Data and Metadata. 2024; 3:.544
doi: 10.56294/dm2024.544

DATA & METADATA

ORIGINAL

Building a Secure Digital Future: Investigating Cyber Hygiene Levels of Accounting, Finance, and Business Students

Construyendo un futuro digital seguro: investigación sobre los niveles de higiene cibernética de los estudiantes de contabilidad, finanzas y negocios

Fivia Eliza[1], Radinal Fadli[2], Yayuk Hidayah[3], M. Aghpin Ramadhan[4], Abdulnassir Yassin[5], Mohammad Bhanu Setyawan[6], Sutrisno[6]

[1]Padang State University, Department Electrical Enginering. Padang, Indonesia.
[2]Muhammadiyah University of Muara Bungo, Department Information Technology Education. Bungo, Indonesia.
[3]Yogaykarta State University, Department Civic Education and Law. Yogyakarta, Indonesia.
[4]Jakarta State University, Department Building engineering education. Jakarta, Indonesia.
[5]Islamic University in Uganda, Department Curriculum and Instruction, Kampala, Uganda.
[6]Muhammadiyah University of Ponorogo, Department of Informatics, Ponorogo, Indonesia.

Cite as: Eliza F, Fadli R, Hidayah Y, Ramadhan MA, Yassin A, Bhanu Setyawan M, et al. Building a Secure Digital Future: Investigating Cyber Hygiene Levels of Accounting, Finance, and Business Students. Data and Metadata. 2024; 3:.554. https://doi.org/10.56294/dm2024.554

Submitted: 01-05-2024 **Revised:** 02-09-2024 **Accepted:** 15-12-2024 **Published:** 16-12-2024

Editor: Adrián Alejandro Vitón-Castillo

Corresponding author: Fivia Eliza

ABSTRACT

Introduction: this study aims to investigate the level of cyber hygiene among accounting, finance and business students, to identify strengths and weaknesses to inform the development of cybersecurity in education.
Method: a quantitative research design was employed, utilizing an objective online test to assess cyber hygiene knowledge. The instrument was validated through tests of validity, difficulty level, discriminatory power, and reliability. The study sample consisted of students in finance, administration and business. Data analysis involved statistical methods to compare awareness levels across the three student groups.
Results: the results indicated that administration students had the highest overall cyber hygiene awareness, particularly in areas such as Rules & Laws, Access & Password, and Security Settings. Business students showed moderate awareness, while accounting students demonstrated significant gaps, especially in Web Access and Social Media Safety. The findings highlighted the need for targeted educational interventions to address specific weaknesses in each group.
Conclusions: this study underscores the importance of cyber hygiene education, especially for accounting, finance, and business students, to prevent cyber incidents. The findings provide actionable insights for the development of curricula and training programs, which contribute to a safer digital environment in professional settings. Further research should expand sample sizes, incorporate qualitative methods, and explore the long-term effectiveness of cyber hygiene education.

Keywords: Cyber Hygiene; Administration; Finance; Business; Cybersecurity Education; Digital Security.

RESUMEN

Introducción: este estudio tiene como objetivo investigar el nivel de ciberhigiene entre los estudiantes de contabilidad, finanzas y negocios, para identificar fortalezas y debilidades que sirvan de base para el desarrollo de la ciberseguridad en la educación.
Método: se empleó un diseño de investigación cuantitativa, utilizando una prueba objetiva en línea para evaluar el conocimiento de la ciberhigiene. El instrumento se validó mediante pruebas de validez, nivel de dificultad, poder discriminatorio y confiabilidad. La muestra del estudio estuvo compuesta por estudiantes

de finanzas, administración y negocios. El análisis de datos implicó métodos estadísticos para comparar los niveles de conocimiento entre los tres grupos de estudiantes.

Resultados: los resultados indicaron que los estudiantes de administración tenían la mayor conciencia general sobre la ciberhigiene, particularmente en áreas como reglas y leyes, acceso y contraseñas y configuraciones de seguridad. Los estudiantes de negocios mostraron una conciencia moderada, mientras que los estudiantes de contabilidad demostraron brechas significativas, especialmente en acceso web y seguridad en redes sociales. Los hallazgos destacaron la necesidad de intervenciones educativas específicas para abordar debilidades específicas en cada grupo.

Conclusiones: este estudio subraya la importancia de la educación sobre ciberhigiene, especialmente para los estudiantes de contabilidad, finanzas y negocios, para prevenir incidentes cibernéticos. Los resultados aportan información útil para el desarrollo de planes de estudio y programas de formación que contribuyan a un entorno digital más seguro en los entornos profesionales. Las investigaciones futuras deberían ampliar el tamaño de las muestras, incorporar métodos cualitativos y explorar la eficacia a largo plazo de la educación sobre higiene cibernética.

Palabras clave: Higiene Cibernética; Administración; Finanzas; Negocios; Educación en Ciberseguridad; Seguridad Digital.

