Online Journal of Communication and Media Technologies, 2024, **14**(4), e202452
e-ISSN: 1986-3497

OPEN ACCESS

Research Article

Assessing student readiness for mobile learning from a cybersecurity perspective

Fivia Eliza [1]
0000-0001-9942-5348

Radinal Fadli [2*]
0000-0003-0933-4894

M. Agphin Ramadhan [3]
0000-0002-0034-9793

Valiant Lukad Perdana Sutrisno [4]
0009-0000-2087-669X

Yayuk Hidayah [5]
0000-0002-8551-1998

Muhammad Hakiki [2]
0000-0001-7459-7952

Deden Dicky Dermawan [6]
0009-0009-7697-0779

[1] Faculty of Engineering, Universitas Negeri Padang, Padang, INDONESIA
[2] Universitas Muhammadiyah Muara Bungo, Jambi, INDONESIA
[3] Universitas Negeri Jakarta, INDONESIA
[4] Universitas Sebelas Maret, Surakarta, INDONESIA
[5] Universitas Negeri Yogyakarta, Yogyakarta, INDONESIA
[6] Universitas Islam 45 Bekasi, Jawa Barat, INDONESIA
[*] Corresponding author: fadliradinal@gmail.com

Citation: Eliza, F., Fadli, R., Ramadhan, M. A., Sutrisno, V. L. P., Hidayah, Y., Hakiki, M., & Dermawan, D. D. (2024). Assessing student readiness for mobile learning from a cybersecurity perspective. *Online Journal of Communication and Media Technologies, 14*(4), e202452. https://doi.org/10.30935/ojcmt/15017

ARTICLE INFO

Received: 27 Jun 2024
Accepted: 27 Jul 2024

ABSTRACT

This research aims to measure student readiness in implementing mobile learning from a cybersecurity perspective. Using a quantitative method with a survey approach, the participants in this research were 150 students of the electrical engineering study program at Padang State University in Indonesia, who were randomly stratified to ensure a balanced representation of the academic year. The research is an online objective test related to cybersecurity topics. The data analysis technique used is quantitative descriptive. The analysis results show that system updates are the only indicator with a "good" awareness level, while other indicators are at the "sufficient" and "poor" levels, indicating the need for further improvement. These findings underscore the importance of integrating cyber security education in mobile learning curricula to increase student readiness to face evolving cyber threats. Thus, this research recommends developing specific training programs and adding comprehensive cybersecurity material to the curriculum to equip students with the skills necessary to maintain cybersecurity effectively.

Keywords: mobile learning, readiness, cybersecurity awareness, digital safety, educational technology

INTRODUCTION

In recent years, the world of education has experienced a significant shift towards mobile learning (m-learning), driven by rapid technological advances and the increasing accessibility of mobile devices. M-learning offers unparalleled flexibility, allowing students to access educational content anytime and anywhere, encouraging continuous learning outside the traditional classroom environment (Fadli et al., 2024). The adoption of m-learning has been accelerated by the need for distance education solutions, especially highlighted during global events such as the COVID-19 pandemic. During the pandemic, many educational institutions were forced to switch to distance learning to continue the educational process. In this context, m-learning is a very practical solution.

Various m-learning applications have been developed in recent years to meet these needs. Various platforms are also used to create m-learning (Eliza et al., 2024). These applications cover many functions, from learning management systems (LMS) to specialized applications for learning languages, mathematics, and science. These applications provide easy access to learning materials and offer interactive features that make the learning process more exciting and effective (Eliza et al., 2023). For example, quiz features and educational games can increase student engagement, while online discussion and collaboration functions enable interaction between students and teachers even in different locations. In addition, developments in augmented reality (AR) and virtual reality (VR) technology are also starting to be integrated into m-learning applications, providing a more immersive and contextual learning experience.

However, although m-learning offers many benefits, the use of this technology also brings its own challenges, especially related to cybersecurity. The use of mobile devices to access information and educational platforms opens up potential risks to cyberattacks, such as malware, phishing, and data breaches (Hnaif et al., 2024). These attacks can not only result in the loss of personal data and sensitive information but can also disrupt the learning process, damage devices, and result in financial losses (González-Granadillo et al., 2021). Malware can infect mobile devices through unsafe downloads or suspicious links (Wang et al., 2020). Another attack is phishing, which aims to obtain sensitive information such as usernames, passwords, and credit card details (van Steen et al., 2020). Students and teachers who are not alert can quickly become victims of attacks.

Several studies have shown the importance of cyber security awareness in protecting individuals from various cyber threats. Research conducted by Mc Mahon (2020) found that most information security incidents were caused by users' negligence in complying with security policies or due to a lack of awareness of cyber threats. This study shows that although security technology has developed rapidly, the biggest weakness still lies in the human factor. Furthermore, research by Alahmari et al. (2023) highlights that cyber-attacks on an organization sometimes start from employees with a low level of cybersecurity awareness, which becomes the entry point for cyber-attacks, thus having an impact on the organization's system as a whole. This research concludes that information security incidents occur more frequently in organizations whose employees are not adequately trained in cybersecurity practices.

Previous research has investigated the level of cybersecurity awareness among secondary school students (Maon et al., 2021; Sari et al., 2020). The research findings provide valuable insight into students' understanding of security threats in educational contexts. Furthermore, research conducted by Huraj et al. (2023) measured the level of cybersecurity awareness between computer science students and media science students. The research findings showed significant differences in cybersecurity awareness between the two groups of students, highlighting the importance of approaches appropriate to the disciplinary context. On the other hand, research conducted by Alharbi and Tassaddiq (2021) focused on measuring cybersecurity awareness among graduate and undergraduate students. The research findings provide a deeper understanding of the differences in levels of cybersecurity awareness between the two groups of students, which may be influenced by their level of education and experience. However, there are shortcomings in previous research, where there has been no research that specifically measures students' readiness to carry out m-learning by considering aspects of cybersecurity awareness holistically. Therefore, the research conducted by this researcher aims to fill this knowledge gap by exploring students' readiness for m-learning from a cybersecurity perspective in a comprehensive manner, with the hope of providing new insights and relevant solutions in the current digital education context.

