International Journal of Safety and Security Engineering
Vol. 14, No. 4, August, 2024, pp. 1115-1123
Journal homepage: http://iieta.org/journals/ijsse

# Assessing Cybersecurity Awareness Among Vocational Students in Office Administration

Radinal Fadli[1*], Herman Dwi Surjono[2], Ratna Candra Sari[3], Yayuk Hidayah[4], Fivia Eliza[5]

[1] Postgraduate Program, Yogyakarta State University, Yogyakarta 55281, Indonesia
[2] Faculty of Engineering, Yogyakarta State University, Yogyakarta 55281, Indonesia
[3] Faculty of Economics and Business, Yogyakarta State University, Yogyakarta 55281, Indonesia
[4] Faculty of Social Sciences, Law and Political Sciences, Yogyakarta State University, Yogyakarta 55281, Indonesia
[5] Faculty of Engineering, Universitas Negeri Padang, Padang 25132, Indonesia

Corresponding Author Email: radinalfadli.2021@student.uny.ac.id



https://doi.org/10.18280/ijsse.140410

**Received:** 27 May 2024
**Revised:** 3 August 2024
**Accepted:** 16 August 2024
**Available online:** 30 August 2024

***Keywords:***
*cybersecurity awareness, office administration, cybersecurity education, vocational education, educational technology integration, digital safety, information security*

**ABSTRACT**

This study aims to evaluate the level of cybersecurity awareness among vocational high school students in the administration and office management program in eight vocational high schools in Indonesia. The research method used is quantitative descriptive research with an online test instrument that has met the criteria of validity, reliability, level of difficulty, and differentiation. The research sample consisted of 180 students who took the test. The data obtained were normally distributed and the population was declared homogeneous. The results of the study indicate that students have a basic understanding of cybersecurity, but there is still a significant need to improve the implementation of more effective cybersecurity practices. The average score for each indicator indicates challenges in understanding and consistently applying cybersecurity principles. The implications of these findings emphasize the need for curriculum revision and development of training programs that can better prepare students to face cybersecurity threats in a professional environment. This study provides a basis for further research to explore more effective educational strategies in improving cybersecurity awareness and skills among vocational program students.

## 1. INTRODUCTION

In the contemporary digital era, cyber security has become an important concern for various sectors, including education. With increasing reliance on technology, educational institutions must ensure that students are aware of cybersecurity principles to protect themselves and the information systems they interact with [1]. This is especially important in vocational education programs, such as office administration, where students are trained to manage and operate complex office technology and information systems. The primary objective of this study is to assess the level of cybersecurity awareness among vocational students in office administration programs, aiming to identify potential weaknesses and areas for improvement. By doing so, this research will not only contribute to the students' professional development but also help strengthen the cybersecurity posture of the organizations they will eventually serve.

As the digital landscape evolves, the nature of cyber threats also becomes more sophisticated, posing significant risks to personal and organizational data [2]. Educational institutions, especially those offering vocational training, play an important role in equipping students with the skills and knowledge necessary to navigate this complex environment [3]. In the office administration program, students are not only expected to be able to perform administrative tasks but also handle various automation systems that require a high level of cyber security awareness [4]. Understanding cybersecurity principles helps students anticipate, recognize, and mitigate potential cyber threats, thereby protecting the integrity of the systems they will manage in their professional careers.

Several studies have explored cyber security awareness in educational contexts. For example, a study conducted by Ghosh and Francia III [5] and Parvez et al. [6], found that cybersecurity education significantly improved students' understanding of online threats and their ability to implement protective measures. The researchers highlighted the importance of integrating cyber security training into education curricula to improve students' practical skills and awareness [7, 8]. Another study conducted by Rahim et al. [9], emphasized the role of ongoing cyber security awareness programs in maintaining a high level of awareness among students. Additionally, research conducted by Okokpujie et al. [10], shows that hands-on cybersecurity practices can effectively bridge the gap between theoretical knowledge and practical application. These studies collectively underscore the need for strong cybersecurity awareness to navigate the ever-evolving digital landscape. Although previous studies have extensively discussed cyber security awareness, they have not explored the level of cyber security awareness of vocational student specialty office administration. This research seeks to fill this gap by providing a focused assessment of the level of

cybersecurity awareness among office administration students, identifying potential weaknesses and areas for improvement. Understanding these unique challenges is critical, as office administration professionals' responsibilities often involve handling and protecting sensitive data, making them a prime target for cyberattacks.

Based on this, the aim of this research is to measure the level of cyber security awareness of vocational students in Office Administration Programs. Identifying the current level of awareness can address these gaps will not only benefit students in their professional development but also strengthen the overall cybersecurity posture of the organizations they will ultimately serve.

