Effectiveness of Cybersecurity Awareness Program Based on Mobile Learning to Improve Cyber Hygiene

Herman Dwi Surdjono[1], Radinal Fadli[2], Ratna Candra Sari[1], Fivia Eliza[3,*], Abdulnassir Yassin[4], G. Kulanthaivel[5], M. Agphin Ramadhan[6], Riki Mukhaiyar[3], Mustofa Abi Hamid[7], M. Rais Ridwan[8], Sigit Purnomo[9], and Asnimawati[10]

[1]Postgraduate Program, Universitas Negeri Yogyakarta, Yogyakarta, Indonesia
[2]Departmentof Information Technology Education, Universitas Muhammadiyah Muara Bungo, Bungo, Indonesia
[3]Department of Electrical Engineering, Universitas Negeri Padang, Padang, Indonesia
[4]Department of Curriculum and Instruction, Islamic University in Uganda, Kampala, Uganda
[5]Department of Electrical Electronics and Communication Engineering, National Institute of Technical Teachers Training and Research, Chennai, India
[6]Department of Building Engineering Education, Universitas Negeri Jakarta, Jakarta, Indonesia
[7]Department of Electrical Engineering Vocational Education, Universitas Sultan Ageng Tirtayasa, Banten, Indonesia
[8]Department of Mathematics Education, STKIP YPUP Makassar, Makassar, Indonesia
[9]Department of Mechanical Engineering Education, Universitas Sarjanawiyata Tamansiswa, Yogyakarta, Indonesia
[10]Department of Social Studies Education, Universitas Negeri Surabaya, Surabaya, Indonesia
Email: hermansurjono@uny.ac.id (H.D.S.); fadliradinal@gmail.com (R.F.); ratna_candrasari@uny.ac.id (R.C.S.); fivia_eliza@ft.unp.ac.id (F.E.); nasiryasin681@gmail.com (A.Y.); gkveldr@gmail.com (G.K.); agphin@unj.ac.id (M.A.R); riki.mukhaiyar@ft.unp.ac.id (R.M.); abi.mustofa@untirta.ac.id (M.A.H); mraisridwan@stkip.ypup.ac.id (M.R.R.); sigitpurnomo@ustjogja.ac.id (S.P.); asnimawati@unesa.ac.id (A.)
[*]Corresponding author

Manuscript received August 2, 2024; revised August 21, 2024; accepted October 14, 2024; published February 11, 2025

***Abstract*—This research aims to investigate the effectiveness of a Mobile Learning-based cybersecurity awareness program in improving cyber hygiene practices among accounting and finance students. This is a research and development conducted using the 4D model approach (Define, Design, Develop, and Disseminate). This research involved three research experts in mobile learning and cybersecurity, with 68 participants being accounting and finance students. Instruments used include validity questionnaires, cybersecurity awareness tests, and cyber hygiene practices questionnaires. Data were analyzed using quantitative descriptive techniques. Consequently, the Mobile learning cybersecurity program proved valid based on expert assessments. The test results revealed a significant improvement in cybersecurity awareness and practices following the program's implementation. The effectiveness test results show that the Mobile Learning-based cybersecurity awareness program improves cybersecurity practices. This study addresses the growing demand for cybersecurity awareness in sectors vulnerable to cyber-attacks, particularly accounting and finance. By leveraging interactive and flexible mobile learning features, this program overcomes limitations found in previous approaches, providing an innovative solution for enhancing cybersecurity practices. However, the study is limited by its short-term scope, and Future research should not only focus on long-term assessments but also explore the program's applicability across different educational disciplines.**

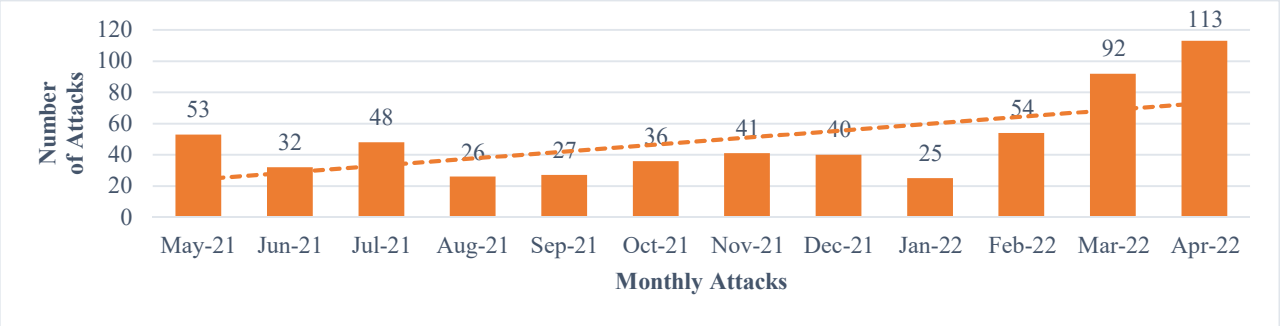
***Keywords*—cybersecurity, cybersecurity awareness, digital safety, mobile learning, cyber hygiene, finance, accounting**

I. Introduction

Today, the digital landscape has transformed our world [1], driving the growth of a digital economy filled with the constant exchange of sensitive data. However, amidst this rapid progress, there is a hidden threat in the form of the increasing threat of cyber-attacks in Indonesia recently [2]. As businesses and individuals increasingly entrust their financial information to the digital world, cybercriminals are honing their skills, devising increasingly sophisticated tactics, and leveraging the latest technologies to exploit vulnerabilities and endanger valuable assets.

Additionally, Cybersecurity is considered a technological problem, further, human factors also play an important role [3]. Many cyber-attacks are caused by human error [4], such as opening unknown attachments or clicking on malicious links [5]. The data most often targeted by hackers is data that contains sensitive and valuable information, such as company financial information [6], financial transaction data, client personal information, and bank account details [7–10]. This data is paramount to hackers because it can be used to commit identity theft, financial fraud, or extortion. This data is data managed by accounting and finance graduates, they stand on the frontline of this digital battlefield. Hacking, identity theft, and other cyberattacks can destroy reputations, threaten privacy, and cause serious financial losses. Therefore, to equip accounting and finance students with a strong cybersecurity awareness, cyber hygiene practices are not only a wise precaution, but also a necessity.

In recent years, the trend of cyber-attacks has changed significantly, as the tactics used by hackers have become more sophisticated. One of the most prominent trends in cyber-attacks is the increase in ransomware attacks, where important data is encrypted and will only be unlocked after a ransom is paid [11]. Based on a report by the European Union Agency for Cybersecurity (ENISA) [12], from 27 European Union countries from May 2021 to April 2022 there were 587 ransomware attacks. The lowest attack occurred in January 2022 with 25, and the highest attack occurred in April 2022, namely 113 attacks, and continues to increase across European Union countries. More complete data can be seen in Fig. 1 below.



