEM) using Smart PLS 3.0 with 64 respondents from students' univeristy. The results obtained from this dataset show a positive significant relationship between knowledge; attitude, behavior, and training all have a positive impact on cybersecurity awareness among university students.

Keywords: Cybersecurity awareness; University students; Cybersecurity education; Cyber threats; Information security.

1. INTRODUCTION

In today's digital age, cybersecurity has become a critical concern for people, businesses, and society as a whole [1]. We have become subject to a range of cybersecurity risks and vulnerabilities as our reliance on digital technologies has grown and the online world has become more linked. Cyberattacks, ranging from data breaches to identity theft and ransomware attacks, pose significant risks to human privacy, financial security, and the integrity of information systems [2].

The effort to protect computer systems, networks, and data from attacks or illegal access referred to as cybersecurity. Malware, DDoS (Distributed Denial of Service), phishing attacks, and data theft are all examples of cyber security attacks. These fraudulent criminals might steal sensitive information, harm digital infrastructure, or disrupt the operations of businesses or individuals.

Cybersecurity is becoming an increasingly critical issue for young people [3]. Students are an extremely active demographic when it comes to using technology like computers, laptops, smartphones, and social media. They frequently participate in online activities such as research, information sharing, communication, and purchasing. However, student cybersecurity knowledge and understanding tends to be low.

Among the various demographic groups, university students represent a particularly important population to focus on when it comes to cybersecurity awareness [4]. Students are avid users of digital technologies, relying on the Internet for academic research, communication, and social interactions. However, studies have shown that many students lack the necessary knowledge, attitudes, and behaviors to protect themselves and their digital assets effectively.

One of the reasons for low cybersecurity awareness among students is the lack of adequate education and training [4]. Formal education curricula rarely cover aspects of cybersecurity, and students often do not have sufficient knowledge about how to protect themselves online. In addition, attitudes and behaviors that are less concerned about cybersecurity can also be contributing factors in this low awareness. Students may not be aware of the risks associated with unsafe online practices or may not respond appropriately to protect themselves.

In the context of globalization and digitalization, it is important for students to have a high awareness of cybersecurity. They are future holders who will be involved in a variety of sectors, including information and communication technologies. Students who have adequate knowledge and skills in cybersecurity will be able to protect themselves and contribute to preventing cyber security threats more broadly[5].

In addition, high cybersecurity awareness among students also has important implications for educational institutions. Many educational institutions rely on technology in the learning process, administration, and storage of student data. The risk of cybersecurity attacks can result in financial losses, loss of important data, or damaged reputation for the institution. Therefore, it is important for educational institutions to ensure that students have the knowledge, attitudes, and behaviors appropriate to face cybersecurity threat [6].

To raise cybersecurity awareness among students, education and training integrated with the educational curriculum is essential [7]. Students should be equipped with basic knowledge of cybersecurity threats, best practices to protect themselves, and measures to deal with possible attacks. In addition, they also need to have a proactive attitude towards cybersecurity, such as taking the security of personal information seriously, avoiding risky actions, and contributing to building a security culture in the digital environment.

Through this research, data on the level of cybersecurity awareness among students expected to be collected. The data can provide valuable insights into the current state of cybersecurity awareness, to what extent students' knowledge, attitudes, and behaviors related to cyberspace, and to what degree cyber security training has an impact on their consciousness. The research results can be used as a basis for designing more effective educational and training programs in raising cybersecurity awareness among students.

1.1 Literature Review

A. Cybersecurity awareness

Cybersecurity awareness refers to an individual's understanding and recognition of security threats and risks associated with the use of digital technologies. This involves an understanding of good security practices, knowledge of types of cyber attacks, and a willingness to take appropriate action in protecting yourself from such threats [8].

Cybersecurity awareness is vital in an increasingly connected and vulnerable digital world to security attacks. In an environment filled with malware, phishing, identity theft, and other cyber attacks, individuals should be able to recognize and address those threats to protect themselves, their personal data, and their interests [9].

B. The Importance of Cybersecurity Awareness in Students

Cybersecurity awareness among students has several important implications [10].