Thus, this research aims to measure student readiness in m-learning from a cybersecurity perspective. It is hoped that this research can provide an in-depth understanding of how students' level of cybersecurity awareness can influence their readiness to face the challenges and risks associated with the use of mobile technology in an educational context.

The Objective of the Research

This research aims to achieve the following objectives:

1. The first objective of this research is to measure the level of cybersecurity awareness among students.
2. The second objective of this research is to identify cybersecurity awareness topics that need to be increased among students.

Importance of This Study

The importance of this research is determined by the following aspects:

1. Student awareness of the cybersecurity threats they face in m-learning. By understanding their current level of awareness and identifying areas that need improvement, this research can help in developing more effective educational strategies to increase their readiness to face cybersecurity risks.
2. This research will provide valuable insights for educational institutions in designing curricula and training programs that are more relevant to today's cybersecurity challenges. By knowing which cybersecurity awareness topics need to be improved, educators can integrate appropriate material into their learning, while administrators can develop specific training programs to increase students' understanding and skills in cybersecurity.

LITERATURE REVIEW

Mobile Learning

M-learning has become a form of innovation in education that offers flexibility and accessibility that traditional learning methods do not. M-learning allows students to access learning materials via mobile devices such as smartphones and tablets anytime and anywhere, thus supporting lifelong learning (Salhab & Daher, 2023). The main benefits of m-learning include increased student engagement, personalized learning, and the ability to support a variety of learning styles (Nazar et al., 2022). Additionally, m-learning enables more dynamic interactions between students and learning materials through the use of interactive applications and digital tools.

M-learning gives students the freedom to learn at their own pace and time, which can increase motivation and learning outcomes. With m-learning, students can access various learning resources such as e-books, learning videos, interactive quizzes, and online discussion forums, all of which can be accessed via their mobile devices (Hakiki et al., 2023). This not only makes the learning process more flexible but also more interesting and interactive. M-learning also supports various learning styles, be it visual, auditory, kinesthetic, or a combination of the three. Learning materials delivered through a variety of formats—text, audio, video, and digital interactions—allow students to choose the method that best suits their learning style (Li, 2020). For example, students who learn visually may prefer videos and infographics, while auditory students may prefer listening to podcasts or recorded lectures.

Thus, m-learning not only expands access to education but also improves the quality and effectiveness of learning. However, implementing m-learning requires adequate technological infrastructure and awareness of the importance of cybersecurity, especially considering that mobile devices are often the target of cyber-attacks. Therefore, students' readiness to utilize m-learning must be supported by adequate cybersecurity knowledge and practices to ensure that they can learn safely and effectively.

Cybersecurity Awareness

Cybersecurity awareness refers to an individual's understanding and attitude toward potential threats, as well as best practices for protecting data and online privacy (Zwilling et al., 2022). In the educational context, cybersecurity awareness is very important, considering the increasing use of digital technology and the

internet in the learning process. Cybersecurity threats such as phishing, malware, and identity theft can disrupt the learning process and endanger students' personal information (Garba et al., 2021).

Research by Mai and Tick (2021) shows that secondary school students have varying awareness of cybersecurity threats, with many students unaware of the risks they face when using the internet for academic purposes. This is supported by the findings of research conducted by Okokpujie et al. (2023), which examined students' responses to phishing emails sent. The results showed that 70.6% of students surveyed were vulnerable to this attack due to unawareness. These findings indicate an urgent need to improve cybersecurity education and training among secondary school students. Low awareness of cyber threats can leave students vulnerable to various forms of attacks, which not only threaten the security of their personal data but can also disrupt their learning process.

In educational settings, high cybersecurity awareness is essential due to the large amount of sensitive information that is handled every day (Amankwa, 2021). Students, teachers, and school staff often access and store personal and academic data on digital platforms. Without adequate awareness and knowledge of cybersecurity, this data is at risk of attacks and security breaches. Therefore, increasing cybersecurity awareness not only protects individuals but also maintains the integrity of the education system as a whole.

Student Readiness for Mobile Learning

Students' readiness for m-learning is determined by various factors, including technical skills, access to mobile devices, motivation, and support from their learning environment (Van et al., 2021). Measuring student readiness is usually carried out through surveys that assess these factors and student perceptions of the effectiveness of m-learning. A summary of previous research (Abuhassna et al., 2022) has shown that technical readiness and access to technology are important factors influencing the success of m-learning implementation. Kampa (2023) also reveals that optimism, innovation, and technological readiness are factors that encourage the use of m-learning. However, little research has explored how cybersecurity awareness influences students' readiness for m-learning.

Cyber security awareness is a crucial aspect in the context of m-learning because mobile devices are often more vulnerable to cyber threats compared to traditional desktop systems. Especially spyware attacks (Naser et al., 2023), revealing that attacks targeting mobile devices are increasing, with more than 26,000 attacks every day. This can, of course, have an impact on Students who are less aware of cybersecurity risks and can become easy targets for attacks such as phishing, malware, and data theft, which can disrupt the learning process and cause significant losses (Ahamed et al., 2024). Therefore, integrating cybersecurity training in preparation for m-learning is becoming increasingly important. Proper awareness of cybersecurity not only protects students but also ensures that they can utilize mobile technology safely and effectively in learning their environment.