Data source: ENISA Threat Landscape for Ransomware Attacks 2022 [12]
Fig. 1. Ransomware attack trends.

In addition, attacks on mobile devices are also increasing, given the increasing use of these devices for financial transactions and other business activities [13]. In addition, the application of Artificial Intelligence (AI) in cyber-attacks is also a serious concern. AI technology has enabled the creation of deepfakes, which can be used to spread false information or manipulate identities [14], aided with advanced AI capabilities, it is possible to automate more targeted and difficult-to-detect phishing attacks [15]. This trend shows that cyber threats are becoming more complex and increasingly targeted at the most sensitive and valuable data, especially in the financial sector. This condition reinforces the urgency to equip students in accounting and finance with strong cyber hygiene awareness and skills. To ensure protection against increasingly evolving threats.

Various cybersecurity awareness program approaches have been developed previously, such as the approach taken by [16], in the form of a security awareness campaign conducted among remote workers. While these campaigns can increase awareness levels, they are often temporary, with messages quickly forgotten after the campaign. Without sustained effort, that awareness can decline over time. Another program carried out by [17], in the form of a cybersecurity awareness program in traditional classes using modules, the results of the research show changes in terms of knowledge and skills as well as desired behavioral practices in protecting personal data. However, the research findings show that undesirable behavior is still being carried out. This happens because, classroom lectures or static modules, often fail to attract participants' interest, causing knowledge retention problems and hindering the development of practical cybersecurity skills [18, 19]. In contrast, mobile learning capabilities present content in an interactive and personalized manner, making learning more engaging [20–22]. Interactive features such as quizzes, simulations, and case studies also help improve knowledge retention and the development of practical skills in cybersecurity [23, 24]. Thus, mobile learning approaches can provide effective alternative solutions for the obstacles associated with cybersecurity awareness programs in traditional classrooms.

Another cybersecurity awareness approach that is widely used is Capture the Flag (CTF), as developed by [25, 26], research results show that CTF is effective in honing technical skills in finding loopholes in systems, but is more suitable for participants with technology educational background, while participants with accounting and financial educational backgrounds who do not have in-depth knowledge of technology are not suitable for this method. In other research conducted by [27–29], who developed a cybersecurity awareness program with games, the research findings revealed that this method was quite good for increasing cybersecurity awareness, however, limited accessibility was a challenge for this approach, apart from implementing it. Requires a lot of resources to run. Compared with game-based cybersecurity awareness programs, mobile learning is more efficient in resources and accessibility. Mobile learning does not require the huge investment in operation that gaming requires. Using devices that users are generally aware of, such as smartphones or tablets, mobile learning-based, cybersecurity awareness programs can be accessible at a relatively low cost. Therefore, mobile learning has become a more economical yet effective option for increasing cybersecurity awareness [30]. The flexibility, accessibility, and interactivity capabilities inherent in mobile-based learning have become a promising alternative [31]. Many studies are showing the effectiveness of mobile learning in improving learning outcomes, understanding, and motivation in various disciplines [32–35], similar approaches have the potential to increase the cybersecurity awareness of vocational school students in accounting and finance. Based on several previous studies, there is still an unexplored knowledge gap in cybersecurity awareness, which has not yet integrated mobile-based learning elements to increase cybersecurity awareness to create cyber hygiene behavior.

With the increasing number of cyber-attacks targeting the financial sector recently, this research is urgently required to address a significant gap in cybersecurity education. Accounting and finance students, who are often responsible for managing highly sensitive financial data, are at the frontline of cyber threats. Despite the existence of advanced technologies to mitigate cyber-attacks, human error remains a primary cause of security breaches. Traditional cybersecurity training methods, such as classroom-based instruction or security awareness campaigns, have proven less effective in engaging students and ensuring long-term retention of critical cyber hygiene practices. This study aims to answer the following research questions: (1) How valid is a mobile learning-based cybersecurity program designed to be used as a medium to improve cyber hygiene? (2) How effective is a mobile learning-based cybersecurity program in improving cybersecurity awareness among accounting and finance students? (3) How effective is a mobile learning-based cybersecurity program in improving cyber hygiene among accounting and finance students? The results of the current research contribute to science, especially in the field of cybersecurity awareness, by overcoming the problems of

previous approaches, namely security awareness programs that are not sustainable, do not attract student interest, can only be used by students with a technology education background, and require investment costs. The big one. Apart from that, the results can be used as a guide for educational institutions in formulating policies regarding the integration of cybersecurity into the curriculum.

II. Method

A. Research Methodology

The research design used in this study is based on the 4D model. The 4D Model, also known as the Four-Dimensional Model of Research and Development, is a systematic framework commonly used in developmental studies. The 4D Model was selected as it provides a structured approach for developing educational programs, ensuring that the final product is both pedagogically sound and practically applicable for the targeted participants. Each phase of the model is designed to address key elements such as content relevance, instructional design, and scalability, which are essential for delivering a cybersecurity awareness program It consists of four iterative phases, namely Define, Design, Develop, and Disseminate [36]. The research stages are illustrated in Fig. 2 below.

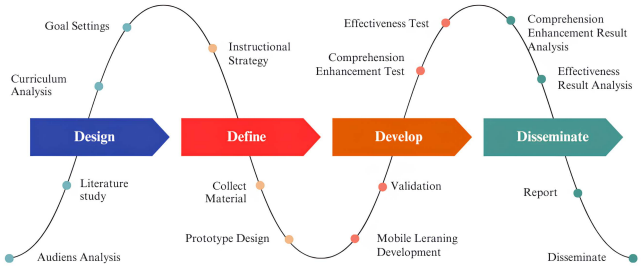


Fig. 2. Research procedure.

Define: the initial phase will carefully define the specific challenges accounting and finance students face in the digital era. Through interviews, surveys, and focus groups, we will gain a comprehensive understanding of their cybersecurity awareness, knowledge gaps, and preferred learning styles. These activities will inform the development of program objectives, ensuring alignment with specific student needs and the broader goal of encouraging robust cyber hygiene practices.

Design: the second phase will focus on carefully designing and developing mobile learning programs. Guided by the principles of engagement and interactivity, the program will incorporate elements such as interactive modules, animations, personalized learning paths, and incident simulations, as well as discussion rooms. Content will be carefully curated to meet the specific knowledge and skills needs of accounting and finance students, covering topics such as data security, password management, phishing awareness, and social engineering strategies.

Develop: In the Development stage, researchers initially implement a cybersecurity awareness program in a limited environment to get feedback and improvements so that it can be perfected. Furthermore, the validity and efficacy of the program will be carefully assessed through a review by 5 cybersecurity experts and media experts. Next, a cybersecurity awareness program was implemented on the research sample. Next, assess cybersecurity awareness with tests, and cyber hygiene behavior with questionnaire instruments.