## 2. RELATED WORK

Cybersecurity in the contemporary digital landscape includes practices, technologies, and policies designed to protect networks, devices, programs, and data from unauthorized access, cyberattacks, and damage [11]. At the heart of cyber security is the concept of cyber security awareness, which refers to an individual's knowledge and understanding of cyber threats, their potential impact, and appropriate actions to mitigate risks [12]. The importance of cybersecurity awareness has been widely discussed in various studies. For example, a study by Georgiadou et al. [13], showed that individuals who understand cybersecurity principles are better able to recognize potential threats, such as phishing attacks or malware, and take proactive steps to reduce risks. In addition, Sari et al. [14] emphasize that this awareness also encourages responsible online behavior and ensures the confidentiality, integrity, and availability of sensitive information.

The importance of cybersecurity awareness cannot be understated. Individuals who understand cybersecurity principles are better able to recognize potential threats, such as phishing or malware attacks, and take proactive steps to mitigate risks [15]. Additionally, awareness drives responsible Online behavior and ensures the confidentiality, integrity, and availability of sensitive information [16]. Theoretical frameworks that support the development of cybersecurity awareness have been widely studied. One such theory is the Human Aspects of Information Security Theory (HAIST) [17], which emphasizes the critical role of human behavior in organizational security outcomes. Research by Parsons et al. [18] supports this by showing that training focused on the human aspects of cybersecurity can significantly enhance individuals' readiness to face digital threats.

In vocational education, particularly in programs such as office administration, cybersecurity awareness has significant relevance. These programs equip students with the technical skills to manage automated office systems, including handling sensitive data and carrying out administrative tasks efficiently [19]. Integrating cybersecurity awareness into vocational education ensures that future office administrators are not only proficient in their technical roles but also alert to cyber threats that could compromise organizational operations and data security. According to Chałubińska–Jentkiewicz [20], office administrators handle a variety of sensitive information, ranging from financial records to employees' personal data, making them prime targets for cyberattacks. The study emphasized that a strong understanding of cybersecurity principles among office administrators can significantly reduce the risk of data breaches and unauthorized access to critical systems. Furthermore, Nyikes et al. [21] highlighted that the increasing use of digital tools and cloud-based systems in office administration requires a high level of cybersecurity awareness to prevent potential vulnerabilities. The study indicated that without proper cybersecurity training, office administrators may inadvertently expose their organizations to cyberthreats through actions such as weak password management or improper handling of sensitive data. Thus, cybersecurity awareness is an absolute must-have competency for office administrators.

Several studies have explored cyber security awareness in various sectors. As research conducted by Al Shabibi and Al-Suqri [22], shows that cyber security education improves students' ability to recognize cyber threats and implement protective measures effectively. The findings are supported by AL-Nuaimi [23], showing that cybersecurity education improves students' ability to recognize cyber threats and implement protective measures effectively. The study conducted by Beuran et al. [24] emphasized the importance of integrating practical cybersecurity training into educational curricula to bridge the gap between theoretical knowledge and real-world applications. Similarly, Ricci et al. [25] highlight the benefits of integrating practical cybersecurity training into educational curricula to bridge the gap between theoretical knowledge and real-world applications. Additionally, Ramezanian and Niemi [26] underline the importance of ongoing cyber security education in maintaining a high level of awareness among students. Despite these insights, there is still a large gap in the literature regarding cybersecurity awareness especially in vocational education programs, particularly in office administration.

To date, there has been no comprehensive research that specifically examines the level of cyber security awareness among students of vocational education programs specializing in office administration. Understanding the current state of cybersecurity awareness in these programs is critical to identifying potential weaknesses and developing targeted educational interventions. This gap in the literature drives the need for research that assesses how prepared vocational students are in terms of cybersecurity awareness, especially considering their future roles in managing sensitive information and automated office systems.

Thus, the existing literature underlines the importance of cyber security awareness in educational contexts and in various sectors. This review highlights the need for focused research to investigate the level of cybersecurity awareness among vocational students in office administration programs. So, this research is to reveal the level of cyber security awareness of vocational education students in administration programs?

## 3. METHODOLOGY

This research uses a quantitative descriptive approach to assess cyber security awareness among vocational students specializing in office administration. Quantitative methods were chosen due to their ability to provide numerical data that can be analyzed statistically, thereby providing insight into the current level of cybersecurity awareness among research participants. This research uses online objective test instruments to collect data efficiently and objectively from various samples of students at several vocational high schools

in Indonesia. The research procedures carried out can be seen in Figure 1.