INTRODUCTION

In an era dominated by digital transformation, the practice of cyber hygiene has become critical in safeguarding not only personal data but also the very backbone of modern businesses and economies. Cyber hygiene refers to the practices and steps that individuals and organizations commonly take to maintain the health of their cyber environment.(1) These practices include updating software regularly, using strong and unique passwords, backing up data, and being alert to potential cyber threats.(2) The importance of cyber hygiene cannot be underestimated as it lays the foundation for strong cybersecurity measures and helps prevent cyber attacks, data breaches and other security incidents.

The rise in cyber attacks has highlighted the urgent need for effective cyber hygiene practices. Cyber hygiene refers to the practices and measures taken by individuals and organizations to maintain the health and security of their digital environment.(3) Over the past decade, cyberattacks have increased significantly with increasingly diverse attack methods targeting individuals and organizations.(4) These attacks range from phishing and ransomware to more complex exploits such as advanced persistent threats.(5) As cyber threats continue to evolve, the need for comprehensive cyber hygiene practices becomes more urgent. Ensuring that individuals, especially those in critical sectors such as accounting,(6) finance,(7) and business,(8) are well versed in cyber hygiene is critical to mitigating risks and protecting sensitive information.

Students in administration, finance, and business, mastering cyber hygiene is not just a skill—it is a critical responsibility. These future professionals will handle sensitive financial data,(9) business strategies,(10) and administrative records,(11) making their understanding of cyber hygiene essential to securing the integrity of the organizations they will serve.(12) Therefore, students with a strong understanding of cyber hygiene are expected to implement effective practices that will directly impact the security of the organizations they work for. (13) By instilling cyber hygiene education, we not only equip them with the tools needed for their careers but also contribute to fostering a safer digital environment across industries. (14,15) Ultimately, this commitment to cyber hygiene will empower them to become proactive defenders against cyber threats, safeguarding not only their organizations but also the broader digital ecosystem.

Several previous studies have examined various aspects of cyber hygiene. Research conducted by Vishwanath, A. et al.(16) demonstrates how cyber hygiene significantly predicts aspects of human interaction with technology that are crucial for cybersecurity, including users' confidence in technology, how they cognitively process information online, and their online banking behavior. Similarly, a study by Baraković, S et al.(17) reveals that while students exhibit acceptable cyber hygiene behaviors, their awareness is less than satisfactory, and their knowledge is quite low. Additionally, this research shows a correlation between gender, current level of education, and knowledge, awareness, and behavior regarding cyber hygiene, as well as the mutual influence and relationship between these outcomes. Another study by Kioskli, K., et al.(18) focused on the role of cyber hygiene in the healthcare sector, highlighting that cyber hygiene practices were low among members of healthcare organizations. This issue is particularly pressing given the rapid increase in cyberattacks on healthcare organizations, most of which are caused by human error. Finally, research by Cain, A. A., et al.(19) investigated the impact of cultural factors on cyber hygiene awareness, indicating that cultural differences play a significant role in shaping perceptions and practices of cyber hygiene. These studies underscore the importance of cyber hygiene but also reveal significant gaps, such as the need for practical training, the influence of cultural factors, and the inconsistent implementation of cyber hygiene practices.

https://doi.org/10.56294/dm2024.554

To address the research gap, this study poses the following research questions: (1) What is the level of cyber hygiene among students in the fields of administration, finance, and business? (2) Which cyber hygiene indicators require greater attention? (3) How do these stuents perceive the importance of cyber hygiene in their future professional roles? Based on the identified gaps, the aim of this research is to evaluate the level of cyber hygiene among students in administration, finance, and business fields. By addressing these gaps, the research aims to contribute to enhancing cyber hygiene education, ultimately leading to better preparedness among future professionals in safeguarding digital information.

METHOD

This study employs a quantitative research design, utilizing an objective online test to assess the level of cyber hygiene awareness among students in the fields of administration, finance, and business. The quantitative approach enables the collection of numerical data, allowing for statistical analysis to identify patterns, correlations, and differences among groups of students. The online test serves as a standardized and effective tool to measure students' knowledge and practices related to cyber hygiene. The research process is conducted in four stages, as outlined in figure 1 below.