Disseminate: At the dissemination stage, test results and student questionnaire responses are analyzed to obtain meaningful insights. Next, the results of the analysis are interpreted and presented in a comprehensive research report. Researchers prepare scientific articles to be published in reputable international journals. The main objective of this stage is to distribute and convey research findings to the scientific and practitioner community in the field of accounting and finance education and the field of cybersecurity awareness.

B. Subject of Research

This research involved Vocational High School students taking educational programs in the fields of Accounting and Finance. The sample used in this study consisted of 68 students who were in their second year of education, which is equivalent to grade 11 in the K-12 education system. The age range of the sample ranged from 16 to 18 years. Of the total sample, there were 26 male students and 42 female students. Ethical approval was obtained prior to conducting the study. All participants were informed about the purpose of the research, and written informed consent was obtained. Participants were assured of their anonymity, and data confidentiality was maintained throughout the research process. Additionally, participants were given the freedom to withdraw from the study at any time without any consequences. The characteristics of the research sample can be seen in the following Table 1.

Table 1. Characteristics of the research sample

Criteria	Details
Type of Education	Vocational High Education
Education Program	Accounting and Finance
Year of Study	2nd Year (11 In K-12)
Age Range	16-18 years
Gender	26 Male 42 Female
Total Sample	68

The sampling method used was total sampling, where the entire population of students from several vocational schools was included as a sample in this research. This approach was chosen to ensure maximum representativeness of the population studied, as total sampling is appropriate when the population size is manageable and when the aim is to include all members of the population in the study to avoid sampling bias [37]. Purposive sampling was not used because the research aimed to generalize the findings across the entire population rather than focusing on specific subgroups or criteria that purposive sampling would target.

C. Research Instrument

In the data collection process, this research uses several instruments that have been carefully prepared. The instruments used consist of validity instruments, knowledge tests, and cyber hygiene behavior instruments. The validity of the instrument was evaluated by several experienced experts in the field. The validity indicators of the instruments used in this research have been documented and can be seen in detail in Table 2 below.

Table 2. Validity instrument indicators

Indicator	No. item
Curriculum Coherence	1,2,3
Operational	4,5,6,7
Performance	8,9,10,11,12
Security	13,14,15,16
Design	17,18,19,20

Next is the cybersecurity awareness test instrument designed with the main objective of assessing the level of students' understanding of cybersecurity awareness material. The method used is pre-test and post-test. In the initial stage, before students take part in the mobile learning-based cybersecurity awareness program, a pre-test is given to measure their basic knowledge of cybersecurity concepts. The pre-test provides an initial overview of students' understanding before taking part in the program. After undergoing the cybersecurity awareness program, students are given a post-test to measure their increase in understanding after taking part in the program. The test instrument was formulated based on previous research [38–45]. So the 6th assessment indicators are obtained, namely Passwords and Access control, Software and Hardware Security, Mail and Data Protection, Network Security, Data Backup and Recovery, and Encryption. Based on the indicators, 30 test questions are formulated which will be tested for validity, reliability, discriminatory power, and level of difficulty first. Details can be seen in Table 3 below.

Table 3. Cybersecurity comprehension test

Indicator	No. item
Passwords and Access control	1,2,3,4,5
Software and Hardware Security	6,7,8,9,10
Mail and Data Protection	11,12,13,14,15
Network Security	16,17,18,19,20
Data Backup and Recovery	21,22,23,24,25
Encryption	26,27,28,29,30

Furthermore, to evaluate the effectiveness of using cybersecurity awareness programs in improving cyber hygiene behavior, a cyber hygiene behavior instrument was used. This cyber hygiene behavior instrument is designed to measure the extent to which students have internalized the cybersecurity concepts taught in the program. Using this instrument, we can assess the extent to which students have changed their behavior concerning cybersecurity after participating in a cybersecurity awareness program. Various behavioral aspects, such as the use of strong passwords, the use of security software, awareness of cyber threats, and other preventive measures were evaluated through this questionnaire, more details can be seen in Table 4.

However, the Cyber Hygiene Behavior questionnaire that had been prepared was first given to several experts who had expertise in the field of cybersecurity and educational media. The purpose of giving the questionnaire was to obtain input and assessments that could assess the level of validity and reliability of the instrument that had been prepared. The validity assessment given by the experts was then analyzed using Aiken's V validity coefficient calculation method and the reliability was analyzed using Cronbach's Alpha which is one of the methods commonly used in assessing the validity of research instruments. The results of the validity assessment from each expert were then collected and analyzed to determine the suitability of the instrument with what was to be studied. The cybersecurity awareness program that had been prepared would be said to be valid if it had met the validity standards in Table 3 and would be declared reliable if it met the reliability standards in Table 4.

Table 4. Cyber hygiene behavior indicators

Indicator	No. item
Passwords and Access control	1,2,3,4,5
Software and Hardware Security	6,7,8,9,10
Mail and Data Protection	11,12,13,14,15
Network Security	16,17,18,19,20
Data Backup and Recovery	21,22,23,24,25
Encryption	26,27,28,29,30

D. Data Collection Technique

1) Mobile learning validity test

The mobile learning validity test was conducted by involving four experts, consisting of two learning media experts and two cybersecurity experts. These experts reviewed and evaluated the design and content of the mobile learning developed, to ensure that this platform is valid and suitable for use in an educational context. This validation covers various aspects according to the indicators in Table 2.

2) Validity and reliability test of cyber hygiene behavior instrument

Validity and reliability tests were conducted to ensure that the Cyber Hygiene behavior measurement instrument has a high level of accuracy and consistency. This instrument was validated by experts in the field of cybersecurity and technology education, to assess whether each item in the questionnaire can measure aspects of cyber hygiene behavior accurately. The validity test was conducted using Aiken's validity coefficient calculation method, which is to compare the score of each item with the total score of the questionnaire. Meanwhile, the reliability test was conducted using Cronbach's Alpha coefficient to ensure that the instrument has adequate internal consistency.

3) Cyber security comprehension test

The Cyber Security Comprehension Test aims to measure students' understanding of cybersecurity before and after they take part in mobile learning-based learning. The test items used have met the standard criteria for validity, level of difficulty, discrimination, and reliability that have been reported in previous studies. Thus, the results of this test can provide a clear picture of the extent to which the learning program implemented can improve students' understanding of important aspects of cybersecurity.

4) Cyber hygiene behavior

The Cyber Hygiene Behavior Test was conducted by giving students a questionnaire after they had taken part in the entire learning series. This questionnaire was designed to measure changes in student behavior related to good cyber hygiene practices. Through this questionnaire, researchers can assess whether the learning that has been carried out has succeeded in influencing students' behavior in maintaining the security of their information and personal data in cyberspace.