The first stage of this research involved designing a cyber security awareness assessment instrument. Before being implemented, the instrument has gone through rigorous prerequisite tests to ensure its validity, reliability, level of difficulty and distinguishing power to ensure the quality of the test instrument. The second stage, after the instrument met the requirements, data collection began at eight selected vocational high schools in Indonesia. The cyber security awareness level test was administered online to 180 students enrolled in a program specializing in office administration. Students are given clear instructions and sufficient time to complete the tests, ensuring standardized conditions for data collection. The third stage involves comprehensive data analysis starting with a data normality test to verify data distribution. Then, a homogeneity test is carried out to ensure homogeneity of variance between different data groups. Quantitative methods were used to analyze the data collected, with a focus on descriptive statistics to summarize student performance across various cybersecurity awareness indicators. The fourth stage in the research process involves synthesizing the findings from the data analysis stage. The results of the synthesis are contextualized within the existing literature on cybersecurity awareness in vocational education, emphasizing the unique contributions and implications of this research. Key findings are discussed in relation to the theoretical framework and practical implications for improving cybersecurity education in vocational settings.

### 3.1 Sample

The research sample consisted of 180 students enrolled in a vocational high school in Indonesia that offered a specialization program in office administration. These schools were selected based on their focus on providing technical skills related to managing automated office systems and handling administrative tasks efficiently. By involving students from various schools, this research aims to obtain a representative sample that reflects the diversity in the vocational education environment.

### 3.2 Research instrument

The main instrument used in this research is an online objective test designed to measure cyber security awareness among vocational students. The test consists of a series of multiple-choice questions, with each question targeting a specific aspect of cybersecurity awareness. These aspects are aligned with widely recognized cybersecurity best practices and are organized into seven key indicators, as outlined in Table 1. The test was administered through a Google Form platform, allowing easy access for all participants. Each participant was only given one opportunity to complete the test for a duration of 50 minutes, ensuring that the responses provided were thoughtful and representative of their understanding of cybersecurity. To ensure maximum participation, the test was open for three weeks. This time allowed participants the flexibility to complete the test according to their availability. Additionally, to remind and encourage participation, reminders were sent to participants at the end of each week during the period. These reminders were intended to ensure that all participants had the opportunity to participate and complete the test before the deadline. With this approach, the online test not only accurately measured cybersecurity awareness levels but was also conducted in a manner that took into account participants' time constraints and accessibility.

**Table 1.** Indicator of cybersecurity awareness test

| No. | Indicator | No. Item |
|---|---|---|
| 1 | Rules & Laws | 1, 2, 3, 4, 5 |
| 2 | Access & Password | 6, 7, 8, 9, 10 |
| 3 | Security settings | 11, 12, 13,14, 15 |
| 4 | Download & Software Update | 16, 17, 18, 19, 20 |
| 5 | Data backup | 21, 22, 23, 24, 25 |
| 6 | Social Media safety | 26, 27, 28, 29, 30 |
| 7 | Web Access | 31, 32, 33, 34, 35 |

Rules & Laws, this indicator assesses students' understanding of legal and regulatory frameworks surrounding cybersecurity, including data protection laws, intellectual property rights, and ethical guidelines. Example questions include scenarios where students must identify legal implications of certain cybersecurity practices.

Access & Password, Questions under this indicator evaluate students' knowledge about secure access protocols, password management strategies, and the importance of multi-factor authentication. Students are asked to identify strong versus weak passwords and the steps to secure access to sensitive information.

Security Settings, this section tests students' ability to understand and configure security settings on various devices and software applications. Questions focus on recognizing secure configurations and identifying potential vulnerabilities in default settings.

Download & Software Update, this indicator examines students' awareness of the risks associated with downloading software and the importance of regular updates. Students are presented with scenarios where they must decide on the safest course of action when prompted to download or update software.

Data Backup, Questions in this section assess students' understanding of data backup practices, including the importance of regular backups, choosing secure backup methods, and restoring data after a breach.


**Figure 1.** Research procedure

Social Media Safety, this indicator focuses on students' ability to navigate social media platforms securely, including recognizing phishing attempts, securing personal information, and understanding the privacy settings of various platforms.

Web Access, the final indicator evaluates students' knowledge of safe web browsing practices, such as recognizing secure websites, avoiding malicious links, and understanding the implications of cookies and tracking technologies.

Each indicator is designed to assess a specific aspect of cybersecurity awareness that is relevant to the vocational education context. This indicator is based on several previous studies [27-37]. Each item has been carefully crafted to reflect realistic scenarios that students might encounter in their professional careers, ensuring that the test not only assesses theoretical knowledge but also practical application.

### 3.3 Data analysis technique

3.3.1 Prerequisites tests

The prerequisite test is the first step in data analysis. This step involves several tests, the first of which is an item validity test to assess the extent to which the measurement instrument (in this case, a cybersecurity awareness test) measures what it is supposed to measure. An item is declared valid if the validity value is > 0.50, and declared invalid if the Validity value is < 0.50. The formula used to test the validity of question items is correlation product moment, which is as follows.

$$r_{xy} = \frac{N\sum xy - (\sum x)(\sum y)}{\sqrt{\left[N\sum x^2 - (\sum x)^2\right]\left[N\sum y^2 - (\sum y)^2\right]}} \quad (1)$$