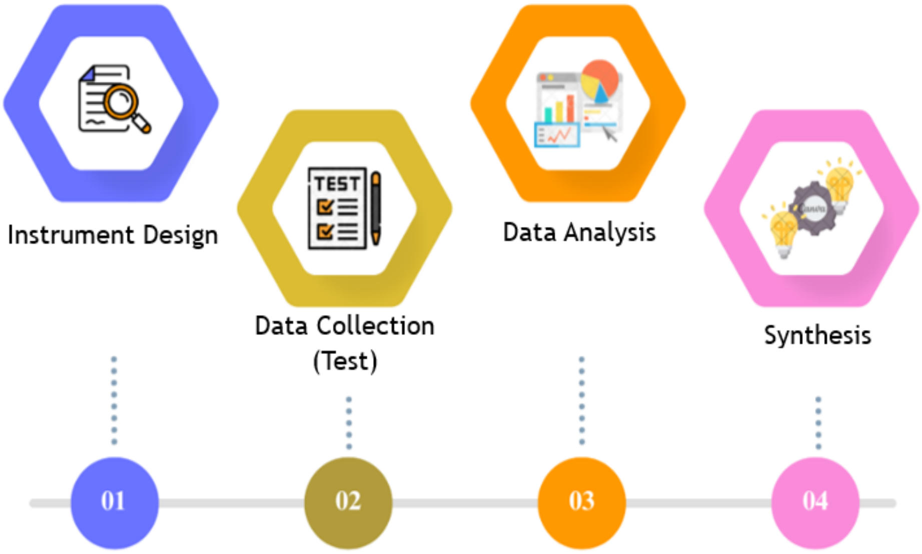

Figure 1. Research Procedure

The instrument employed in this research is an objective online test designed to evaluate various aspects of cyber hygiene awareness. The test was developed based on a comprehensive review of existing literature and expert input, ensuring both validity and reliability. It comprises multiple-choice questions targeting different indicators of cyber hygiene.

Data Collection

The data collection process involved administering the online test to participants. The test was distributed electronically, and students were allotted a specific time frame to complete it. Participant responses were automatically collected through an online platform, ensuring efficiency and accuracy.

Data Analysis

The collected data was analyzed using statistical methods to assess the level of cyber hygiene awareness among students. This analysis aimed to identify trends, patterns, and significant insights into their knowledge and practices.

Synthesis and Conclusion

In the final stage, the results of the data analysis were synthesized to draw meaningful conclusions and formulate recommendations. This synthesis process involved interpreting the statistical findings within the context of the existing literature and the study's specific objectives.

Sample

The sample for this research consisted of 100 students in finance, administration and business students who took online tests. The sample included 32 administration program students, 35 finance program students, and

33 business program students. The participants were selected using a purposive sampling method to ensure representation from each of the three disciplines.

Instrument

The instrument used in this research is an objective online test designed to measure cyber hygiene awareness. This test includes indicators that cover aspects of cyber hygiene. Indicators are prepared based on previous research which also measures cyber hygiene.[21,22,23,24,25,26,27] indicators can be seen in table 1 below.

Table 1. Indicator of cyber hygiene

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

The Rules & Laws indicator assesses students' understanding of cybersecurity laws and regulations. The Access & Password indicator evaluates knowledge of secure access methods and password management practices. The Security Settings indicator examines students' ability to configure and manage security settings across various devices and platforms. The Software Downloads & Updates indicator focuses on safe download practices and the importance of regular software updates. The Data Backup indicator measures awareness of effective data backup methods and the significance of maintaining regular backups. The Social Media Security indicator addresses safe practices on social media platforms, including privacy settings and the ability to recognize potential threats. Finally, the Web Access indicator evaluates safe web browsing habits and the ability to identify secure websites. The test is designed to be comprehensive, covering critical aspects of cyber hygiene relevant to students in administration, finance, and business programs. These indicators were selected based on insights from multiple previous studies.

Analisis Data

Prerequisites Tests

The first step in data analysis is to examine the test prerequisites. This involves several tests, including item validity tests to ensure that each question in the test measures the intended concept appropriately. The formula used is as follows.

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

The second test conducted is the reliability test, which aims to determine the instrument's ability to produce consistent results when applied to the same population or at different points in time. This test uses the Cronbach's alpha coefficient as the measurement formula. An instrument is considered reliable if the Cronbach's alpha value exceeds 0,70, as demonstrated below.

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

The third test is the Discrimination Index Item Test, which evaluates how effectively a question item distinguishes between respondents with varying levels of knowledge or skills in the subject being assessed. Questions included in the test are those with a discrimination index value ranging from 0,20 to less than 1,00. The formula applied for this calculation is as follows.

$$\mathrm{T} = \frac{\text{number of respondents answered correctly}}{\text{Total respondent}} \qquad (3)$$

The fourth test focuses on assessing the difficulty level of each question to determine how challenging or

https://doi.org/10.56294/dm2024.554

straightforward the test items are. Questions selected for this purpose have a difficulty index value between 0,40 and 0,80. The formula applied for this test is outlined as follows.

Normality and Homogeneity Test

Prior to conducting further analysis, tests for data normality and homogeneity were performed to ensure the data distribution and variance across groups were appropriate for analysis. The normality test, conducted using the Kolmogorov-Smirnov (D) method, evaluates whether the data conforms to a normal distribution. The data is considered normally distributed if the D value exceeds 0,05. The formula utilized for the normality test is as follows.

$$D = \max|Fn(X) - F0(X) \qquad (4)$$

The normality test is conducted using the Levene test (W), which aims to ensure that comparisons between groups are unbiased and fair, enabling accurate interpretation of the analysis results. The data is considered homogeneous when the W value exceeds 0,05. The formula applied for this test is as follows.

$$W = \frac{(N-k)}{(k-1)} \frac{\sum_{i=1}^{k} n_i (Z_i - Z)2}{[\sum_{i=1}^{k} ni \ln(S_i) - (S_T)]} \qquad (5)$$

Cyber Hygiene Test

The Cyber Hygiene Test is conducted to assess knowledge and understanding of various aspects of cybersecurity among students in finance, administration and business. 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 cyber hygiene. which is then compared with the standard level of Cybers Hygiene Knowledge listed in table 2 below.