E. Data Analysis

Quantitative descriptive data analysis was employed to assess both the validity of the program and the improvement in cybersecurity awareness and hygiene behavior. This

method was chosen as it allows for the systematic evaluation of pre-test and post-test results, providing empirical evidence of the program's effectiveness in enhancing student awareness and practices.

1) Mobile learning validity test

In data analysis for the mobile learning validity test, researchers used descriptive analysis techniques to assess the responses of the experts involved in the evaluation. For each aspect assessed, the average score from the experts is then compared with the validity criteria in Table 5. If the score shows that most aspects are considered valid by the experts, then mobile learning is considered suitable for use in further research. The formula used to analyze the validity test is as follows.

$$V = \sum S/[n(c-1)] \quad (1)$$

Description:
V = Validity Index
s = $r - lo$
n = Number of validators or panel of raters
lo = The lowest validity assessment number (in this case = 1)
c = The highest validity assessment number (in this case = 5)
r = Value given by a validator.

Table 5. Validity criteria

Criteria	Description
≥0.6	Valid
<0.6	Invalid

2) Validity and reliability test of cyber hygiene behavior instrument

In the analysis of the validity and reliability test of the Cyber Hygiene behavior instrument, researchers analyzed the data using two main methods. The validity test was conducted using Aiken's validity coefficient, to determine whether the items in the instrument collectively measure the same construct. Items that have validity values that do not meet the standards will be removed from the instrument. The formula used is the same as formula 1, and the indicators used are the same as in Table 5. Furthermore, the reliability test was conducted using Cronbach's Alpha to measure the internal consistency of the instrument. The resulting Cronbach's Alpha value will indicate whether the instrument is stable and reliable in measuring cyber hygiene behavior. If the Cronbach's Alpha value is equal to or greater than 0.60, then the instrument is considered reliable and ready to be used in research.

3) Cyber security comprehension test

Data obtained from the Cyber Security Comprehension Test were analyzed by comparing the score gains before and after learning with mobile learning. By analyzing the differences in pre-test and post-test scores, researchers can determine how much students' understanding has increased after following the learning program based on the improvement criteria that can be seen in Table 6. The results of this analysis provide empirical evidence regarding the effectiveness of the learning program in increasing awareness and understanding of cybersecurity. The formula used to analyze the results of the Cyber Security Comprehension Test is as follows.

$$< g >= \frac{(\%<Sf>-\%<c>}{(100-\%<Si>} \quad (2)$$

Description:
g = gain score
Sf = posttest score
Sf = pretest score.

Table 6. Gain score criteria

Gain Score	Interpretation
(<g>) ≥ 0.7	High
0.7 > (<g>) ≥ 0.3	Medium
(<g>) < 0.3	Low

4) Cyber Hygiene Behavior

Data analysis for the Cyber Hygiene Behavior test was carried out using descriptive statistics. This is to identify student behavior patterns in maintaining information security after participating in learning. The results of this analysis provide insight into the extent to which mobile learning-based learning has succeeded in influencing and changing student behavior in maintaining their digital security. Data obtained from the cyber hygiene behavior questionnaire will be compared with the effectiveness categories presented in Table 7. Data obtained from the questionnaire will be analyzed using the following formula.

$$NA = \frac{S}{M} \times 100\% \quad (3)$$

Description:
NA = Final Score
S = Score obtained
M = Maximum score.

Table 7. Category effectiveness

Indicator	Criteria
85–100	Very Effective
75–84	Effective
60–74	Moderately Effective
55–59	Less Effective
0–54	Not Effective

III. Result and Discussion

A. Design Result

In the design stage of the cybersecurity awareness program, we developed learning content specifically designed for accounting and finance. The application is designed to cover five lessons consisting of an introduction to cybersecurity, Password and Access control, Software and Hardware safety, Mail and Data Protection, Network safety, Data Backup and Recovery, and Data encryption.

The Welcome Page Displays the main title of the "cybersecurity awareness" program, along with related icons that represent each sub-material contained in this educational media. The page contains two different buttons: A 'Get Started' button that takes the user to the Main Page to select the desired learning material, and a 'Get Hacked' button that allows the user to close the interface. The initial display can be seen in Fig. 3 below.

The Main Page Providing a variety of cybersecurity awareness lessons allows students to choose content based on their academic needs. Each lesson selection button is

accompanied by an icon representing the related sub-lesson, making it easy to navigate to the selected topic. In addition, this page features a simulation menu that guides students to a phishing mail simulation for practical cyber-attack analysis exercises. The layout of the main page is illustrated in Fig. 4 below.

Fig. 3. Intro.

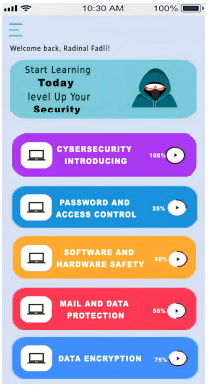


Fig. 4. Main page.

The Lesson Page The learning content is displayed through textual information, animations, images, and case studies of accounting and finance-related cybersecurity incidents that have occurred. In addition, animated videos are incorporated to attract students' interest and explain the concept of real-life cyber hygiene behavior. Students have the flexibility to replay the videos based on their learning pace, thus enabling them to comprehensively understand the lesson. The visual representation of the lesson page is depicted in Fig. 5 below.

Fig. 5. Lesson page.

The Simulation Page The simulation practice page is a simulation provided to improve analysis in identifying mail phishing, fake links, hoax websites, malware, deep fake voice, and deep fake video. In this environment, students can test what happens if they fail to analyze these types of phishing. The simulation is designed to create a learning experience like real-life conditions, with advantages in flexibility and accessibility. Students can simulate without time constraints, allowing them to repeat their analysis and deepen their understanding of cyber hygiene concepts. A visual representation of the Simulation page is depicted in Fig. 6 below.

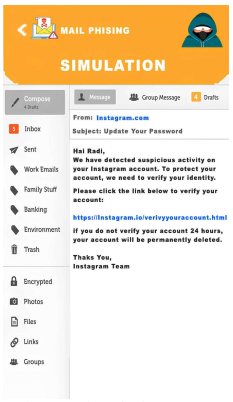


Fig. 6. Simulation page.

The Discussion Room is specifically designed to make it easier for students to communicate and discuss various aspects of cybersecurity that they have not yet understood. If students encounter certain obstacles or problems they can open a new discussion topic in this room, letting their friends provide views, suggestions, or solutions. In addition, the Discussion Room also allows students to respond and interact with the topic at hand, enriching the discussion with various views and experiences. This creates a collaborative learning environment where each student can benefit from the expertise and experience of their peers. Sometimes students require further guidance or explanation from the teacher. Therefore, this app has a chat feature that allows students to communicate directly with the lecturer. Through this feature, students can get quick answers or additional guidance that they may need. The appearance of the discussion room can be seen in Fig. 7 below.