The second test is the reliability test, this aims to measure the extent to which the instrument can provide consistent results if tested on the same population or at different times. The formula used in this test is Cronbach's alpha coefficient, where the test is declared reliable if the Cronbach's alpha value is > 0.70, namely as follows.

$$\alpha = \frac{n}{n-1}\left(1 - \frac{\sum \sigma_i^2}{\sigma_x^2}\right) \quad (2)$$

where,

n = total items

$\sigma^2_i$ = item variance

$\sigma^2_x$ = total score

Next, the third is the Discrimination Index Item Test to determine how well a question item can differentiate between respondents who have different levels of knowledge or ability in the topic being measured. The questions used are questions with a power difference value of $0.20 \leq P < 1.00$. The formula used is as follows.

$$P = \frac{\text{top group answered correctly}}{\text{bottom group answered correctly}} - 1 \quad (3)$$

Next, the fourth is a test of the difficulty level of the questions to determine how difficult or easy each question is in the test. The questions used are questions that have a difficulty index value of 0.40 – 0.80. The formula used is as follows.

$$\mathrm{T} = \frac{\text{number of respondents answered correctly}}{\text{Total respondent}} \quad (4)$$

3.3.2 Normality and homogeneity test

Before carrying out further analysis, data normality and homogeneity tests were carried out to verify the distribution and homogeneity of variance between data groups. The normality test using Kolmogorov-Smirnov (D), aims to assess whether the data follows a normal distribution. Data is normally distributed if the D value is > 0.05. The formula used in the normality test is as follows.

$$D = \max|F_n(X) - F_o(X) \quad (5)$$

where,

$D$ = Kolmogorov-Smirnov

$Fo(x)$ = Empirical distribution function

$Fn(x)$ = Theoretical distribution function

Σ = Standard deviation

The Normality test was carried out using the Lavene test (W), this test aims to ensure that comparisons between groups are carried out fairly and without bias, so that the results of the analysis can be interpreted accurately. Data is declared homogeneous if the W value is> 0.05. The formula used is as follows.

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

where,

$N$ = Total observations,

$k$ = Number of groups,

$n_i$ = Number of observations in the i-th group,

$Z_i$ = Average value of the i-th group,

$Z$ = Average value of all data.

3.3.3 Cybersecurity awareness level test

A cyber security awareness level test was conducted to assess knowledge and understanding of various aspects of cyber security among vocational students specializing in office administration. Test results are analyzed by comparing the average scores of each indicator to identify areas of strength and areas that need improvement among students. The analysis begins by calculating the average score for each indicator, which provides a clear picture of students' overall performance in various aspects of cybersecurity awareness. which is then compared with the standard level of cyber security awareness listed in Table 2.

**Table 2.** Criteria level of cybersecurity awareness

| Level | Score | Advice |
|---|---|---|
| Good | 80-100 | Need to Maintain |
| Sufficient | 60-79 | Need Improvement |
| Poor | <60 | Need Treatment |

## 4. RESULT

### 4.1 Prerequisites tests

In the prerequisite tests, question validity tests, reliability tests, discrimination tests and question difficulty tests are carried out. After carrying out the test, the prerequisites are obtained as in Table 3.

**Table 3.** Prerequisites tests result

| Question Number | Validity | Discrimination | Difficulty | Decision |
|---|---|---|---|---|
| Q 1 | 0.78 | 0.45 | 0.55 | Accepted |
| Q 2 | 0.82 | 0.50 | 0.60 | Accepted |
| Q 3 | 0.65 | 0.35 | 0.48 | Accepted |
| Q 4 | 0.60 | 0.30 | 0.52 | Accepted |
| Q5 | 0.70 | 0.40 | 0.57 | Accepted |
| Q 6 | 0.85 | 0.55 | 0.65 | Accepted |
| Q 7 | 0.75 | 0.42 | 0.50 | Accepted |
| Q 8 | 0.80 | 0.50 | 0.58 | Accepted |
| Q 9 | 0.68 | 0.38 | 0.47 | Accepted |
| Q 10 | 0.73 | 0.44 | 0.54 | Accepted |
| Q 11 | 0.77 | 0.48 | 0.59 | Accepted |
| Q 12 | 0.62 | 0.32 | 0.49 | Accepted |
| Q 13 | 0.79 | 0.50 | 0.61 | Accepted |
| Q 14 | 0.65 | 0.35 | 0.51 | Accepted |
| Q 15 | 0.74 | 0.45 | 0.55 | Accepted |
| Q 16 | 0.67 | 0.37 | 0.48 | Accepted |
| Q 17 | 0.72 | 0.40 | 0.50 | Accepted |
| Q 18 | 0.80 | 0.52 | 0.63 | Accepted |
| Q 19 | 0.58 | 0.30 | 0.46 | Accepted |
| Q 20 | 0.76 | 0.45 | 0.57 | Accepted |
| Q 21 | 0.83 | 0.53 | 0.62 | Accepted |
| Q 22 | 0.71 | 0.42 | 0.51 | Accepted |
| Q 23 | 0.66 | 0.36 | 0.49 | Accepted |
| Q 24 | 0.69 | 0.38 | 0.47 | Accepted |
| Q 25 | 0.78 | 0.46 | 0.55 | Accepted |
| Q 26 | 0.64 | 0.34 | 0.50 | Accepted |
| Q 27 | 0.75 | 0.44 | 0.53 | Accepted |
| Q 28 | 0.81 | 0.50 | 0.60 | Accepted |
| Q 29 | 0.70 | 0.40 | 0.52 | Accepted |
| Q 30 | 0.77 | 0.48 | 0.59 | Accepted |
| Q 31 | 0.61 | 0.31 | 0.45 | Accepted |
| Q 32 | 0.68 | 0.38 | 0.49 | Accepted |
| Q 33 | 0.74 | 0.44 | 0.54 | Accepted |
| Q 34 | 0.79 | 0.50 | 0.58 | Accepted |
| Q 35 | 0.82 | 0.53 | 0.61 | Accepted |
| | Reliability Test | | 0.82 | Reliable |