Table 2. Criteria Level of Cybers Hygiene Knowledge

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

RESULTS

Prerequisetes Tests

The validity, discrimination index, level of difficulty, and reliability of the test items were thoroughly evaluated to ensure the strength and effectiveness of the cyber hygiene tests. Each of the 35 items was examined against these criteria, and a decision was made to use all items based on their performance. The results obtained can be seen in table 3. Below.

Table 3. Prerequisites Tests Result

No	Validity	Discrimination	Difficulty	Decision	No	Validity	Discrimination	Difficulty	Decision
1	0,78	0,45	0,55	Used	19	0,58	0,30	0,46	Used
2	0,82	0,50	0,60	Used	20	0,76	0,45	0,57	Used
3	0,65	0,35	0,48	Used	21	0,83	0,53	0,62	Used
4	0,60	0,30	0,52	Used	22	0,71	0,42	0,51	Used
5	0,70	0,40	0,57	Used	23	0,66	0,36	0,49	Used
6	0,85	0,55	0,65	Used	24	0,69	0,38	0,47	Used
7	0,75	0,42	0,50	Used	25	0,78	0,46	0,55	Used
8	0,80	0,50	0,58	Used	26	0,64	0,34	0,50	Used
9	0,68	0,38	0,47	Used	27	0,75	0,44	0,53	Used
10	0,73	0,44	0,54	Used	28	0,81	0,50	0,60	Used

11	0,77	0,48	0,59	Used	29	0,70	0,40	0,52	Used
12	0,62	0,32	0,49	Used	30	0,77	0,48	0,59	Used
13	0,79	0,50	0,61	Used	31	0,61	0,31	0,45	Used
14	0,65	0,35	0,51	Used	32	0,68	0,38	0,49	Used
15	0,74	0,45	0,55	Used	33	0,74	0,44	0,54	Used
16	0,67	0,37	0,48	Used	34	0,79	0,50	0,58	Used
17	0,72	0,40	0,50	Used	35	0,82	0,53	0,61	Used
18	0,80	0,52	0,63	Used	Reliability		0,82	Reliable	

Item validity ranged from 0,58 to 0,85, with average validity well above acceptable thresholds, indicating that the questions effectively measured what they were intended to assess. The discrimination index, which evaluates each item's ability to differentiate between high and low performers, varies from 0,30 to 0,55. Items with a discrimination index above 0,40, such as item 6 (0,55) and item 18 (0,52), demonstrate good ability to differentiate between different levels of student understanding. The difficulty level of test questions ranges from 0,45 to 0,65, reflecting a balanced range that ensures the test is neither too easy nor too difficult. Overall test reliability, assessed using Cronbach's alpha, was calculated as 0,82. These high reliability scores confirm that the test consistently measures the construct of cyber hygiene across items and student groups. This prerequisite test underscores the power of the evaluation tool used in this study and confirms its suitability for assessing cyber hygiene among finance, administration and business students. This comprehensive validation process increases the credibility of the findings and supports subsequent analysis and discussion of the results.

Normality and Homogeneity Test

Before proceeding with further analysis of the collected data, a normality test was performed using the Kolmogorov-Smirnov (D) method to determine whether the data conformed to a normal distribution. Additionally, a homogeneity test was conducted using Levene's Test (W) to assess the consistency of variance across groups. The outcomes of these tests are summarized in table 4 below.

Table 3. Prerequisites Tests Result

Statistic	**Normality**	**Homogeneity**
Score	0,135	0,174
Sign.	α = 0,05	α = 0,05
Conclusion	D > α Normal Distribution	F > α Homogenous

For the normality test, the Kolmogorov-Smirnov test was used which produces a statistic (D) of 0,135. If compared with the significance level (α) of 0,05, it is determined that D > α. These results indicate that the data follows a normal distribution. A normal distribution implies that data points are distributed symmetrically around the mean, allowing for more accurate and reliable statistical conclusions. Homogeneity of variance was assessed using Levene's test which produced a statistic (F) of 0,174. As with the normality test, the significance level (α) is set at 0,05 and it is obtained that F > α. These findings indicate that the variance between the different groups being compared is homogeneous. Homogeneity of variance is essential to ensure that comparisons between groups are valid and that observed differences are not due to variability in the distribution of the data. This test increases the robustness and credibility of the overall research methodology and subsequent results.

Cyber Hygiene Test

Cyber hygiene knowledge test results on various indicators for students in accounting, administration, and business show different patterns and areas of strengths and weaknesses among these groups.

Rules & Laws

For the Rules & Laws indicator, administration program students achieved the highest average score of 77, which reflects a strong understanding of cybersecurity laws and regulations. This shows that administration students better understand the legal framework and compliance requirements related to cybersecurity. Business students scored an average of 68, indicating a moderate level of awareness, while accounting students scored the lowest at 60. The relatively lower scores among accounting students highlight potential gaps in their education regarding the importance and specifics of cybersecurity law, which is a very important thing. for their future role in safeguarding financial data. Comparison of results Graphically can be seen in the following figure 2.