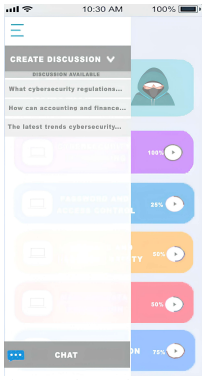


Fig. 7. Discussion room.

B. Validity and Reliability Test of Cyber Hygiene Behavior Instrument

The cyber hygiene behavior instrument given to students was first tested for validity using product moment correlation. This is done by comparing the calculated "r" value with the critical value "r" from the n-2 degrees of freedom (df) table, where in this case n represents the number of samples in this

study, namely $n = 68$. Therefore, df can be calculated as 68-2 = 66. Considering $df = 66$ and alpha set at 0.05, the critical value "r" from the table is determined to be 0.3104 (based on a two-tailed test at $df = 66$). As a rule, if the calculated "r" value exceeds the critical value "r" (0.3104), then the questions in the questionnaire can be considered valid. Complete results can be seen in Table 8 below.

Table 8. Validity test results of the cyber hygiene behavior instrument

No. Item	R calculated	R table	Criteria
1	0.315	0.3104	Valid
2	0.368	0.3104	Valid
3	0.685	0.3104	Valid
4	0.468	0.3104	Valid
5	0.457	0.3104	Valid
6	0.325	0.3104	Valid
7	0.595	0.3104	Valid
8	0.388	0.3104	Valid
9	0.386	0.3104	Valid
10	0.985	0.3104	Valid
11	0.756	0.3104	Valid
12	0.365	0.3104	Valid
13	0.486	0.3104	Valid
14	0.398	0.3104	Valid
15	0.545	0.3104	Valid
16	0.425	0.3104	Valid
17	0.390	0.3104	Valid
18	0.592	0.3104	Valid
19	0.355	0.3104	Valid
20	0.752	0.3104	Valid
21	0.365	0.3104	Valid
22	0. 651	0.3104	Valid
23	0.475	0.3104	Valid
24	0.550	0.3104	Valid
25	0.525	0.3104	Valid
26	0.458	0.3104	Valid
27	0.420	0.3104	Valid
28	0.465	0.3104	Valid
29	0.325	0.3104	Valid
30	0.482	0.3104	Valid

Based on the results of the instrument validity test, 30 valid statement items were obtained so that they can be used to measure the effectiveness of cybersecurity awareness programs in improving cyber hygiene behavior. Next, the instrument was tested for reliability using Cronbach's Alpha, the results obtained were 0.830 > 0.60 so the instrument was declared reliable.

C. Validity Test

This development phase evaluates the validity, determines the level of understanding through tests, and tests the effectiveness of the mobile learning-based cybersecurity awareness program that has been produced. The validation process began with testing by three experienced experts in technology and education who have expertise in cybersecurity awareness. The experts were asked to evaluate the content according to a given questionnaire. During the evaluation, valuable feedback was obtained from the experts regarding potential improvements and enhancements to the content. The assessment results from the experts were analyzed to obtain comprehensive information. The results of the validity evaluation can be seen in Fig. 8 below.

The results of the validity test of the cybersecurity awareness program based on mobile learning show a very positive achievement, with each indicator getting consistent scores and meeting the established validity criteria. The evaluation of Curriculum, Operationalization, Performance, Security, and Design resulted in an average validity score of 0.8 to 0.9, all of which fall into the Valid category. This indicates that every aspect of the program, including its curriculum content, operationalization, performance, security, and design, has successfully passed the validity testing with excellent results. The Valid category indicates that each component of the program has been recognized as credible and in line with the standards set in the context of cybersecurity awareness. The assessment by technology and education experts of each indicator provided positive validation of the overall program structure and content. Therefore, the conclusion from the results of this validity test states that this mobile learning-based cybersecurity awareness program is reliable and meets the standards of validity required to achieve the learning objectives. The program's success in achieving validity confirms that this approach can be used as an effective and reliable learning method in improving students' understanding and awareness of cybersecurity.

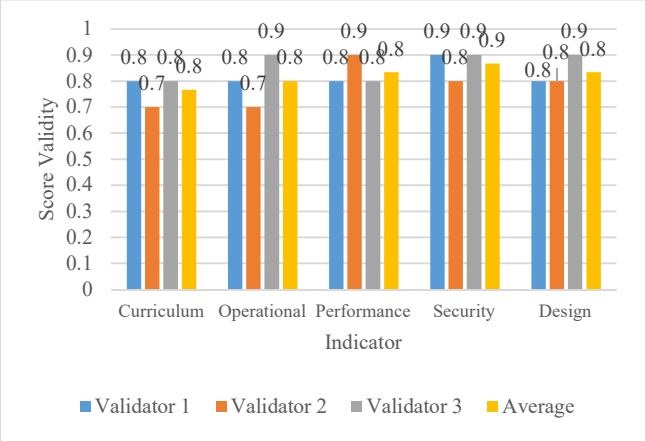


Fig. 8. Validity result.

D. Comprehension Enhancement Test

The test of understanding the cybersecurity lesson was given before and after students implemented a series of cybersecurity awareness programs based on mobile learning. The test results were analyzed with a gain score to see how much the learning outcomes improved before and after. The results of the pretest and post-test gain score test of the cybersecurity awareness program show a satisfactory number, which is reflected in the gain score value of 0.72. This gain score value is the difference between the post-test and pre-test, illustrating the increase in student understanding after participating in the program. With a minimum gain score range of 0.50 and a maximum gain score of 0.93, the gain score value of 0.72 can be categorized as "High." This high category reflects a significant change in students' understanding after engaging in the cybersecurity awareness program. This substantial increase indicates that the program has successfully achieved its goal of improving students' understanding of cybersecurity concepts.

E. Effectiveness Test

The effectiveness test of the mobile learning-based cybersecurity awareness program to improve cyber hygiene was given after the students finished running the program. The instrument was given to 68 Vocational High School students in accounting and finance. Respondents were asked

to provide an assessment and response according to the questionnaire given. The collected data was then analyzed to obtain results which can be seen in Table 9 below.