Validity measures how well the test items reflect the aspects being measured, with the correlation value between the item score and the total score. Validity values range from 0.58 to 0.85, indicating that the items are effective in measuring cybersecurity awareness. Items with validity values above 0.50 are considered to show good ability in assessing relevant aspects of cybersecurity awareness.

Discrimination Index measures how well test items can distinguish between students with good and poor understanding of cybersecurity. The discrimination value ranges from 0.30 to 0.55. Where the value is > 0.20 and < 1.00 so that the results of this value indicate that the test items can well distinguish between students with different levels of understanding.

Difficulty Level shows how difficult the test items are for participants, with values ranging from 0.45 to 0.65. Where the value is > 0.40 and < 0.80 so that the results of this value indicate that the test items have a moderate level of difficulty, which is not too easy or too difficult, so that they can be relied on to measure the level of cybersecurity awareness effectively.

The reliability of the test is 0.82, which exceeds the threshold value of 0.70. This shows that the test instrument provides consistent results when applied to the same population or at different times.

Based on the results of this analysis, all 35 question items were accepted for use in the cybersecurity awareness test because the validity, discrimination, level of difficulty, and reliability of each item met the criteria for good instrument quality. Thus, this test instrument can be relied on to provide an accurate picture of the level of cybersecurity awareness among students in administrative skills programs in vocational high schools.

### 4.2 Normality and homogeneity test

Before carrying out further analysis of the data that has been collected, a normality test was carried out using Kolmogorov-Smirnov (D) to verify whether the data followed a normal distribution, and a homogeneity test was carried out using Levene's Test (W) to check the uniformity of variance between groups. The results obtained are as presented in Table 4.

**Table 4.** Normality and homogeneity test result

| Statistic | Normality | Homogenity |
|---|---|---|
| Score | 0.135 | 0.174 |
| Sign | $\alpha = 0.05$ | $\alpha = 0.05$ |
| Conclution | D > α Normal Distribution | F > α Homogenous |

Based on the test results shown in the Table 4, the Kolmogorov-Smirnov (D) value of 0.135 indicates that the data follows a normal distribution because the D value is greater than α (0.05). In addition, the Levene's Test (W) result of 0.174 shows that the variance between data groups is homogeneous, because the W value is greater than α (0.05). Thus, the data obtained meets the assumptions of normality

and homogeneity, allowing further parametric statistical analysis to be carried out with a high level of confidence. Data that shows normal distribution and homogeneity of variance is met, indicating that the results of the test are conducted with a high level of confidence. This allows researchers to make valid and accurate inferences about the data.

### 4.3 Cybersecurity awareness test

After a cybersecurity awareness online test was conducted on 180 students enrolled in a program specializing in office administration at several vocational schools in Indonesia. The average results obtained from the indicators used for the assessment are summarized in Figure 2.