Cybersecurity Awareness and Mobile Learning Readiness

Some Awareness of cybersecurity plays a crucial role in determining students' readiness for m-learning. In an era where mobile technology is becoming increasingly dominant in learning environments, a strong understanding of cybersecurity threats is a must. Students who are aware of cybersecurity risks and practices will be better able to safeguard themselves and their data when using mobile devices for learning (Taha & Dahabiyeh, 2021). This awareness includes recognition of attacks such as phishing, malware, and data theft, as well as preventative steps you can take to protect yourself.

Previous studies have shown that students who are less aware of cybersecurity are more likely to be targets of cyber-attacks, which can disrupt the learning process and threaten their privacy and information security (Garba et al., 2022). Therefore, students who have a good understanding of cybersecurity will be better prepared to use mobile technology in their learning, while those who are less aware of security risks tend to be more vulnerable to attacks and intrusions.

Thus, increasing cybersecurity awareness among students is a must in efforts to increase their readiness for m-learning. Integrating training and education on cybersecurity into m-learning curricula can help students develop a better understanding of security risks and the preventative steps they can take. This will

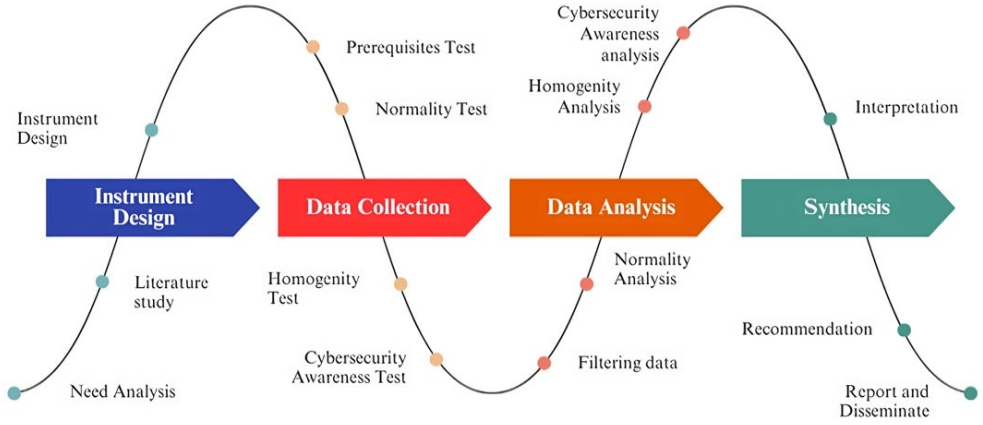

Figure 1. Research procedure (Source: Authors)

not only protect students from cyber threats but also increase the overall effectiveness and success of m-learning.

METHOD

This research uses quantitative methods with a survey approach to measure student readiness in m-learning from a cybersecurity perspective. The survey method was chosen because it allows for broad and representative data collection from a diverse student population. allowing for comprehensive analysis of m-learning readiness across different academic levels. The research procedure to be carried out can be seen in **Figure 1**.

This research procedure was carried out through several main, interrelated stages to ensure the suitability of the method and the validity of the results obtained. The procedure consists of instrument design, data collection, data analysis, and synthesis.

Instrument Design

The first stage is instrument design, which starts with a need analysis. At this stage, research needs are identified to ensure that the developed instruments are in accordance with the research objectives. Furthermore, a literature study is carried out to collect relevant information and theories as the basis for the development of the instrument. After that, the design of the instrument was carried out to compile objective tests that would be used in data collection.

Data Collection

Once the instrument is ready, the next stage is data collection. At this stage, data from research participants is collected for 30 days through a pre-designed cybersecurity awareness test. At the end of each week participants will be reminded to take the test to ensure all participants take the test. Before data collection, a prerequisite test is carried out to ensure that the data collected meets the requirements. Namely, it is valid, has a moderate level of difficulty, has sufficient differentiation, and is reliable. Furthermore, a normality test was also carried out to ensure that the distribution of data was expected. In addition, the Homogeneity Test is applied to ensure that the variance between groups is uniform.

Data Analysis

The third stage is data analysis, where the data that has been collected is analyzed using various statistical techniques. This process starts with data filtering to eliminate invalid, incomplete, and duplicate data. Next, a normality analysis and a homogeneity analysis are carried out to ensure that the data is ready for further analysis. Furthermore, a cybersecurity awareness analysis was conducted to identify the participants' awareness of cybersecurity.

Table 1. Cybersecurity assessment topics

No	Indicator	Item numbers
1	Cybersecurity basics	1, 2, 3, 4
2	Password management	5, 6, 7, 8
3	Device and data protection	9, 10, 11, 12
4	Phishing	13, 14, 15, 16
5	Network security	17, 18, 19, 20
6	System update	21, 22, 23, 24
7	Privacy and protection of personal data	25, 26, 27, 28
8	Online ethics and behavior	29, 30, 31, 32
9	Security incident response	33, 34, 35, 36
10	Regulations and policies	37, 38, 39, 40

Table 2. Product moment correlation criteria

No	R_{xy}	Category
1	$0.80 \leq R_{xy} \leq 1.00$	Very high
2	$0.60 \leq R_{xy} < 0.80$	Tall
3	$0.40 \leq R_{xy} < 0.60$	Enough
4	$0.20 \leq R_{xy} < 0.40$	Low
5	$0.00 \leq R_{xy} < 0.20$	Very low

Synthesis

The final stage is synthesis, where the results of the analysis are interpreted to draw meaningful conclusions. This process involves data interpretation to understand the implications of research results. Based on the results of the interpretation, recommendations were prepared to increase cybersecurity awareness among students. Finally, the research results are reported and disseminated (report and disseminate) through the publication of scientific articles.

Population and Sample

Participants in this research were students from several levels in the Electrical Engineering, Electrical Engineering Education, and Electrical Engineering specialty programs at Padang State University in Indonesia. The sample was drawn stratified randomly to ensure a balanced representation of the academic year. There were 150 students in total.