Table 9. Effectiveness test results

Indicator	Score	Category
Passwords and Access control	85	Very Effective
Software and Hardware Security	80	Effective
Mail and Data Protection	87	Very Effective
Network Security	80	Effective
Data Backup and Recovery	77	Effective
Encryption	80	Effective

The Results of the effectiveness test of the security awareness program in improving cyber hygiene show a positive and satisfactory achievement based on the scores obtained on each indicator. In the Password and Access Control aspect, the program achieved a score of 85, the category can be classified as Highly Effective. This indicates that the program successfully encouraged the practice of the importance of adequate password management and access control. On the Software and Hardware Safety aspect, the program achieved a score of 80, reaching the Effective category. Likewise, on the Mail and Data Protection indicator, the program showed very positive results with a score of 87, categorized as Highly Effective, signifying the program's success in successfully encouraging the practice of the need to effectively protect email and data. Network Safety, Data Backup and Recovery, and Encryption also achieved scores of 80, 77, and 80, respectively, all categorized as Effective. This indicates that the program has successfully encouraged the practice of skills related to these aspects of cybersecurity. With consistent results in the effective to highly effective categories, it can be concluded that this cybersecurity awareness program has successfully achieved its goal of improving cyber hygiene among accounting and finance students. These results provide a positive indication of the program's success in providing significant understanding and motivating safer behavioral changes related to cybersecurity.

F. Discussion

This research produces a mobile learning-based cybersecurity awareness program that is valid and effective for improving cyber hygiene practices among accounting and finance students. Validation results confirm the program's alignment with quality standards and its potential to meet specific needs that align with accounting and finance requirements. In addition, the results of the increased understanding test showed an increase in participants' understanding after engagement with the mobile learning-based cybersecurity awareness program. The significant post-implementation improvement underscores the program's effectiveness in delivering cybersecurity content and promoting a deeper understanding of key concepts. Based on these results, the findings of this research support the hypothesis that this program has succeeded in increasing cyber hygiene practices among accounting and finance students.

These findings align with previous research conducted by [46], which demonstrated that mobile learning is more effective than traditional methods due to its ability to accommodate students' learning speeds and provide personalized learning experiences. The interactive features of mobile learning, such as quizzes, animations, simulations, and case studies, have been shown to significantly improve knowledge retention and skill development, as they actively engage learners and make abstract concepts more tangible. This result is further supported by research conducted by [47] which highlights the effectiveness of mobile learning in presenting complex material in a more understandable and engaging manner. Additionally [48], found that mobile learning enhances learning experiences across various contexts, reinforcing the idea that this approach can be highly effective in improving student engagement and retention in cybersecurity education. The improvement in understanding observed in this study can be attributed to several factors, including the flexibility of mobile learning, which allows students to learn at their own pace. This flexibility is particularly important for learners with varying levels of prior knowledge, as it provides a more personalized and adaptive learning environment. Interactive elements, such as real-time quizzes and simulations, may have played a pivotal role in reinforcing key cybersecurity concepts, offering students the opportunity to apply their knowledge in practical scenarios. These findings are consistent with cognitive learning theories, which suggest that interactive and experiential learning fosters deeper knowledge retention and practical skill development.

In addition to validating previous research, this study contributes new insights by focusing specifically on accounting and finance students, a group that is often overlooked in cybersecurity education. While studies like [49–51], emphasize the importance of cybersecurity awareness in general, this research demonstrates that mobile learning can be a particularly effective tool for non-technical students, helping them to develop the necessary skills to protect sensitive financial data. Furthermore, this study highlights the potential of mobile learning to overcome challenges associated with traditional classroom-based cybersecurity programs, such as limited engagement and knowledge retention.

However, several limitations should be acknowledged. First, the study's short-term focus limits the ability to assess the long-term impact of the program on cybersecurity awareness and behavior. Additionally, this study did not account for potential variations in students' prior exposure to digital tools and cybersecurity knowledge, which could have influenced their learning outcomes. Differences in motivation levels and personal interest in cybersecurity were also not controlled, potentially affecting the results. These variables should be addressed in future research to provide a more comprehensive understanding of how different factors influence the effectiveness of mobile learning in cybersecurity education.

Finally, while the findings suggest that mobile learning is an effective method for improving cybersecurity awareness, further research is needed to validate these results across different educational contexts and populations. Future studies should include a more diverse sample to enhance the generalizability of the findings. By addressing these limitations, this research opens new opportunities for the development of scalable, cost-effective, and engaging cybersecurity awareness programs tailored to the needs of various student groups.

IV. Conclusion

This research developed a mobile learning-based cybersecurity awareness program that effectively improves cyber hygiene practices among accounting and finance students. The increase in cyber-attacks in this sector makes it urgent to carry out a cybersecurity awareness program. This program has been validated by experts and ensures that it meets the set quality standards. Understanding improvement tests showed significant improvements, indicating that students became more aware of cyber threats after implementing the program. Effectiveness tests show that the program successfully delivers cybersecurity awareness content, encourages a deeper understanding of cybersecurity concepts and practices, and brings about real changes in student behavior regarding cyber hygiene. This research makes several unique contributions to the field of cybersecurity education. First, it provides a specialized intervention for accounting and finance students, a group that is often overlooked in cybersecurity training programs despite their direct involvement in managing sensitive financial data. By focusing on this non-technical audience, the study expands the scope of cybersecurity education and demonstrates the applicability of mobile learning to diverse educational contexts. Second, the use of mobile learning as a delivery method addresses common challenges found in traditional classroom-based or module-based cybersecurity programs, such as limited engagement and low knowledge retention. The program's interactive elements—quizzes, simulations, and real-time feedback—enhance student engagement and practical understanding, aligning with cognitive learning theories that emphasize active and experiential learning. In conclusion, this research offers a strong foundation for the development of more scalable, cost-effective, and engaging cybersecurity awareness programs. The findings are especially relevant for educational institutions seeking to integrate cybersecurity awareness into their curricula, ensuring that students in various fields are better prepared to navigate the complex digital landscape. By addressing both the human and technological dimensions of cybersecurity, this study contributes to the ongoing efforts to enhance cybersecurity practices, not only in educational settings but also in broader professional environments where cybersecurity is increasingly critical. Future research should build on these findings by exploring additional variables and conducting more comprehensive assessments to further refine cybersecurity education strategies.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Herman Dwi Surjono: conceptualization, supervision; Radinal Fadli: writing—review & editing, software, Investigation; Ratna Candra Sari: supervision; Fivia Eliza: writing—original draft, resources, funding acquisition; Abdulnassir Yassin: visualization, grammar improvements, G Kulanthaivel: validation; M. Agphin Ramadhan: validation; Riky Mukhaiyar: validation; Mustofa Abi Hamid: data curation; M. Rais Ridwan: formal analysis; Sigit Purnomo: project administration, Asnimawati: Methodology. All authors had approved the final version.