Students often become active technology users, access the internet and use a variety of digital platforms for academic and personal purposes. They often interact with sensitive information, including personal data and online accounts. Therefore, cybersecurity awareness among students is essential to protect themselves from fraud, cyber attacks, and identity theft.

Students are also an important part of the broader digital ecosystem. With high levels of reliance on technology, high cybersecurity awareness among students can help prevent the spread of cyber attacks to the wider community. Cyber-conscious students can act as cybersecurity ambassadors, sharing good security practices with friends, family, and colleagues.High cybersecurity awareness among students can help them in preparing for their careers. In an increasingly digitally connected world of work, expertise and understanding of cybersecurity is becoming crucial. Students who have a good cybersecurity awareness will become prospective workforce who are better prepared to face cyber security challenges and can contribute to protecting enterprise data and systems [11].

C. Study on Cybersecurity Awareness in Students

Several previous studies have been conducted to investigate the level of cybersecurity awareness among students. The study focuses on students' understanding of cybersecurity risks, knowledge of good security practices, as well as attitudes and behaviors related to cyber security.

Several previous studies have shown some relevant findings about cybersecurity awareness among students. One study conducted by [12] investigated the level of university students' awareness towards cyber security is at moderate leve. Many proactive steps need to be implement by the stakeholders so that issues that are relevant to cybercrime can be reduce. Some factors that contribute to the low cybersecurity awareness among students include a lack of formal education on cyber security, excessive confidence in technology, and a shortage of consciousness about the serious implications of cyber attacks.

Another study conducted by [13] examined student attitudes and behaviors related to cybersecurity in the university environment. Based on the research conducted that knowledge of password security, browser security, and social media activities significantly influences cybersecurity awareness in students. Overall, students have realized the importance of cybersecurity awareness. A lack of understanding of the serious consequences of cybersecurity attacks and a lack of awareness of the importance of self-protection online are some of the factors causing such attitudes and behaviors.

In addition, another study conducted by [14] identified factors that affect cybersecurity awareness among students. The results of the research show that the level of knowledge and education about cybersecurity has a significant impact on cyber security awareness. Students with a higher level of knowledge about cybersecurity threats tend to have a higher awareness of good security practices. Furthermore, factors such as personal experiences with cybersecurity attacks, media concerns about cyber security issues, and compliance with security policies also contribute to higher cyber-security awareness.

Although some studies show a low level of cybersecurity awareness among students, there are also several initiatives and programs that have been undertaken to raise cyber-security Awareness in colleges [15]. Several colleges have provided compulsory cybersecurity training programmes for new students and provided easily accessible cyber security resources and guidelines [16]. In addition, cybersecurity awareness campaigns carried out to increase students' understanding and consciousness of security threats. Accourding to [17] These studies show that although students have extensive access to technology and the internet, their level of cybersecurity awareness is not significantly low, but there are some knowledge gaps with new threats.

1.2 Conteptual Framework

A. Variable research

- Training

Training variables reflect whether students have received, formal training or education related to cybersecurity [18]. This training can include lectures, seminars, workshops, or other training programs aimed at enhancing students' cybersecurity knowledge, attitudes, and behavior. Training variables can be measure by gathering information about the type of training students have undergone and to what extent the training has affected their knowledge, attitudes, and behaviors related to cybersecurity.

H1-H2-H3 Relationship between training and other research variables: Cybersecurity training can have a significant impact on other study variables, namely knowledge, attitudes, and behavior. Through effective training, students can enhance their knowledge of cybersecurity, change their attitude towards security practices, and encourage better security behavior.

- Knowledge

Knowledge variables refer to the level of students' understanding and knowledge of cybersecurity[19]. This includes an understanding of cybersecurity threats, the types of attacks that may occur, good security practices, and measures to protect yourself from such attacks. These knowledge variables measured through tests or questionnaires to evaluate students' understanding of cybersecurity.

H4. The relationship between knowledge and attitude: Adequate knowledge of cybersecurity can form a positive attitude towards security practices. Students who have good knowledge of security threats and risks tend to have a more proactive attitude in protecting themselves and adopting necessary security measures.