Instrument

The instrument used in this research is an online objective test, which focuses on ten important topics in understanding cybersecurity concepts and practices. **Table 1** shows these topics.

These test indicators are based on topics that have been identified in several previous studies (Alharbi & Tassaddiq, 2021; Alsobeh et al., 2023; Hnaif et al., 2024; Hodhod et al., 2023; Huraj et al., 2023; Johri & Kumar, 2023; Moallem, 2019; Taha & Dahabiyeh, 2021; Taylor & Whitty, 2023) as critical areas that students must understand to increase cybersecurity awareness and security.

Data Analysis

Test prerequisites test

The tests given to students pass item validity tests, reliability tests, level of difficulty tests, and difficulty index tests, to ensure that each question in the test measures the concept in question accurately. The formula used is the product moment correlation below, with categories which can be seen in **Table 2**.

$$R_{xy} = \sum S(X - \bar{X})(Y - \bar{Y}) \sqrt{\sum (X - \bar{X})^2 \sum (Y - \bar{Y})^2} \quad (1)$$

where R_{xy} is item-total correlation, X is item score, $\bar{X}$ is average item score, Y is total test score without the item, $\bar{Y}$ is average total test score without the item.

Table 3. Cronbach's alpha criteria

No	α	Category
1	0,00 ≤ α < 0,50	Low
2	0,50 ≤ α < 070	Medium
3	0,70 ≤ α < 0,90	Enough
4	0,90 ≤ α ≤ 1,00	Very high

Table 4. Difficulty index criteria

No	Di	Category
1	0.00 ≤ Di < 0.30	Difficult
2	0.30 ≤ Di < 0.80	Moderate
3	0.80 ≤ Di < 1.00	Easy

Table 5. Discrimination index

No	$rpbi$	Category
1	Negative	Poor
2	0.00 ≤ $rpbi$ < 0.20	Weak
3	0.20 ≤ $rpbi$ < 0.40	Enough
4	0.40 ≤ $rpbi$ < 0.70	Good
5	0.70 ≤ $rpbi$ < 1.00	Very well

Reliability testing is carried out to assess the test's internal consistency so that the results are reliable and consistent. The formula used is Cronbach's alpha, as follows, with categories, which can be seen in **Table 3**.

$$\alpha = \frac{N}{N-1}\left(1 - \frac{\sum S_x^2}{S_t^2}\right) \tag{2}$$

where α is Cronbach's alpha coefficient, N is number of respondents, S_x^2 is item score variance, S_t^2 is total variance of test scores.

Test the level of difficulty to ensure that the test questions given have a moderate level of difficulty so that they are not too difficult and not too easy. The formula used is as follows, with categories which can be seen in **Table 4**.

$$Difficulty\ index\ (Di) = \frac{Number\ of\ Correct\ answers}{Number\ of\ Respondents} \tag{3}$$

Next, the discrimination index test is carried out to ensure that there are differences between the test questions so that each question item makes a significant contribution to the evaluation of student performance. The formula used is as follows, with categories which can be seen in **Table 5**.

$$rpbi = \frac{N_1 - N_2}{\sqrt{N_1 N_2 (N-1)(N-1-D)}} \tag{4}$$

where $Rpbi$ is discrimination index, N_1 is number of respondents who answered correctly, N_2 is number of respondents who answered incorrectly, N is total respondents, D is number of people who answered correctly minus the number of people who answered wrong.

The test items given to students are those that meet the level of validity and reliability in the "sufficient" category, with a level of difficulty in the "moderate" category, and with different strengths in the "sufficient" category. By meeting these standards, the test can provide an accurate and informative picture of students' cybersecurity readiness and level of awareness in the context of m-learning.

Normality and homogeneity test

Before proceeding with further statistical analysis, it is important to check whether the data collected is normally distributed or not. In this study, we used the Kolmogorov-Smirnov normality test, to evaluate whether data on student readiness in m-learning and cybersecurity awareness were normally distributed. The formula used is as follows.

$$D = \max|F_n(X) - F_0(X) \tag{5}$$

where $F_n(X)$ is empirical value of the cumulative distribution function (CDF) of the sample and $F_0(X)$ is theoretical value of the CDF of the normal distribution.

Table 6. Criteria level of cybersecurity awareness

Level	Score	Advice
Good	80–100	Need to maintain
Sufficient	60–79	Need improvement
Poor	< 60	Need treatment

In addition to the normality of the data, we will also evaluate the homogeneity of variance of the compared data groups. Homogeneity of variance shows whether the variability or spread of data between groups of data is uniform or not. In this study, we will use Levene's test. The formula used is as follows.

$$W = \frac{(N-k)}{(k-1)} \frac{\sum_{i=1}^{k} n_i (Z_i - Z)^2}{\left[\sum_{i=1}^{k} n_i \ln(S_i) - (S_T)\right]} \quad (6)$$

where N is total observations, k is number of groups, n_i is number of observations in the i-th group, Z_i is average value of the i-th group, and Z is average value of all data.

Cybersecurity awareness level test

The primary analysis is carried out by comparing the average value of the test results for each indicator of cybersecurity awareness. This process involves calculating the average value for each indicator in the test, which is then compared with the standard level of cybersecurity awareness listed in **Table 6**.

RESULT

Test Prerequisites Test

Prerequisite tests consist of test item validity tests, reliability tests, tests of differentiability, tests of difficulty level of questions, and tests of differentiability. The prerequisite test results are shown in **Table 7**.