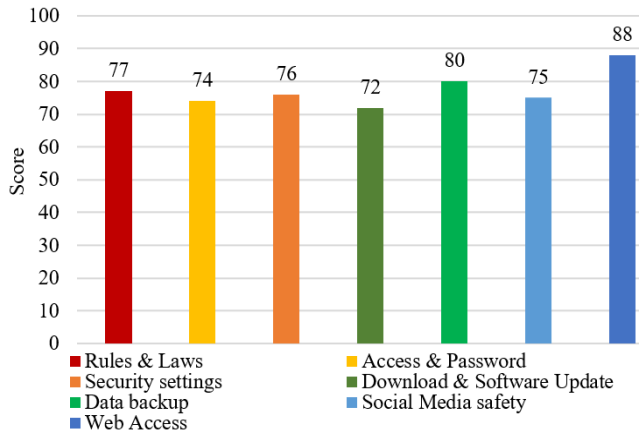


**Figure 2.** Cybersecurity awareness test result

Overall, the level of cybersecurity awareness among students in the administration skills program is at a Fair level, but this general assessment masks significant variations across different indicators. For example, the Web Access indicator, with the highest average score of 88, suggests that students are relatively well-versed in recognizing and managing secure web access. This could be attributed to the prevalence of web-based activities in both educational and personal contexts, where students frequently interact with web platforms, potentially increasing their familiarity with secure practices in this area. In contrast, the Download & Software Update indicator received the lowest average score of 72, indicating a concerning gap in awareness. This low score may reflect a lack of emphasis on the risks associated with unsafe downloading practices and the critical importance of keeping software up to date in the curriculum. The deficiency in this area is particularly alarming, as failure to regularly update software can leave systems vulnerable to cyber threats, such as malware or exploits targeting outdated software.

The Rules & Laws indicator also shows an area needing improvement, with an average score of 77. While students appear to have a basic understanding of cybersecurity-related regulations and laws, this score suggests that more comprehensive education on legal aspects of cybersecurity is required. This could be essential for their future roles, where understanding legal implications is crucial in protecting their organizations from legal and financial repercussions due to cyber incidents. Similarly, the scores for Access & Password (74) and Security Settings (76) highlight moderate gaps in understanding critical cybersecurity practices. Weak password management and improper security settings are often exploited in cyberattacks, so these areas require targeted educational interventions to ensure students develop a robust awareness and can apply best practices in their professional environments.

The Data Backup indicator received a slightly higher average score of 80, yet it still indicates a need for better education on the importance of regular data backups. Although students may recognize the importance of this practice, the score suggests that further emphasis is needed to ensure they can implement effective backup strategies in the workplace. Finally, the Social Media Safety indicator, with an average score of 75, suggests that students have a moderate understanding of safe practices when using social media. Given the increasing use of social media for professional networking and communication, enhancing awareness in this area is vital to prevent risks such as data breaches or reputational damage.

In summary, while students in the administration program demonstrate a foundational understanding of various cybersecurity practices, the results reveal critical areas where their knowledge and application need strengthening. To address these gaps, targeted educational interventions focusing on the lower-scoring indicators should be implemented to ensure that students are fully equipped to handle cybersecurity challenges in their future careers.

## 5. DISCUSSIONS

Cybersecurity awareness level test findings revealed significant areas of improvement across all tested indicators among vocational students specializing in office administration. The results of the normality and homogeneity tests confirm that the data meets the statistical assumptions required for further analysis, so we can conclude that the analysis carried out has a high level of reliability. The average score indicates a need to improve understanding and practice of cybersecurity principles. scores for Regulatory & Legal, Access & Passwords, Security Settings, Software Downloads & Updates, Data Backup, Social Media Security, and Web Access show that although students have basic knowledge, there is still great room for growth in understanding and implementing security cyber. action effectively.

These findings are in line with previous research, which also highlighted a lack of cyber security awareness among educational institutions [38]. The findings emphasize the important role of targeted cybersecurity education in educational settings, underscoring the importance of integrating practical skills and theoretical knowledge to foster a culture of cybersecurity awareness. Research by Erendor and Yildirim [39], also notes that gaps in understanding cyber security protocols can make educational institutions vulnerable to cyber threats, thus requiring proactive measures to strengthen awareness and preparedness.

The implications of these findings are profound, particularly in the context of vocational education, where students are being prepared for roles that may involve handling sensitive information and managing digital infrastructure. As noted by prior research, a lack of comprehensive understanding of cybersecurity protocols can leave educational institutions—and by extension, future workplaces—vulnerable to cyber threats. Therefore, it is imperative that educational curricula be revised to incorporate more robust cybersecurity training. This training should not only cover theoretical knowledge but also emphasize practical skills, possibly through real-world

simulations and hands-on exercises that can better prepare students for the challenges they will face in their professional careers.

This study is not without its limitations. The focus on quantitative assessment may have overlooked qualitative insights that could provide a deeper understanding of students' attitudes and behaviors toward cybersecurity. Additionally, the scope of the research was limited to specific geographic areas and educational programs, which may affect the generalizability of the findings. Future research should concentrate on developing and evaluating integrated cybersecurity awareness programs within vocational education curricula. Specifically, research can explore how embedding comprehensive cybersecurity training into vocational programs influences students' practical skills and preparedness for real-world cyber threats. Additionally, research should investigate best practices for integrating these programs into existing curricula to ensure they are engaging and relevant. By addressing these aspects, future research can provide valuable insights into optimizing curriculum design and training strategies, ultimately enhancing students' cybersecurity competencies and equipping them to navigate the increasingly complex digital landscape.