- Behavior

Behavioral variables refer to real actions and security practices carried out by students in the use of digital technologies [20][21]. This involves implementing good security practices, such as using strong passwords, updating software regularly, limiting access to personal information, and avoiding actions that could invite security risks. These behavioral variables can be measured through direct observations, self-reports, or questionnaires to evaluate student cybersecurity behavior.

H5.The relationship between knowledge and behavior: A good knowledge of cybersecurity can affect student behaviour in terms of implementing correct security practices. Students who have adequate knowledge of security threats are more likely to take necessary protective measures, such as installing security software, performing regular data backups, or using secure networks.

- Attitude

The attitude variables reflect the attitude and perception of students towards cybersecurity [22]. It involves a positive or negative assessment of security practices, perceptions of the importance and relevance of cybersecurity, as well as the level of motivation and readiness to adopt good security practice. These attitude variables can be measured through attitude scales or questionnaires designed to evaluate student attitudes to cybersecurity [23].

H6. The relationship between attitudes and behaviors: Attitudes towards cybersecurity can affect student behavior in their digital lives. Students with a positive attitude toward security practices tend to be more careful and careful in protecting personal information, using strong passwords, and avoiding risky behavior.

B. The relationship between research variables

In this conceptual framework, there is a relationship between the research variables that should be described in the research. This relationship can be describe figure 1 Proposed Model & Hypotheses.

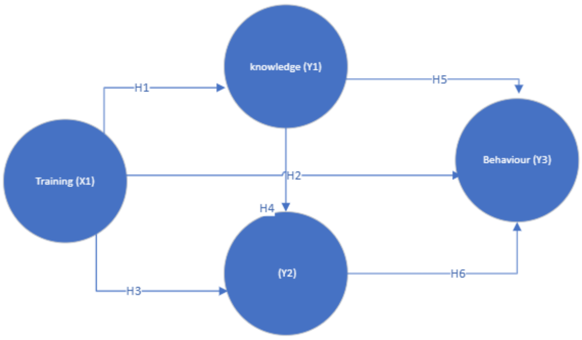

Figure 1. Proposed Model & Hypotheses

2. RESEARCH METHOD

The research will adopt a quantitative approach, employing a cross-sectional survey design. This design allows for the collection of data at a specific point in time, providing a snapshot of cybersecurity awareness among university students. The survey questionnaire will be used to gather information on students' knowledge, attitudes, and behaviors related to cybersecurity.

The target population for this study will be university students from various academic disciplines. The sample will be drawn from student Balikpapan university, with 64 Student already participate in this survey. A self-administered survey questionnaire developed to collect data on students' cybersecurity awareness. The questionnaire will include items related to their knowledge of cybersecurity concepts, attitudes towards cybersecurity practices, and behaviors exhibited in relation to online security. Analyze the data using the Chi-Square test with a confidence level of (a = 0.05). The hypothesis is that if p 0.05 or T-statistics (1, 96), then the variable is deemed significantly connected, and if p>0.05, then the variable is declared unrelated. Evaluate and validate this model used the Structural Equatiion Modeling (SEM). For further testing of research hypothesis used by SMART PLS 3.3.9.

3. RESULTS AND DISCUSSIONS

A. Measurement Model Validation

The Reliability and validity of each construct are measured in the measurement model assessment.With the exception K3, all indicators had factor loadings (table x) that are more that the threashold limit of 0.7 [24] ranging 0,952 to 0.763. These indicarors were thus eliminated.