The results of the validity analysis, the differentiating power of the questions, and the level of difficulty of the 40 test items show that all items meet the predetermined criteria. Validity scores range from 0.50 to 0.90, indicating that the items have a relatively high level of validity. The differentiating power of the questions is in the range of 0.45 to 0.80, suggesting that these items can differentiate well between students who have a good and poor understanding of the material being tested. The item difficulty level ranges from 0.35 to 0.80, which means the items are in the moderate category and can be answered well by the majority of students. Based on these results, all test items were marked "can be used," indicating that these items are suitable for use in testing students' readiness for m-learning from a cybersecurity perspective. Apart from that, the reliability test results show a score of 0.83, which means this test instrument has a high level of reliability and is consistent in measurement.

Normality and Homogeneity Test

The next test carried out is a normality and homogeneity test to ensure that the data is usually distributed, and that the population used is homogeneous. The test results are presented in **Table 8**.

Cybersecurity Awareness Level Test Results

The results of a cybersecurity awareness test conducted on 150 students of the electrical engineering study program at Padang State University showed various levels of understanding in ten main indicators. The average results of indicators were obtained, which became assessment, which is summarized in **Figure 2**.

Overall, there are several areas that require urgent attention. On the basics of cybersecurity indicator, students obtained an average score of 56.7, which is classified as "poor," indicating an urgent need for significant improvement in this basic understanding. The same thing can be seen in the device and data protection indicator, with an average value of 53.4, as well as response to security incidents (42.7) and regulations and policies (44.3), all of which are at the "poor" level and require immediate intervention. Meanwhile, indicators for password management (77.3), phishing (65.8), network security (72.1), and privacy and personal data protection (68.3) are at the "sufficient" level. Although these indicators demonstrate a sufficient level of awareness, they still require further improvement to reach higher standards. On the other hand, students showed satisfactory results in the system update indicator with an average score of 80.7,

Table 7. Criteria level of cybersecurity awareness

No	Validity	Discrimination	Difficulty	Decision
1	0.719	0.576	0.493	Can be used
2	0.786	0.603	0.536	Can be used
3	0.741	0.694	0.379	Can be used
4	0.718	0.471	0.662	Can be used
5	0.669	0.683	0.605	Can be used
6	0.758	0.685	0.469	Can be used
7	0.675	0.524	0.585	Can be used
8	0.857	0.495	0.392	Can be used
9	0.885	0.560	0.609	Can be used
10	0.653	0.577	0.768	Can be used
11	0.817	0.650	0.493	Can be used
12	0.712	0.604	0.650	Can be used
13	0.727	0.796	0.409	Can be used
14	0.870	0.486	0.672	Can be used
15	0.528	0.523	0.480	Can be used
16	0.535	0.506	0.432	Can be used
17	0.508	0.679	0.614	Can be used
18	0.833	0.539	0.359	Can be used
19	0.811	0.613	0.723	Can be used
20	0.848	0.536	0.352	Can be used
21	0.891	0.506	0.655	Can be used
22	0.820	0.489	0.472	Can be used
23	0.685	0.680	0.681	Can be used
24	0.812	0.498	0.783	Can be used
25	0.547	0.519	0.462	Can be used
26	0.756	0.579	0.609	Can be used
27	0.557	0.737	0.616	Can be used
28	0.878	0.484	0.608	Can be used
29	0.709	0.743	0.450	Can be used
30	0.666	0.484	0.779	Can be used
31	0.606	0.792	0.551	Can be used
32	0.810	0.614	0.731	Can be used
33	0.682	0.792	0.665	Can be used
34	0.727	0.662	0.484	Can be used
35	0.508	0.709	0.716	Can be used
36	0.747	0.464	0.528	Can be used
37	0.745	0.549	0.746	Can be used
38	0.747	0.492	0.612	Can be used
39	0.877	0.554	0.747	Can be used
40	0.773	0.492	0.662	Can be used
Reliability test score			0.830	Reliable

Table 8. Normality and homogeneity test results

Test	Statistic	Sign.	Score	Conclusion
Normality	Kolmogorov-Smirnov (D)	α = 0.05	0.128	D > α normal distribution
Homogeneity	Levene's test (F)	α = 0.05	0.076	F > α homogenous

which is at the “good” level, indicating that their understanding of the importance of updating the system is good enough and needs to be maintained. However, the online ethics and behavior indicator recorded an average score of 58.5, also at the “poor” level, indicating that there is an urgent need to increase awareness and understanding of ethics in cyberspace. These results confirm that although there are several areas in which students have demonstrated a good understanding, there are still many important aspects of cybersecurity that require continuous improvement. Therefore, additional educational and training measures are urgently needed to increase students’ overall awareness and readiness to face cybersecurity challenges in the m-learning era.

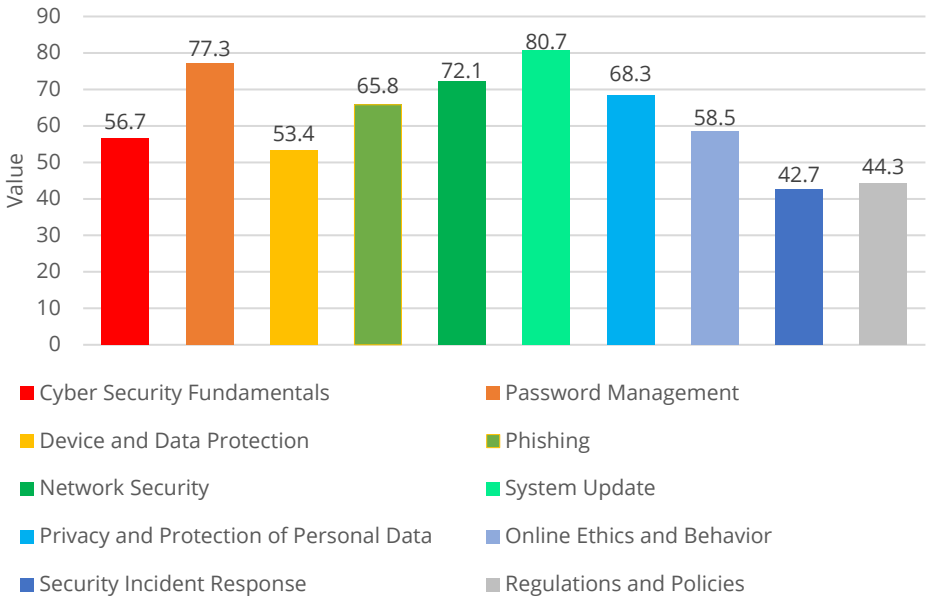

Figure 2. Cybersecurity awareness level test results (Source: Authors)