References

[1] F. Eliza *et al.*, "Revolution in engineering education through android-based learning media for mobile learning: Practicality of mobile learning media to improve electrical measuring skills in the industrial Age 4.0," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 20, pp. 60–75, Nov. 2023. doi: 10.3991/IJIM.V17I20.42093

[2] A. Marwan, D. O. C. Garduno, and F. Bonfigli, "Detection of digital law issues and implication for good governance policy in Indonesia," *Bestuur*, vol. 10, no. 1, pp. 22–32, Aug. 2022. doi: 10.20961/BESTUUR.V10I1.59143

[3] V. Khattri and D. K. Singh, "Implementation of an additional factor for secure authentication in online transactions," *J. Organ. Comput. Electron. Commer.*, vol. 29, no. 4, pp. 258–273, Oct. 2019. doi: 10.1080/10919392.2019.1633123

[4] V. Zimmermann and K. Renaud, "Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset," *Int. J. Hum. Comput. Stud.*, vol. 131, pp. 169–187, Nov. 2019. doi: 10.1016/J.IJHCS.2019.05.005

[5] M. U. Shah, F. Iqbal, U. Rehman, and P. C. K. Hung, "A comparative assessment of human factors in cybersecurity: Implications for cyber governance," *IEEE Access*, vol. 11, pp. 87970–87984, 2023. doi: 10.1109/ACCESS.2023.3296580

[6] S. Walker-Roberts, M. Hammoudeh, O. Aldabbas, M. Aydin, and A. Dehghantanha, "Threats on the horizon: Understanding security threats in the era of cyber-physical systems," *J. Supercomput.*, vol. 76, no. 4, pp. 2643–2664, Apr. 2020. doi: 10.1007/S11227-019-03028-9

[7] C. S. Lee and D. Kim, "Pathways to cybersecurity awareness and protection behaviors in South Korea," *J. Comput. Inf. Syst.*, 2022. doi: 10.1080/08874417.2022.2031347

[8] C. Vanessa, P. Herrera, J. S. M. Valcarcel, M. Díaz, J. L. H. Salazar, and L. Andrade-Arenas, "Cybersecurity in health sector: A systematic review of the literature," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 31, no. 2, pp. 1099–1108, Aug. 2023. doi: 10.11591/ijeecs.v31.i2.pp1099-1108

[9] A. A. Ahmed, A. H. Elmi, A. Abdullahi, A. Y. Ahmed, and A. H. Elmi, "Cybersecurity awareness among university students in Mogadishu: A comparative study," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 32, no. 3, pp. 1580–1588, Dec. 2023. doi: 10.11591/ijeecs.v32.i3.pp1580-1588

[10] S. Kemp, D. Buil-Gil, A. Moneva, F. Miró-Llinares, and N. Díaz-Castaño, "Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19," *J. Contemp. Crim. Justice*, vol. 37, no. 4, pp. 480–501, Nov. 2021. doi: 10.1177/10439862211027986

[11] M. H. Ko, Pyo-Gil-Hong, and D. Kim, "Trends in mobile ransomware and incident response from a digital forensics perspective," *J. Inf. Commun. Converg. Eng.*, vol. 20, no. 4, pp. 280–287, 2022. doi: 10.56977/JICCE.2022.20.4.280

[12] ENISA. (July 2022). Threat landscape for ransomware attacks. *European Union Agency For Cybersecurity* [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

[13] N. Debnath and A. K. Jain, "A comprehensive survey on mobile browser security issues, challenges and solutions," *Inf. Secur. J.*, 2024. doi: 10.1080/19393555.2024.2347256

[14] N. Chakravarty and M. Dua, "Data augmentation and hybrid feature amalgamation to detect audio deep fake attacks," *Phys. Scr.*, vol. 98, no. 9, Sep. 2023. doi: 10.1088/1402-4896/ACEA05

[15] D. Kadyshevitch, "Generative AI has democratised fraud and cybercrime," *Comput. Fraud Secur.*, vol. 2024, no. 5, May 2024. doi: 10.12968/S1361-3723(24)70018-9

[16] A. Johri and S. Kumar, "Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation," *Hum. Behav. Emerg. Technol.*, vol. 2023, 2023. doi: 10.1155/2023/2103442

[17] G. Culot, F. Fattori, M. Podrecca, and M. Sartor, "Addressing Industry 4.0 cybersecurity challenges," *IEEE Eng. Manag. Rev.*, vol. 47, no. 3, pp. 79–86, Jul. 2019. doi: 10.1109/EMR.2019.2927559

[18] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. Cano, "A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)," in *Proc. 2017 Int. Conf. Inf. Syst. Comput. Sci. INCISCOS 2017*, vol. 11, 2018, pp. 253–259. doi: 10.1109/INCISCOS.2017.20

[19] I. Mustapha, Y. Vaicondam, A. Jahanzeb, B. A. Usmanovich, and S. H. B. Yusof, "Cybersecurity challenges and solutions in the fintech mobile app ecosystem," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 22, pp. 100–116, Nov. 2023. doi: 10.3991/IJIM.V17I22.45261

[20] M. Muskhir, A. Luthfi, R. Julian, and A. Fortuna, "Exploring iSpring suite for Android-based interactive instructional media in electrical lighting installation subject," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 22, pp. 67–84, Nov. 2023. doi: 10.3991/IJIM.V17I22.42625

[21] M. Hakiki, Halomoan, R. Fadli, Y. Hidayah, R. Zunarti, and V. Y. Yanti, "CT-mobile: Enhancing computational thinking via Android graphic design APP," *Int. J. Interact. Mob. Technol.*, vol. 18, no. 13, pp. 4–19, Jul. 2024. doi: 10.3991/IJIM.V18I13.47711

[22] D. T. P. Yanto *et al.*, "Evaluating the practicality of Android-based courseware in enhancing electrical circuit proficiency among vocational students," *Int. J. Interact. Mob. Technol.*, vol. 18, no. 02, pp. 27–42, Jan. 2024. doi: 10.3991/IJIM.V18I02.46341

[23] Sukardi *et al.*, "Soft skills and hard skills needed in Industry 4.0 for electrical engineering students," *J. Appl. Eng. Technol. Sci.*, vol. 5, no. 1, pp. 142–149, Dec. 2023. doi: 10.37385/JAETS.V5I1.2174

[24] A. D. Samala, N.-J. Howard, S. Criollo-C, R. D. A. Budiman, M. Hakiki, and Y. Hidayah, "What does an IMoART application look like? IMoART—An interactive mobile augmented reality application for support learning experiences in computer hardware," *Int. J. Interact. Mob. Technol.*, vol. 18, no. 13, pp. 148–165, Jul. 2024. doi: 10.3991/IJIM.V18I13.47565

[25] N. Fisk, "Developmental challenges: Capture the flag and the professionalization of cybersecurity," *Hum. Organ.*, vol. 82, no. 1, pp. 61–72, Mar. 2023. doi: 10.17730/1938-3525-82.1.61

[26] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, "Cybersecurity knowledge and skills taught in capture the flag challenges," *Comput. Secur.*, vol. 102, Mar. 2021. doi: 10.1016/j.cose.2020.102154