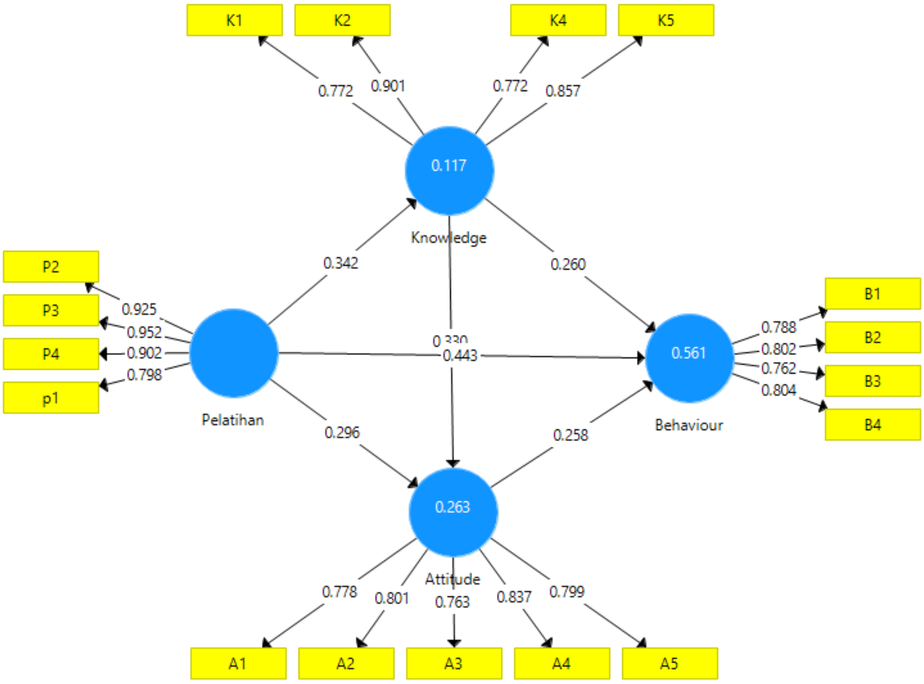

Figure 1: Structural model and path coefficient

Further, Cronbach's alpha and composite reliability (CR) are more than threshold [25]. Avarage variance extracted (AVE) (Table 1) is calculated to assess the convergent validity and is found to be between 0.623 and 0.803, above the threashold of more than 0.05 [26]. In case of disctiminant valididiy, we used the Fornell-Larcker criterion are supported by Table 2 finding that the square toots examined for the AVE values are higher than the correlations between the variables and results show the HTMT value (inbrackets)[27] and are less than 0.742, thus these outpus indicate the validation of measurement model.

TABLE 1. RESULT CONSTRUCTS RELIABILITY AND CONVERGENT VALIDTY

Construct	Indicators	Outer Loading	Composite reliability	Cronbach's Alpha	Average of Variance	VIF
Attitude	A1	**0.778**	**0.896**	**0.856**	**0.633**	**1.781**
	A2	**0.801**				**1.868**
	A3	**0.763**				**2.043**
	A4	**0.837**				**2.075**
	A5	**0.799**				**2.227**
Behaviour	B1	**0.788**	**0.868**	**0.799**	**0.623**	**1.551**
	B2	**0.802**				**1.916**
	B3	**0.762**				**1.421**
	B4	**0.804**				**1.914**
Knowledge	K1	**0.772**	0.896	**0.848**	**0.685**	**1.793**

Construct	Indicators	Outer Loading	Composite reliability	Cronbach's Alpha	Average of Variance	VIF
	K2	**0.901**				**2.576**
	K3	**0.772**				**1.782**
	K4	**0.857**				**2.343**
Training	P1	**0.772**	**0.942**	**0.917**	**0.803**	**1.972**
	P2	**0.901**				4.221
	P3	**0.772**				**6.834**
	P4	**0.857**				4.111

TABLE 2. DISCRIMINANT VALIDITY: FORNELL-LACKER CRITERIA AND HTMT RATIO

	Attitude	Behaviour	Knowledge	Training
Attitude	0.796			
Behaviour	0.552 (0.656)	0.789		
Knowledge	0.431 (0.489)	0.523(0.607)	0.828	
Training	0.409(0.499)	0.638(0.742)	0.342 (0.368)	0.896