DISCUSSION

The results of this study show that the level of cybersecurity awareness among students varies among the ten indicators measured. Fundamental cybersecurity indicators, device and data protection, security incident response, and regulations and policies show low average scores at the "poor" level. This indicates that many students still have a limited understanding of basic cybersecurity concepts and data protection measures, as well as handling security incidents and applicable regulations, so this can be an obstacle in implementing m-learning. This finding is in line with previous research by Nagahawatta et al. (2020), which found that students who do not have a basic understanding of cybersecurity make them vulnerable to cyber threats. This is in line with the findings of research conducted by Bognár and Bottyán (2024), which revealed that with awareness and good cyber hygiene habits, students can protect their personal information and academic data from cyber threats. So, this condition further strengthens the need for students to increase in-depth cybersecurity awareness before implementing m-learning.

On the other hand, several indicators such as password management, phishing, network security, and privacy and personal data protection are at the fair level. Although at a better level, these results still indicate the need for further improvement. Especially when it comes to phishing and privacy, where cyber threats continue to evolve, and students need to be equipped with more in-depth and up-to-date knowledge. As research conducted by Riggs et al. (2023) summarizes cyber-attacks in the last 20 years, the findings reveal that cyber-attacks are increasingly developing and becoming more sophisticated, where hackers no longer only target large infrastructure but also target individuals. These findings are supported by research findings conducted (Alotibi, 2024), which show that cyber-attacks are increasingly difficult to recognize and increasingly target users with sophisticated social engineering techniques utilizing artificial intelligence. So, improvements in this area need to be made through special training programs and the integration of cybersecurity material into the existing curriculum. This is especially important in the context of m-learning, where students often use personal devices and social media, which inadvertently exposes private data.

The system update indicator is at a good level. This shows that students understand the importance of keeping their systems up to date as a precaution against cyber threats. This awareness is critical, especially in the context of m-learning, where outdated software can be an entry point for various types of cyberattacks. Research by Okokpujie et al. (2023) confirms that regular system updates are one of the best practices for keeping devices safe from exploitation of newly discovered vulnerabilities. These findings are supported by Zhao et al. (2024), who stated that system updates were carried out to adapt to improved security policies.

This heightened awareness must be maintained. Given that m-learning relies on frequent use of devices outside secure institutional networks, it is important for students not only to update their devices but also to strengthen their understanding of cybersecurity.

Overall, these findings confirm that although there are some areas in which students have adequate understanding, many important aspects of cybersecurity still require greater attention. The recommendation resulting from this research is the need for a more holistic and integrated approach to cybersecurity education. This includes improving learning materials, providing additional educational resources, and ongoing practical training. Thus, by studying comprehensive cybersecurity in the context of m-learning, students can be better prepared to face evolving cyber threats. This will not only help protect them during their studies but also equip them with the skills necessary to maintain cybersecurity in their future professional careers. Several previous studies also support the importance of increasing cybersecurity awareness among students. According to Hobbs (2023), deeper education about cyber threats and best practices is very important in forming a proactive attitude towards digital security among students and academics. Furthermore, research by Eltahir and Ahmed (2023) highlights that effective cybersecurity education can increase students' awareness and ability to recognize and respond to cyber threats. In addition, Ortiz-Garcés et al. (2024) show that the integration of cybersecurity material in higher education curricula has a positive impact on equipping students with the knowledge and skills needed to face digital security challenges. So, the findings of this research open up opportunities to develop comprehensive cybersecurity awareness programs that are integrated with m-learning curricula.

CONCLUSION

So, this research has measured students' readiness for m-learning from the perspective of cybersecurity awareness using quantitative methods and survey approaches. Through the development and application of online objective tests, this study succeeded in identifying the level of cybersecurity awareness among students of the Electrical Engineering, Electrical Engineering Education, and Electrical Engineering Expertise study programs at Padang State University.

Through normality and homogeneity tests, it is ensured that the data collected comes from homogeneous samples and that the data analyzed is normally distributed data. So that the data can be used to present the population in general. From the results of the data analysis, it was found that most students have a level of cybersecurity awareness that is in the "adequate" category, with an average score between 60-79. However, there are also a number of students who fall into the "less" category with a score below 60, indicating a need for increased knowledge and awareness in this field. The results of the validity and reliability test show that the instruments used in this study have good internal consistency and are reliable for measuring cybersecurity awareness.

The findings of this study not only provide insight into the level of cybersecurity awareness among students but also offer practical recommendations that educational institutions can implement to improve the readiness and security of m-learning. Thus, this research contributes to the existing literature by providing empirical data and implementation suggestions for the development of cybersecurity policies in the context of higher education.

Implication

This research has important implications for educational policies and teaching practices in the field of electrical engineering and electrical engineering education. By identifying the level of cybersecurity awareness among students, educational institutions can design and implement more targeted training programs to improve cybersecurity literacy. In addition, the results of this research can be the basis for the development of a more comprehensive curriculum that covers aspects of cybersecurity so that students are better prepared to face security challenges in an increasingly complex digital world.