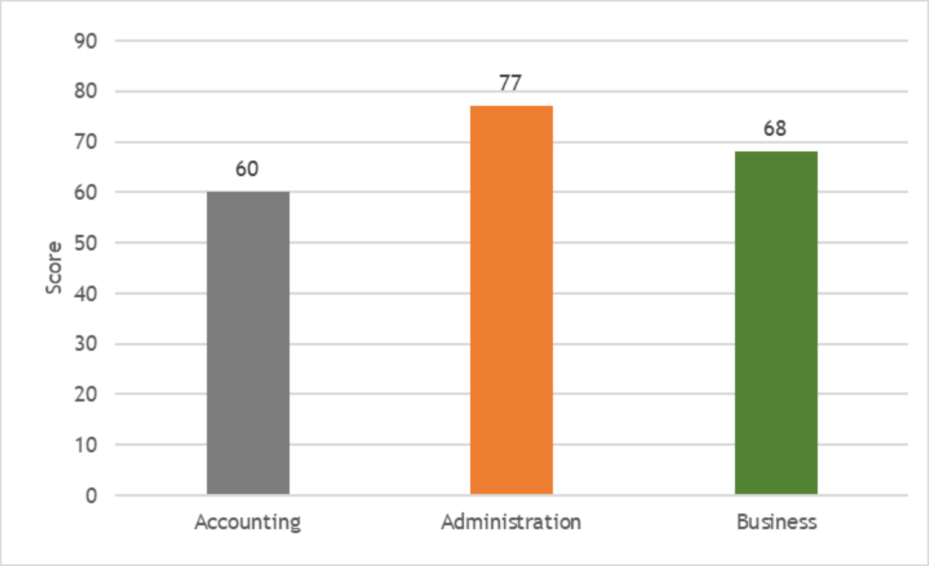

Figure 2. Level Cyber Hygiene: Rule and Law

Access & Password

In the Access & Password category, administration students again led with an average score of 74, followed by accounting students with a score of 68, and business students with a score of 63. The high score among administration students indicates that they have a better understanding. secure access methods and password management practices, which are essential for protecting sensitive information. Lower scores among business and accounting students indicate the need for additional training and awareness programs focused on creating and managing strong passwords, as well as secure access protocols to prevent unauthorized access. Comparison of results Graphically can be seen in the following figure 3.

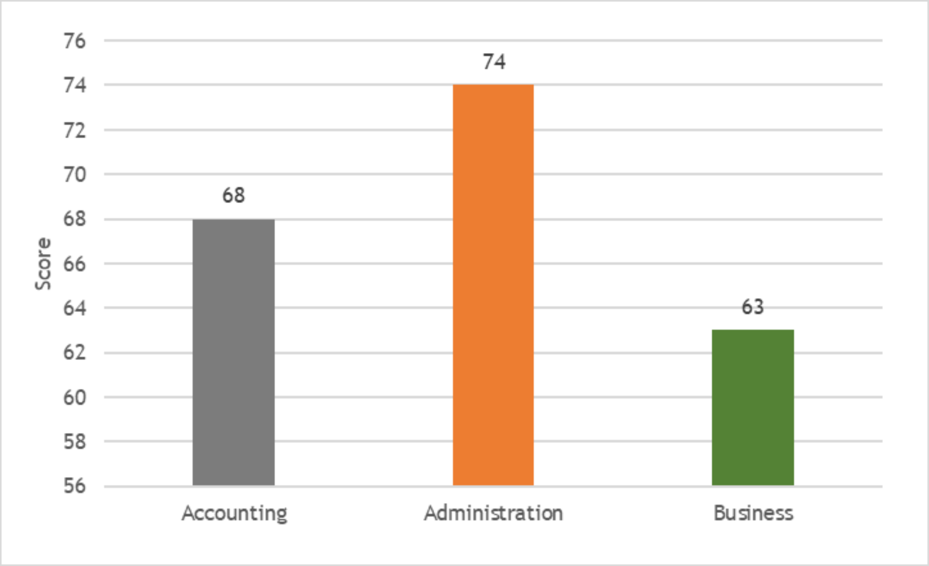

Figure 3. Level Cyber Hygiene: Access and Password

Security Settings

Regarding Security Settings, administration students demonstrate a high level of knowledge with an average score of 76. Business students scored 65, and accounting students scored the lowest at 56. These results show that administration students are more proficient in configuring and managing security settings across different devices and platforms. The significant gap between the grades of administration and accounting students suggests that the latter group may need further education to improve the understanding and implementation of security arrangements, which are critical to protecting organizational and personal data. Comparison of results

Graphically can be seen in the following figure 4.