B. Structural Model validation

Smart PLS Bootstrapping function was used to examine the model fit trus view the significant of relationships between the various variables. Latent collinearity was firt addressed. The variance inflation factor was conducted to identify (VIF) [24]. Values of VIF should be more than 0.2 and less than 5.0. Table 1 demostrates thath the independent variable's inner VIF value are ranging 0.2 and below 5.0 ow indicates correlation of that predictor with other predictors. . Except P3 6.834 indicates a moderate correlation. Table 3 and figure 1 show that the R2 values for Ranging 0.102-0.539 mean that these variables have low to moderate predictive potential. Futhermore, the R2 Value of actual usage is shown to explain 23.9%, indicating that this construct have low predictive power. A measure of predictive power expected to employ PLS for prediction. For fetermining predictive relevance, the blind folding method has been suggested. Tabel 3 shows that the Q2 value for all latent constructs is greater than 0.053. In this case, the model was low predictive. Structure model validation is model fit index. For the approximate fit indices such as SRMR and NFI, the criteria values for 0.1 > SRMR ≥ 0.08 and NFI > 0.90 [28]. This model has SRMR less than 0.1 but greater than 0.08 and for NFI index less than 0.90. Therefore, if we use SRMR for model fit, this model is good enough.

TABLE 3. Q2 AND R2 FOR PREDICTIVE RELEVANCE

	R Square	R Square Adjusted	Results	Q2 =(1-SSE/SSO)
Attitude	0.263	0.239	Low	0.121
Behaviour	0.561	0.539	Moderate	0.313

Knowledge	0.117	0.102	Low	0.053

TABLE 4. MODEL FIT VALUES

Model Fit measures	**Value**
SRMR	0.089
d_ULS	1.208
d_G	0.507
Chi-Square	182.860
NFI	0.752

C. *Test of Hypothesis-Path Coefficients*

[29] evaluated the direct effects among construct with Bootstrapping techniques with 5000 re-sampling methods. The result of structural model hypotheses are show in Table 5. In case of Knowledge, Training (β= 0.342), T Statistics = 2.175, p<0.05) positively affects Knowledge, so H1 is supported. In the term of Behaviour, Training (β= 0.638), T Statistics = 6.245, p<0.05) positively affects Behaviour [30]. So study accepted for H1, H2, H3, H4, H5 and H6.

TABLE 5. HYPOTHESIS TESTING RESULTS

Hypothesis	**β**	**Sample Mean (M)**	**Standard Deviation (STDEV)**	**T Statistics (|O/STDEV|)**	**P Values**	**Remarks**
Attitude -> Behaviour (H6)	0.258	0.236	0.126	2.056	**0.040**	**Supported**
Knowledge -> Attitude (H4)	0.330	0.349	0.149	2.219	**0.027**	**Supported**
Knowledge -> Behaviour (H5)	0.346	0.387	0.159	2.168	**0.031**	**Supported**
Training -> Attitude (H3)	0.409	0.396	0.128	3.197	**0.001**	**Supported**
Training -> Behaviour (H2)	0.638	0.628	0.102	6.245	**0.000**	**Supported**
Training -> Knowledge (H1)	0.342	0.360	0.157	2.175	**0.030**	**Supported**

The research findings suggest that knowledge, attitude, behavior, and training all have a positive impact on cybersecurity awareness among university students. To enhance cybersecurity awareness effectively, educational interventions should focus on providing comprehensive knowledge, shaping positive attitudes, encouraging secure behaviors, and offering training programs.

H1: Training have Positive Impact on Knowledge:

Cybersecurity training programs designed to equip students with comprehensive knowledge and understanding of cybersecurity principles, best practices, and emerging threats. Through these programs, students gain insights into the latest technologies, vulnerabilities, and protective measures.

Training exposes students to real-world scenarios, case studies, and practical exercises that deepen their knowledge and enhance their problem-solving skills[18].

By participating in cybersecurity training, students expand their knowledge base and become aware of the evolving landscape of cyber threats. They learn about encryption, network security, secure coding practices, incident response, and ethical considerations. This knowledge empowers them to make informed decisions, identify potential risks, and take appropriate preventive measures.

H2: Training's Positive Impact on Behavior:

Training programs have a direct influence on students' behavior regarding cybersecurity. By providing practical skills and simulated scenarios, training enables students to apply their knowledge in real-world situations. They learn how to identify and respond to potential threats, implement security measures, and make informed decisions to protect themselves and others.