Recommendations

Based on the findings of this study, it is recommended that a special training program and curriculum be developed that focuses on increasing cybersecurity awareness. The program should cover critical topics such

as cyber threat identification, the use of security software, and best practices in maintaining privacy and personal data. The implementation of this training program is expected to increase students' readiness to face cybersecurity challenges in the era of m-learning.

Research Limitations

While this study provides valuable insights, there are some limitations that need to be noted. First, this study only involved students from one university, so the results may not be generalized to students at other universities. Second, the survey method used may have respondent bias, where students who are more interested or more aware of cybersecurity may be more likely to participate. Third, this study relies on online objective tests that may not fully reflect students' understanding and practical skills in cybersecurity. For future research, it is recommended to expand the sample to different universities and use more diverse evaluation methods, including practical skills assessments.

Author contributions: FE: conceptualization, resources, methodology, administration, funding; **RF:** writing draft, data collection, data analysis, data curation; **MAR:** validation, review, supervision; **VLPS:** revision, editing; **YH:** validation, supervision; **MH:** investigation, data curation; **DDD:** visualization. All authors approved the final version of the article.

Acknowledgements: The authors would like to thank the Higher Education Funding Agency (BPPT) and the Education Fund Management Institute (LPDP) and the Indonesian Education Scholarship (BPI).

Funding: The authors received no financial support for the research and/or authorship of this article.

Ethics declaration: The authors declared that the study did not require ethics committee approval or other documentation. The authors further declared that they adhered to the highest ethical standards in academic publishing and written informed consents were obtained from the participants.

Declaration of interest: The authors declare no competing interest.

Data availability: Data generated or analyzed during this study are available from the authors on request.

REFERENCES

Abuhassna, H., Awae, F., Bayoumi, K., Alzitawi, D. U., Alsharif, A. H., & Yahaya, N. (2022). Understanding online learning readiness among university students: A bibliometric analysis. *International Journal of Interactive Mobile Technologies, 16*(13), 81–94. https://doi.org/10.3991/IJIM.V16I13.30605

Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Fahad, A. Al, Chowdhury, S., & Rani Dey, M. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: The role of cybersecurity attitude in the 4.0 Industrial Revolution era. *SAGE Open, 14*(1). https://doi.org/10.1177/21582440241228920

Alahmari, S., Renaud, K., & Omoronyia, I. (2023). We are moving beyond cybersecurity awareness and training to engendering security knowledge sharing. *Information Systems and e-Business Management, 21*(1), 123–158. https://doi.org/10.1007/s10257-022-00575-2

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing, 5*(2), Article 23. https://doi.org/10.3390/bdcc5020023

Alotibi, G. (2024). A cybersecurity awareness model for the protection of Saudi students from social media attacks. *Engineering, Technology and Applied Science Research, 14*(2), 13787–13795. https://doi.org/10.48084/ETASR.7123

Alsobeh, A. M. R., Alazzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technologies, 13*(2), Article e202312. https://doi.org/10.30935/ojcmt/12942

Amankwa, E. (2021). Relevance of cybersecurity education at pedagogy levels in schools. *Journal of Information Security, 12*(4), 233–249. https://doi.org/10.4236/jis.2021.124013

Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences, 14*(6), Article 588. https://doi.org/10.3390/EDUCSCI14060588

Eliza, F., Candra, O., Tri, D., Yanto, P., Fadli, R., Myori, D. E., Islami, S., Hidayah, Y., & Balti, L. (2024). Effective virtual laboratory to build constructivist thinking in electrical measurement practicum. *Indonesian Journal of Electrical Engineering and Computer Science, 34*(2), 814–824. https://doi.org/10.11591/IJEECS.V34.I2.PP814-824

Eliza, F., Fadli, R., Hakiki, M., Trisnawati, W., Abdulah, Putra, Y. I., Fauziah, Marind, G., & Hidayah, Y. (2023). 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. *International Journal of Interactive Mobile Technologies, 17*(20), 60–75. https://doi.org/10.3991/IJIM.V17I20.42093

Eltahir, M. E., & Ahmed, O. S. (2023). Cybersecurity awareness in African higher education institutions: A case study of Sudan. *Information Sciences Letters, 12*(1), 171–183. https://doi.org/10.18576/ISL/120113

Fadli, R., Surjono, H. D., Sari, R. C., Eliza, F., Hakiki, M., Hidayah, Y., Triyono, M. B., & Samala, A. D. (2024). Effectiveness of mobile virtual laboratory based on project-based learning to build constructivism thinking. *International Journal of Interactive Mobile Technologies, 18*(06), 40–55. https://doi.org/10.3991/IJIM.V18I06.47643

Garba, A. A., Siraj, M. M., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. *International Journal of Electrical and Computer Engineering, 12*(1), 572–584. https://doi.org/10.11591/IJECE.V12I1.PP572-584

Garba, A. A., Siraj, M. M., Othman, S. H., & Zogaan, W. A. (2021). Cybersecurity awareness of university students in Nigeria: Analysis approach. *Turkish Journal of Computer and Mathematics Education, 12*(12), 3739–3752. https://doi.org/10.11591/ijece.v12i1.pp572-584

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors, 21*(14). https://doi.org/10.3390/S21144759

Hakiki, M., Surjono, H. D., Wagiran, Fadli, R., Budiman, R. D. A., Ramadhani, W., Habibie, Z. R., Suhardiman, S., & Hidayah, Y. (2023). Enhancing practicality of web-based mobile learning in operating system course: A developmental study. *International Journal of Interactive Mobile Technologies, 17*(19), 4–19. https://doi.org/10.3991/IJIM.V17I19.42389

Hnaif, A. A., Derbas, A. M., Almanasra, S., & Hnaif, A. (2024). Cybersecurity integration in distance learning: An analysis of student awareness and attitudes. *Indonesian Journal of Electrical Engineering and Computer Science, 33*(2), 1057–1066. https://doi.org/10.11591/ijeecs.v33.i2.pp1057-1066