## 6. CONCLUSIONS

The findings of this study underscore the critical need to significantly enhance cybersecurity awareness among students in administrative skills programs. Despite a basic understanding of cybersecurity principles, there is substantial room for improvement in adopting more effective security practices. These findings highlight the urgent need for a comprehensive overhaul of curricula to integrate cybersecurity training that blends both practical and theoretical approaches. By restructuring educational programs to include hands-on simulations and real-world scenarios, institutions can better equip students to manage cybersecurity risks, thereby enhancing their preparedness for future challenges. This approach not only aims to bolster students' ability to navigate complex cyber threats but also contributes to the overall sustainability and security of educational institutions. Future research should focus on developing and evaluating integrated cybersecurity awareness programs within vocational education curricula. Specifically, studies should investigate how these programs, incorporating both theoretical knowledge and practical exercises, impact students' readiness to tackle real-world cyber threats. This could lead to the creation of more effective training models that can be implemented across various educational settings, ensuring that students are well-prepared to address the evolving cybersecurity landscape.

## ACKNOWLEDGMENT

We would like to express our heartfelt gratitude to the Ministry of Education, Culture, Research, and Technology (KEMENDIKBUDRISTEK), the Center for Educational Financing Services (Puslapdik), the Higher Education Financing Agency (BPPT), and the Education Fund Management Agency (LPDP) of the Republic of Indonesia for providing the Indonesian Education Scholarship (BPI). Their support has been instrumental in enabling us to complete this research.

## REFERENCES

[1] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., Choo, K.K.R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119: 102754. https://doi.org/10.1016/J.COSE.2022.102754

[2] Fakiha, B. (2021). Business organization security strategies to cyber security threats. International Journal of Safety and Security Engineering, 11(1): 101-104. https://doi.org/10.18280/IJSSE.110111

[3] Catota, F.E., Morgan, M.G., Sicker, D.C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1): tyz001. https://doi.org/10.1093/CYBSEC/TYZ001

[4] Li, H., Sun, Z., Huang, F. (2024). The impact of audit office cybersecurity experience on Nonbreach client's audit fees and cybersecurity Risks. Journal of Information Systems, 38(1): 177-206. https://doi.org/10.2308/ISYS-2023-014

[5] Ghosh, T., Francia III, G. (2021). Assessing competencies using scenario-based learning in cybersecurity. Journal of Cybersecurity and Privacy, 1(4): 539-552. https://doi.org/10.3390/JCP1040027

[6] Parvez, M.T., Alsuhibani, A.M., Alamri, A.H. (2023). Educational and cybersecurity applications of an Arabic CAPTCHA gamification system. Ingénierie des Systèmes d'Information, 28(5): 1275-1285. https://doi.org/10.18280/ISI.280516

[7] Boss, S.R., Gray, J., Janvrin, D.J. (2022). Accountants, cybersecurity isn't just for “techies”: Incorporating cybersecurity into the accounting curriculum. Issues in Accounting Education, 37(3): 73-89. https://doi.org/10.2308/ISSUES-2021-001

[8] Azzeh, M., Altamimi, A.M., Albashayreh, M., AL-Oudat, M.A. (2022). Adopting the cybersecurity concepts into curriculum: The potential effects on students’ cybersecurity knowledge. Indonesian Journal of Electrical Engineering and Computer Science, 25(3): 1749-1758. https://doi.org/10.11591/IJEECS.V25.I3.PP1749-1758

[9] Rahim, N.H.A., Hamid, S., Kiah, L.M. (2019). Enhancement of cybersecurity awareness program on personal data protection among youngsters in Malaysia: An assessment. Malaysian Journal of Computer Science, 32(3): 221-245. https://doi.org/10.22452/mjcs.vol32no3.4

[10] Okokpujie, K., Kennedy, C.G., Nnodu, K., Noma-Osaghae, 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 & Planning, 18(1): 255-263. https://doi.org/10.18280/IJSDP.180127

[11] Tn, N., Shailendra Kulkarni, M. (2023). Zero click attacks - A new cyber threat for the e-banking sector. Journal of Financial Crime, 30(5): 1150-1161. https://doi.org/10.1108/JFC-06-2022-0140

[12] Ramlo, S., Nicholas, J.B. (2021). The human factor: Assessing individuals’ perceptions related to cybersecurity. Information & Computer Security, 29(2): 350-364. https://doi.org/10.1108/ICS-04-2020-0052