Training programs emphasize the importance of adopting secure behaviors and provide guidance on implementing best practices. Students learn about password hygiene, safe browsing habits, secure data storage, social engineering awareness, and secure communication practices. By participating in hands-on exercises and simulations, students develop the skills and confidence necessary to practice secure behaviors consistently.

H3: Training's Positive Impact on Attitude:

Cybersecurity training programs not only impart knowledge but also shape students' attitudes towards cybersecurity [23]. Training provides students with firsthand experiences and practical examples that highlight the importance of cybersecurity in their personal and professional lives. It raises their awareness of the potential consequences of cyber threats and instills a sense of responsibility towards practicing secure behaviors.

Through training, students gain a deeper understanding of the impact of cybersecurity breaches on individuals, organizations, and society as a whole [31]. They develop a proactive and positive attitude towards cybersecurity, recognizing it as a shared responsibility. Training programs emphasize the importance of ethical behavior, privacy protection, and the role of individuals in safeguarding digital assets. This positive attitude drives students to prioritize cybersecurity and adopt secure behaviors in their online activities.

H4 : Knowledge's Positive Impact on Attitude:

When students possess adequate knowledge about cybersecurity, they develop a better understanding of the risks and threats associated with the digital landscape [32]. This knowledge equips them with the necessary information to make informed decisions and form positive attitudes towards cybersecurity practices. Students who are knowledgeable about cybersecurity are more likely to perceive it as a priority and understand the potential consequences of inadequate security measures. This awareness fosters a positive attitude towards adopting and maintaining secure behaviors.

The students are aware of the importance of strong passwords, encryption, and regular software updates, they are more likely to view these practices positively and incorporate them into their digital routines. Knowledge empowers students to recognize the value of cybersecurity and instills a sense of responsibility towards protecting their digital assets and privacy.

H5: Knowledge's Positive Impact on Behavior:

Knowledge is a key driver in influencing students' behaviors related to cybersecurity. When students possess a comprehensive understanding of cybersecurity concepts, threats, and preventive measures, they are more likely to engage in secure behaviors [15], [31], [33]. They are equipped with the knowledge to recognize potential risks, identify suspicious activities, and implement effective security measures.

Students with knowledge about safe browsing practices, data protection, and social engineering techniques are more likely to exhibit cautious online behavior. They are less likely to click on suspicious links, share sensitive information with unknown sources, or fall victim to phishing attempts. Knowledge provides students with the confidence and competence to make informed decisions and take proactive steps to protect themselves from cyber threats.

H6: Attitude's Positive Impact on Behavior:

Attitude plays a crucial role in translating knowledge into behaviour [34]. A positive attitude towards cybersecurity is a driving force that motivates students to implement secure practices consistently. When students hold positive attitudes, they perceive cybersecurity as important and relevant to their daily lives. They understand the potential risks and believe in their ability to mitigate those risks through responsible behavior.

A positive attitude towards cybersecurity creates a mindset that prioritizes security and resilience. It fosters a willingness to adopt and maintain secure behaviors, even in the face of challenges or inconvenience. Students with positive attitudes are more likely to take proactive measures such as using strong passwords, enabling multi-factor authentication, regularly updating software, and being cautious with online interactions. Their attitudes shape their behaviors and contribute to a culture of cybersecurity awareness [35].

4. CONCLUSION

Cybersecurity awareness among university students is a critical issue that requires attention and intervention. This research has explored the current state of cybersecurity awareness among university students and identified key areas of improvement. The literature review highlighted the gaps in knowledge, attitudes, and behaviors related to cybersecurity among students. It emphasized the importance of education and training programs in enhancing cybersecurity awareness and fostering responsible online behavior.

The research method outlined in this study, which employs a quantitative approach and a cross-sectional survey design, provides a systematic and rigorous means of collecting data on cybersecurity awareness. The survey questionnaire will capture information on students' knowledge, attitudes, and behaviors, allowing for a comprehensive understanding of their cybersecurity awareness levels.

The findings from this research will contribute to the existing body of knowledge on cybersecurity awareness among university students. By identifying specific areas of weakness and factors that influence cybersecurity awareness, universities can develop targeted interventions and educational programs to address these gaps. Collaboration with industry partners and cybersecurity professionals can ensure that the educational initiatives align with current industry practices and emerging threats.