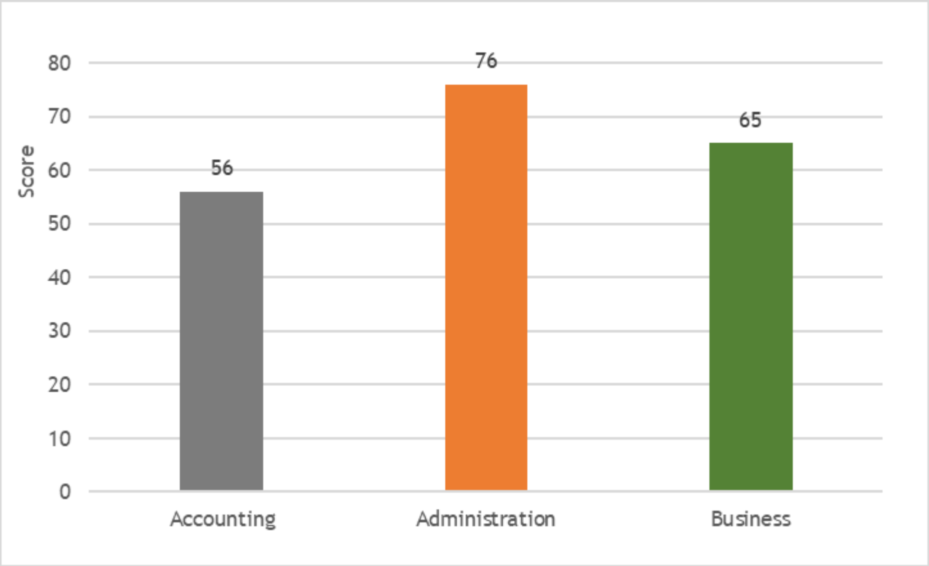

Figure 4. Level Cyber Hygiene: Security Setting

Download & Software Update

On the Software Downloads & Updates indicator, administration students scored an average of 72, which reflects a relatively good understanding of secure downloading practices and the importance of regular software updates. Accounting students followed with a score of 66, while business students got the lowest score of 62. Higher scores among administration students indicate that they are more aware of the risks associated with software downloads and the need to update software to reduce vulnerabilities. Lower grades for business and accounting students highlight the need for increased education regarding safe downloading habits and the importance of software updates to maintain system security. Comparison of results Graphically can be seen in the following figure 5.

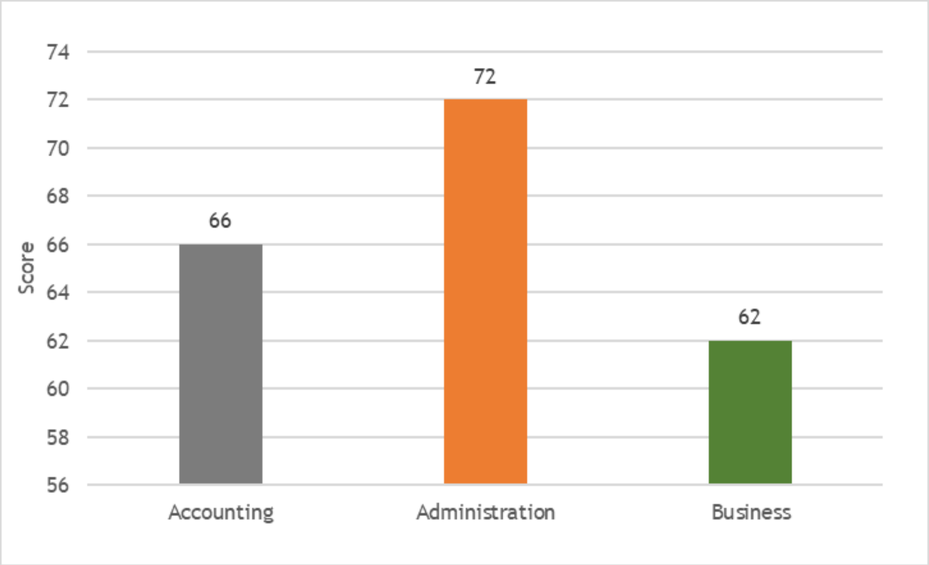

Figure 5. Level Cyber Hygiene: Download and Software Update

Data backup

For the Data Backup indicator, administration students again excelled with an impressive average score of 80, demonstrating a strong awareness of data backup methods and the importance of regular backups. Accounting students get a score of 64, and business students get the lowest score of 60. These results show that administration students are well prepared to implement data backup strategies, which are crucial for data recovery in the event of a cyber incident. The relatively low scores among accounting and business students indicate an important need for targeted training on effective data backup practices to ensure that these students can maintain data integrity in their future professional roles. Comparison of results Graphically can be seen in the following figure 6.