[13] Georgiadou, A., Mouzakitis, S., Bounas, K., Askounis,

D. (2022). A cyber-security culture framework for assessing organization readiness. Journal of Computer Information Systems, 62(3): 452-462. https://doi.org/10.1080/08874417.2020.1845583
[14] 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
[15] Mc Mahon, C. (2020). In defence of the human factor. Frontiers in Psychology, 11: 1390. https://doi.org/10.3389/FPSYG.2020.01390
[16] Candiwan, C., Azmi, M., Alamsyah, A. (2022). Analysis of behavioral and information security awareness among users of zoom application in COVID-19 era. International Journal of Safety and Security Engineering, 12(2): 229-237. https://doi.org/10.18280/IJSSE.120212
[17] Shah, M.U., Iqbal, F., Rehman, U., Hung, P.C. (2023). A comparative assessment of human factors in cybersecurity: Implications for cyber governance. IEEE Access, 11: 87970-87984. https://doi.org/10.1109/ACCESS.2023.3296580
[18] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66: 40-51. https://doi.org/10.1016/J.COSE.2017.01.004
[19] Yemanov, V., Dzyana, H., Dzyanyi, N., Dolinchenko, O., Didych, O. (2023). Modelling a public administration system for ensuring cybersecurity. International Journal of Safety & Security Engineering, 13(1): 81-88. https://doi.org/10.18280/IJSSE.130109
[20] Chałubińska–Jentkiewicz, K. (2022). Cybersecurity as a public task in administration. In Cybersecurity in Poland, pp. 191-208. https://doi.org/10.1007/978-3-030-78551-2_13
[21] Nyikes, Z., Kovács, T.A., Honfi, V.S., Illési, Z. (2022). Digital competence and security awareness from the perspective of sustainability. In Security-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach, pp. 139-150. https://doi.org/10.1007/978-94-024-2174-3_12
[22] Al Shabibi, A.M., Al-Suqri, M.N. (2022). Cybersecurity awareness among students during the COVID-19 digital transformation of education: A case study at the Muscat (Oman) schools. In The Sharjah International Conference on Education in Post COVID-19, Sharjah, United Arab Emirates, pp. 39-51. https://doi.org/10.1007/9789819919277_4
[23] AL-Nuaimi, M.N. (2024). Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: A systematic review. Global Knowledge, Memory and Communication, 73(1/2): 1-23. https://doi.org/10.1108/GKMC-12-2021-0209
[24] Beuran, R., Tang, D., Tan, Z., Hasegawa, S., Tan, Y., Shinoda, Y. (2019). Supporting cybersecurity education and training via LMS integration: CyLMS. Education and Information Technologies, 24: 3619-3643. https://doi.org/10.1007/s10639-019-09942-y
[25] Ricci, S., Parker, S., Jerabek, J., et al. (2024). Understanding cybersecurity education gaps in Europe. IEEE Transactions on Education, 67(2): 190-201. https://doi.org/10.1109/TE.2023.3340868
[26] Ramezanian, S., Niemi, V. (2024). Cybersecurity education in universities: A comprehensive guide to curriculum development. IEEE Access, 12: 61741-61766. https://doi.org/10.1109/ACCESS.2024.3392970
[27] Alharbi, T., Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2): 23. https://doi.org/10.3390/bdcc5020023
[28] Johri, A., Kumar, S. (2023). Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation. Human Behavior and Emerging Technologies, 2023(1): 2103442. https://doi.org/10.1155/2023/2103442
[29] Tran, T.M., Beuran, R., Hasegawa, S. (2023). Gamification-based cybersecurity awareness course for self-regulated learning. International Journal of Information and Education Technology, 13(4): 724-730. https://doi.org/10.18178/IJIET.2023.13.4.1859
[30] Daengsi, T., Pornpongtechavanich, P., Wuttidittachotti, P. (2022). Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. Education and Information Technologies, 27: 4729-4752. https://doi.org/10.1007/S10639-021-10806-7
[31] Lee, C.S., Kim, D. (2023). Pathways to cybersecurity awareness and protection behaviors in South Korea. Journal of Computer Information Systems, 63(1): 94-106. https://doi.org/10.1080/08874417.2022.2031347
[32] Abdukadir Ahmed, A., Hussein Elmi, A., Abdullahi, A., Yahye Ahmed, A. (2023). Cybersecurity awareness among university students in Mogadishu: A comparative study. Indonesian Journal of Electrical Engineering and Computer Science, 32(3): 1580-1588. https://doi.org/10.11591/ijeecs.v32.i3.pp1580-1588
[33] 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): e202312. https://doi.org/10.30935/ojcmt/12942
[34] Huraj, L., Lengyelfalusy, T., Hurajová, A., Lajčin, D. (2023). Measuring cyber security awareness: A comparison between computer science and media science students. TEM Journal, 12(2): 623-633. https://doi.org/10.18421/TEM122-05
[35] Moallem, A. (2019). Cybersecurity Awareness Among Students and Faculty. CRC Press. https://doi.org/10.1201/9780429031908
[36] Alrobaian, S., Alshahrani, S., Almaleh, A. (2023). Cybersecurity awareness assessment among trainees of the technical and vocational training corporation. Big Data and Cognitive Computing, 7(2): 73. https://doi.org/10.3390/BDCC7020073
[37] 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
[38] 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

[39] Erendor, M.E., Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis. IEEE Access, 10: 52319-52335. https://doi.org/10.1109/ACCESS.2022.3171829