The outcomes of this research will have practical implications for universities, policymakers, and cybersecurity practitioners. The findings can guide the development of cybersecurity curricula, training programs, and awareness campaigns tailored to the needs of university students. By improving cybersecurity awareness among students, universities can play a vital role in cultivating a safer digital environment and preparing future professionals to navigate the evolving cybersecurity landscape.

It is important to acknowledge the limitations of this research, including the reliance on self-reported data and the cross-sectional design, which restricts the ability to establish causality. However, these limitations provide opportunities for future research to delve deeper into specific aspects of cybersecurity awareness and conduct longitudinal studies to assess the effectiveness of educational interventions over time.

Research contributes to the broader understanding of cybersecurity awareness among university students. By addressing the gaps in knowledge, attitudes, and behaviors, universities can empower students to protect themselves and others from cyber threats. Ultimately, fostering cybersecurity awareness among university students will have a positive impact on the overall security of individuals, organizations, and society in the digital age.

REFERENCES

[1] L. P. Asllani, A., White, C.S., & Ettkin, “iewing Cybersecurity as a Public Good: The Role

of Governments, Businesses, and Individuals.," *J. Leg. Ethical Regul.*, vol. 7, no. 16, 2013.

[2] B. K. Mamade and D. M. Dabala, "Exploring The Correlation between Cyber Security Awareness, Protection Measures and the State of Victimhood: The Case Study of Ambo University's Academic Staffs," *J. Cyber Secur. Mobil.*, 2021, doi: 10.13052/jcsm2245-1439.1044.

[3] F. R. Bechara and S. B. Schuch, "Cybersecurity and global regulatory challenges," *J. Financ. Crime*, 2021, doi: 10.1108/JFC-07-2020-0149.

[4] L. Alzahrani, "Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes," *Int. J. Adv. Comput. Sci. Appl.*, 2021, doi: 10.14569/IJACSA.2021.0121172.

[5] L. A. Alexei, "Cyber security strategies for higher education institutions," *J. Eng. Sci.*, 2021, [Online]. Available: https://ibn.idsi.md/vizualizare_articol/145834

[6] T. Hunt, "Cyber Security Awareness in Higher Education," *Cent. Washingt. Univ.*, 2016.

[7] N. K. Swain, "A Multi-Tier Approach to Cyber Security Education, Training, and Awareness in the Undergraduate Curriculum (CSETA)," in *121st ASEE Annual Conf*, 2014, p. Page 24.72.1-9.

[8] Y. Wang, B. Qi, H. X. Zou, and J. X. Li, "Framework of raising cyber security awareness," in *International Conference on Communication Technology Proceedings, ICCT*, 2019. doi: 10.1109/ICCT.2018.8599967.

[9] A. Mamun, J. Ibrahim, and S. M. Mostofa, *Cyber Security Awareness in Bangladesh: An Overview of Challenges and Strategies*. 2021.

[10] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," *Heliyon*, 2021, doi: 10.1016/j.heliyon.2021.e06016.

[11] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Comput. Secur.*, 2020, doi: 10.1016/j.cose.2020.102003.

[12] S. Hamzah, *Level of Awareness of Social Media Users on Cyber Security: Case Study among Students of University Tun Hussein Onn Malaysia*. 2021. doi: 10.17762/TURCOMAT.V12I2.923.

[13] M. Alqahtani, *Factors Affecting Cybersecurity Awareness among University Students*. 2022. doi: 10.3390/app12052589.

[14] S. Mousa, *Cyber Security : Exploring Awareness among University Students at a Public Educational Institution*. 2019.

[15] P. T. Mai and A. Tick, "Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in hungary and Vietnam," *Acta Polytech. Hungarica*, 2021, doi: 10.12700/APH.18.8.2021.8.4.

[16] L. Slusky and P. Partow-Navid, *Students Information Security Practices and Awareness*. 2012. doi: 10.1080/15536548.2012.10845664.

[17] R. Nagahawatta, M. Warren, and W. Yeoh, *A Study of Cyber Security Issues in Sri Lanka*. 2020. doi: 10.4018/ijcwt.2020070105.