[27] T. D. Ashley, R. Kwon, S. N. G. Gourisetti, C. Katsis, C. A. Bonebrake, and P. A. Boyd, "Gamification of cybersecurity for workforce development in critical infrastructure," *IEEE Access*, vol. 10, pp. 112487–112501, 2022. doi: 10.1109/ACCESS.2022.3216711

[28] T. Van Steen and J. R. A. Deeleman, "Successful gamification of cybersecurity training," *Cyberpsychology, Behav. Soc. Netw.*, vol. 24, no. 9, pp. 593–598, Sep. 2021. doi: 10.1089/CYBER.2020.0526

[29] M. Coenraad, A. Pellicone, D. J. Ketelhut, M. Cukier, J. Plane, and D. Weintrop, "Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games," *Simul. Gaming*, vol. 51, no. 5, pp. 586–611, Oct. 2020. doi: 10.1177/1046878120933312

[30] S. Papadakis, *IoT, AI, and ICT for Educational Applications*, 2024. doi: 10.1007/978-3-031-50139-5

[31] R. Fadli *et al.*, "Effectiveness of mobile virtual laboratory based on project-based learning to build constructivism thinking," *Int. J. Interact. Mob. Technol.*, vol. 18, no. 6, pp. 40–55, Mar. 2024. doi: 10.3991/IJIM.V18I06.47643

[32] A. Baharum *et al.*, "Mobile learning application: Flipped classroom," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 17, no. 2, pp. 1084–1090, Feb. 2020. doi: 10.11591/ijeecs.v17.i2.pp1084-1090

[33] F. Eliza *et al.*, "Effective virtual laboratory to build constructivist thinking in electrical measurement practicum," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 34, no. 2, pp. 814–824, May 2024. doi: 10.11591/IJEECS.V34.I2.PP814-824

[34] R. Fadli, H. D. Surjono, R. C. Sari, Y. Hidayah, and F. Eliza, "Assessing cybersecurity awareness among vocational students in office administration," *Int. J. Saf. Secur. Eng.*, vol. 14, no. 4, pp. 1115–1123, Aug. 2024. doi: 10.18280/ijsse.140410

[35] F. Eliza *et al.*, "Assessing student readiness for mobile learning from a cybersecurity perspective," *Online J. Commun. Media Technol.*, vol. 14, no. 4, p. e202452, Oct. 2024. doi: 10.30935/OJCMT/15017

[36] M. Hakiki *et al.*, "Enhancing practicality of web-based mobile learning in operating system course: A developmental study," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 19, pp. 4–19, Oct. 2023. doi: 10.3991/IJIM.V17I19.42389

[37] D. Natalia, A. Johari, E. Anggereini, and I. Lestari, "Analysis of the effectiveness of the case study approach in the learning of entomology," *J. Entomol. Res.*, vol. 48, no. 1, pp. 126–129, 2024. doi: 10.5958/0974-4576.2024.00026.4

[38] F. T. Ngo, A. Agarwal, and K. Holman, "Cyber hygiene and cyber victimization among Limited English Proficiency (LEP) internet users: A mixed-method study," *Vict. Offenders*, 2024. doi: 10.1080/15564886.2024.2329765

[39] S. Baraković and J. B. Husić, "Cyber hygiene knowledge, awareness, and behavioral practices of university students," *Inf. Secur. J.*, vol. 32, no. 5, pp. 347–370, 2023. doi: 10.1080/19393555.2022.2088428

[40] E. Argyridou *et al.*, "Cyber hygiene methodology for raising cybersecurity and data privacy awareness in healthcare organisations (Preprint)," *J. Med. Internet Res.*, Jul. 2022. doi: 10.2196/41294

[41] A. S. Wilner, H. Luce, E. Ouellet, O. Williams, and N. Costa, "From public health to cyber hygiene: Cybersecurity and Canada's healthcare sector," *Int. J.*, vol. 76, no. 4, pp. 522–543, Dec. 2021. doi: 10.1177/00207020211067946

[42] A. R. Neigel, V. L. Claypoole, G. E. Waldfogle, S. Acharya, and G. M. Hancock, "Holistic cyber hygiene education: Accounting for the human factors," *Comput. Secur.*, vol. 92, May 2020. doi: 10.1016/J.COSE.2020.101731

[43] A. Vishwanath *et al.*, "Cyber hygiene: The concept, its measure, and its initial tests," *Decis. Support Syst.*, vol. 128, Jan. 2020. doi: 10.1016/J.DSS.2019.113160

[44] T. Karayel, B. Aktaş, and A. Akbıyık, "Human factors in remote work: Examining cyber hygiene practices," *Inf. Comput. Secur.*, 2024. doi: 10.1108/ICS-11-2023-0215

[45] M. A. Salem and A. E. E. Sobaih, "A quadruple 'E' approach for effective cyber-hygiene behaviour and attitude toward online learning among higher-education students in Saudi Arabia amid COVID-19 pandemic," *Electron.*, vol. 12, no. 10, May 2023. doi: 10.3390/ELECTRONICS12102268

[46] P. S. Huang, P. S. Chiu, Y. M. Huang, H. X. Zhong, and C. F. Lai, "Cooperative mobile learning for the investigation of natural science courses in elementary schools," *Sustain.*, vol. 12, no. 16, Aug. 2020. doi: 10.3390/SU12166606

[47] A. Minichiello *et al.*, "Developing a mobile application-based particle image velocimetry tool for enhanced teaching and learning in fluid mechanics: A design-based research approach," *Comput. Appl. Eng. Educ.*, vol. 29, no. 3, pp. 517–537, May 2021. doi: 10.1002/CAE.22290

[48] K. Okokpujie, C. G. Kennedy, K. Nnodu, and E. Noma-Osagha, "Cybersecurity awareness: Investigating students' susceptibility to phishing attacks for sustainable safe email usage in academic environment (A Case Study of a Nigerian leading university)," *Int. J. Sustain. Dev. Plan.*, vol. 18, no. 1, pp. 255–263, Jan. 2023. doi: 10.18280/IJSDP.180127

[49] A. A. Hnaif, A. M. Derbas, S. Almanasra, and A. Hnaif, "Cybersecurity integration in distance learning: An analysis of student awareness and attitudes," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 33, no. 2, pp. 1057–1066, Feb. 2024. doi: 10.11591/ijeecs.v33.i2.pp1057-1066

[50] M. Alsharif, S. Mishra, and M. AlShehri, "Impact of human vulnerabilities on cybersecurity," *Comput. Syst. Sci. Eng.*, vol. 40, no. 3, pp. 1153–1166, Sep. 2021. doi: 10.32604/CSSE.2022.019938

[51] S. Ramlo and J. B. Nicholas, "The human factor: Assessing individuals' perceptions related to cybersecurity," *Inf. Comput. Secur.*, vol. 29, no. 2, pp. 350–364, 2021. doi: 10.1108/ICS-04-2020-0052