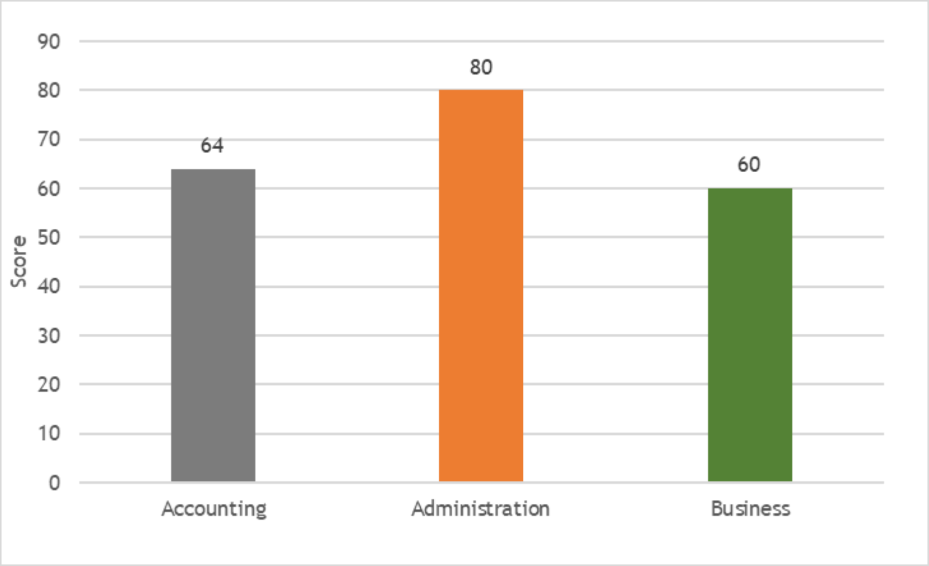

Figure 6. Level Cyber Hygiene: Data Backup

Social Media safety

The Social Media Safety indicator shows an interesting deviation, with business students getting the highest average score of 78, which indicates a good understanding of safe practices on social media platforms, including privacy settings and recognizing threats. Administration students are next with a score of 75, while accounting students get the lowest score of 55. This shows that business students are more sensitive to the risks associated with using social media, which is important for protecting personal and organizational reputations online. The much lower scores among accounting students underscore the need for increased education about social media security, emphasizing the potential risks and the steps needed to mitigate them. Comparison of results Graphically can be seen in the following figure 7.

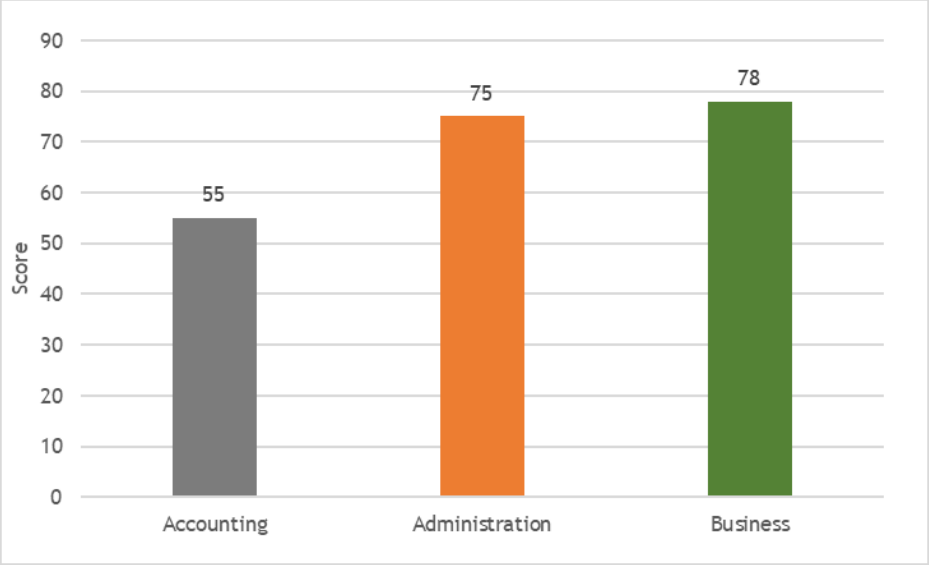

Figure 7. Level Cyber Hygiene: Social Media Safety

Web Access

Lastly, for the Web Access category, administration students excelled with a high average score of 88, demonstrating a strong knowledge of safe web browsing habits and the ability to recognize secure websites. Business students get a score of 73, while accounting students get the lowest score of 40. A very high score for administration students demonstrates a good understanding of web security practices, which is essential for avoiding malicious websites and ensuring safe use of the internet. The very low grades for accounting students highlight a large gap in their knowledge and indicate an urgent need for comprehensive training on secure web access practices to protect against web-based threats. Comparison of results Graphically can be seen in the following figure 8.