[18] S. Al-Janabi and I. Al-Shourbaji, "A Study of Cyber Security Awareness in Educational Environment in the Middle East," *J. Inf. Knowl. Manag.*, 2016, doi: 10.1142/S0219649216500076.

[19] M. M. NOOR, M. A. S. H. J. Shah, and N. S. H. M. Zamri, *USER ACCEPTANCE OF CYBER SECURITY APPLICATION (OUR CYBERHERO) AMONG SECONDARY SCHOOL STUDENTS, TEACHERS AND LOCAL COMMUNITIES IN COASTAL TERENGGANU DISTRICT: A PRELIMINARY STUDY FOR MARITIME EDUCATION*. 2022. doi: 10.46754/jml.2022.12.006.

[20] B. Venard, *The determinants of individual cyber security behaviours: Qualitative research among French students*. 2019. doi: 10.1109/CyberSA.2019.8899648.

[21] K. Lynet, C. Mbogo, and N. Mwaniki, *A Digital Storytelling Model for Increasing Information Security Awareness among Kenyan Smartphone Users*. 2020.

[22] A. R. Ahlan, Y. Arshad, and M. Lubis, *Implication of human attitude factors toward information security: awareness in Malaysia Public University*. 2011.

[23] M. D. E. Alsiddig, A. A. alraheem A. Badwi, and O. I. A. Idriss, "Cyber security awareness among students and faculty members in a Sudanese college," *Electr. Sci. Eng.*, 2020, doi:

10.30564/ese.v2i2.2477.

[24] M. S. Joseph F. Hair, Jr,G. Tomas M. Hult, Christian M. Ringle, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 3rd ed. Los Angeles: SAGE Publications, 2022.

[25] J. V. E. Vinzi, W. W. Chin and H. & H. Wang, *Handbook of Partial Least Squares: Concepts, Methods and Applications*, New York: Heidelberg, Dordrecht, London, 2010.

[26] W. W. Chinn, “The Partial Least Squares Approach to Structural Equation Modelling,” *Mod. Methods Bus. Res.*, 1998.

[27] C. M. Ringle, M. Sarstedt, and D. W. Straub, “A critical look at the use of PLS-SEM in MIS quarterly,” *MIS Quarterly: Management Information Systems*. 2012.

[28] C. M. Ringle, S. Wende, and S. Will, “SmartPLS 2.0 (M3) Beta,” *Hamburg*, 2005.

[29] J. F. Hair Jr, W. C. Black, B. J. Babin, and R. E. Anderson, “Multivariate data analysis (7th edition): Pearson Education Inc,” *New Jersey, USA*, 2010.

[30] W. Abdillah and H. Jogiyanto, “Partial Least Square (PLS) Alternatif Structural Equation Modeling (SEM) dalam Penelitian Bisnis,” in *book*, 2015.

[31] S. Shukla, M. M. Tiwari, A. C. Lokhande, T. Tiwari, R. Singh, and A. Beri, *A Comparative Study of Cyber Security Awareness, Competence and Behavior*. 2022. doi: 10.1109/IC3I56241.2022.10072880.

[32] P. R. J. Trim and Y. I. Lee, “The role of B2B marketers in increasing cyber security awareness and influencing behavioural change,” *Ind. Mark. Manag.*, 2019, doi: 10.1016/j.indmarman.2019.04.003.

[33] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, “Cyber Security Awareness, Knowledge and Behavior: A Comparative Study,” *J. Comput. Inf. Syst.*, 2022, doi: 10.1080/08874417.2020.1712269.

[34] Y. Salem, M. Moreb, and K. S. Rabayah, *Evaluation of Information Security Awareness among Palestinian Learners*. 2021. doi: 10.1109/ICIT52682.2021.9491639.

[35] S. A. Adelekan, M. Williamson, and S. O. Atiku, “Influence of social entrepreneurship pedagogical initiatives on students’ attitudes and behaviours,” *J. Bus. Retail Manag. Res.*, vol. 12, no. 3, 2018, doi: 10.24052/jbrmr/v12is03/art-15.