Hobbs, J. (2023). Cybersecurity awareness in higher education: A comparative analysis of faculty and staff. *Issues in Information Systems, 24*(1), 159–169. https://doi.org/10.48009/1_IIS_2023_114

Hodhod, R., Hardage, H., Abbas, S., & Aldakheel, E. A. (2023). CyberHero: An adaptive serious game to promote cybersecurity awareness. *Electronics*, *12*(17), Article 3544. https://doi.org/10.3390/ELECTRONICS12173544

Huraj, L., Lengyelfalusy, T., Hurajová, A., & Lajčin, D. (2023). Measuring cybersecurity awareness: A comparison between computer science and media science students. *TEM Journal, 12*(2), 623–633. https://doi.org/10.18421/TEM122-05

Johri, A., & Kumar, S. (2023). Exploring customer awareness towards their cybersecurity in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation. *Human Behavior and Emerging Technologies*, *2023*. https://doi.org/10.1155/2023/2103442

Kampa, R. K. (2023). Combining technology readiness and acceptance model for investigating the acceptance of m-learning in higher education in India. *Asian Association of Open Universities Journal, 18*(2), 105–120. https://doi.org/10.1108/AAOUJ-10-2022-0149

Li, X. (2020). Students' acceptance of mobile learning: An empirical study based on blackboard mobile learn. In *Mobile devices in education: Breakthroughs in research and practice* (pp. 354–373). IGI Global. https://doi.org/10.4018/978-1-7998-1757-4.CH022

Mai, P. T., & Tick, A. (2021). Cybersecurity awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytechnica Hungarica, 18*(8), 67–89. https://doi.org/10.12700/APH.18.8.2021.8.4

Maon, S. N., Hassan, N. M., Jailani, S. F. A. K., & Kassim, E. S. (2021). Gender differences in digital competence among secondary school students. *International Journal of Interactive Mobile Technologies, 15*(04), 73–84. https://doi.org/10.3991/IJIM.V15I04.20197

Mc Mahon, C. (2020). In defence of the human factor. *Frontiers in Psychology, 11*. https://doi.org/10.3389/FPSYG.2020.01390

Moallem, A. (2019). Cybersecurity awareness among students and faculty. In A. Mallem (Ed.), *Cybersecurity awareness among students and faculty*. CRC Press. https://doi.org/10.1201/9780429031908

Nagahawatta, R., Warren, M., & Yeoh, W. (2020). A study of cybersecurity issues in Sri Lanka. *International Journal of Cyber Warfare and Terrorism, 10*(3), 59–72. https://doi.org/10.4018/IJCWT.2020070105

Naser, M., Bazar, H. Al, & Abdel-Jaber, H. (2023). Mobile spyware identification and categorization: A systematic review. *Informatica (Slovenia), 47*(8), 45–56. https://doi.org/10.31449/INF.V47I8.4881

Nazar, M., Rusman, Puspita, K., & Yaqin, H. (2022). Android-based mobile learning resource for chemistry students in comprehending the concept of redox reactions. *International Journal of Interactive Mobile Technologies, 16*(3), 123–135. https://doi.org/10.3991/IJIM.V16I03.24133

Okokpujie, K., Kennedy, C. G., Nnodu, K., & Noma-Osagha, E. (2023). Cybersecurity awareness: Investigating students' susceptibility to phishing attacks for sustainable safe email usage in academic environment (a case study of a Nigerian leading university). *International Journal of Sustainable Development and Planning, 18*(1), 255–263. https://doi.org/10.18280/IJSDP.180127

Ortiz-Garcés, I., Govea, J., Sánchez-Viteri, S., & Villegas-Ch., W. (2024). CyberEduPlatform: An educational tool to improve cybersecurity through anomaly detection with Artificial Intelligence. *PeerJ Computer Science, 10*, Article e2041. https://doi.org/10.7717/PEERJ-CS.2041

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors, 23*(8), Article 4060. https://doi.org/10.3390/S23084060

Salhab, R., & Daher, W. (2023). University students' engagement in mobile learning. *European Journal of Investigation in Health, Psychology and Education, 13*(1), 202–216. https://doi.org/10.3390/EJIHPE13010016

Sari, D. I., Rejekiningsih, T., & Muchtarom, M. (2020). Students' digital ethics profile in the era of disruption: An overview from the Internet use at risk in Surakarta City, Indonesia. *International Journal of Interactive Mobile Technologies, 14*(3), 82–94. https://doi.org/10.3991/IJIM.V14I03.12207

Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: A comparison between smartphones and computers. *Education and Information Technologies, 26*(2), 1721–1736. https://doi.org/10.1007/s10639-020-10330-0

Taylor, J., & Whitty, M. (2023). An exploration of the awareness and attitudes of psychology students regarding their psychological literacy for working in the cybersecurity industry. *Psychology Learning & Teaching, 23*(2), 298–314. https://doi.org/10.1177/14757257231214612

Van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behavior change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity, 6*(1), 1–8. https://doi.org/10.1093/CYBSEC/TYAA019

Van, N. T., Abbas, A. F., Abuhassna, H., Awae, F., & Dike, D. (2021). Digital readiness for social educators in health care and online learning during COVID-19 pandemic: A bibliometric analysis. *International Journal of Interactive Mobile Technologies, 15*(18), 104–115. https://doi.org/10.3991/IJIM.V15I18.25529

Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access, 8*, 85094–85115. https://doi.org/10.1109/ACCESS.2020.2992807

Zhao, T., Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2024). Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry training. *Journal of Systems and Software, 210*. https://doi.org/10.1016/J.JSS.2023.111946

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cybersecurity awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269