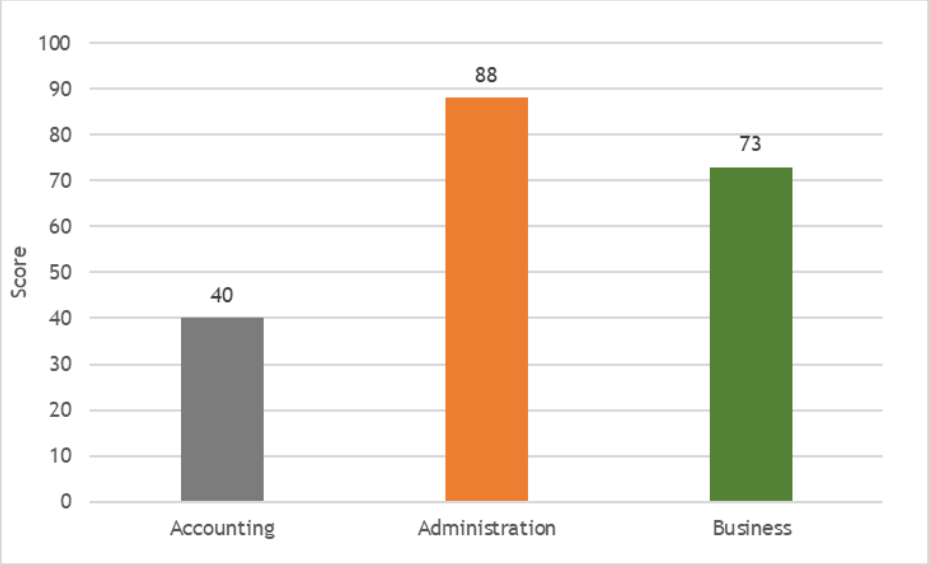

Figure 8. Level Cyber Hygiene: Web Access

DISCUSSION

The results of the prerequisite tests including validity, level of difficulty, differentiating power, and reliability show that the instruments used in this study are powerful and well-constructed instruments. The validity test ensures that the questions accurately measure cyber hygiene knowledge, while the difficulty and discriminatory power test ensures that the questions are challenging enough and can differentiate students with different levels of knowledge. Reliability tests show consistency in test results, thus reinforcing the dependability of the instrument. In addition, normality and homogeneity tests showed that the data were normally distributed and came from homogeneous populations, validating the suitability of the samples for this study and ensuring that the statistical analysis conducted would provide meaningful and reliable results.

The results of the cyber knowledge hygiene test reveal significant insights regarding the level of awareness among students in the fields of administration, finance, and business. Administration students consistently outperform their peers in most indicators, particularly in areas such as Rules & Laws, Access & Passwords, and Security Settings. This indicates that these students have a more comprehensive understanding of cyber hygiene principles, most likely due to the more extensive training or curriculum coverage in their programs. In contrast, accounting students scored the lowest in several key areas, particularly in Web Access and Social Media Security, highlighting the critical need to improve education and training in these areas. The difference in scores underscored the importance of targeted interventions to address the specific weaknesses identified in each group of students.

The findings of this study are in line with previous research on cyber hygiene awareness in educational settings. Research conducted by Okokpujie, K., et al.(28) found a significant gap in cybersecurity knowledge between computer students and media students, similar to the gap identified among students in this study. The findings of the research conducted by Al-Janabi, S., et al.(29) highlight the need for practical application of cybersecurity concepts in secondary education, a recommendation that is in line with the results of our research, where practical knowledge, especially among accounting students, was found to be lacking. Additionally, research conducted by Salem, Y., et al.(30) emphasizes the role of ongoing training and awareness programs in improving cyber hygiene practices, supporting the need for ongoing educational efforts identified in this research. The uniqueness of this research lies in its focus on students in three different fields: administration, finance, and business. This analysis highlights areas where targeted educational interventions are needed to improve cyber hygiene knowledge and practices among students in these fields, thereby ensuring they are better prepared to address cybersecurity challenges in their future professional environments.

This study, although its comprehensive analysis of cyber hygiene awareness among students in the fields of administration, finance, and business, has certain limitations that must be acknowledged. Although the sample size is representative, it is limited to 100 students, so it can affect the ability to generalize findings in a wider population. In addition, the study relies solely on self-reported online tests, which can lead to bias in responses. Future research should consider expanding sample size and geographic coverage to improve generalization capabilities, incorporating qualitative methods such as interviews or focus groups to gain deeper insights, and longitudinal studies to assess the effectiveness of cyber hygiene education in the long term. Additionally, exploring the impact of different pedagogical approaches and integrating emerging cybersecurity threats into the curriculum can provide valuable insights for improving cyber hygiene education.

CONCLUSION

This study highlights the significant variations in cyber hygiene awareness among students in administration, finance, and business fields, with administration students consistently outperforming their peers. These findings emphasize the urgent need for targeted educational interventions to address specific weaknesses, particularly among accounting students, to ensure a safer digital environment. This research contributes to the development of cybersecurity education by providing insights that inform curriculum design and training programs, thereby equipping future professionals with essential skills to mitigate cyber threats effectively.

REFERENCES

1. Fikry A, Hamzah MI, Hussein Z, Abdul AJ, Abu Bakar KA. Defining the Beauty of Cyber Hygiene: A Retrospective Look. IEEE Eng Manag Rev. 2024 Apr 1;52(2):174-80.Available from: https://doi.org/10.1109/EMR.2024.3361023

2. Kamarudin S, Tang L, Bolong J, Adzharuddin NA. A systematic literature review of mitigating cyber security risk. Qual Quant [Internet]. 2024;58(4):3251-73. Available from: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85180255676&doi=10.1007%2Fs11135-023-01791-9&partnerID=40&md5=cce4f149628a1f43e8e412f04ad58311

3. Et. al. NHNZ. Synthesizing Cybersecurity Issues And Challenges For The Elderly. Turkish J Comput Math Educ [Internet]. 2021;12(5):1775-81. Available from: https://www.turcomat.org/index.php/turkbilmat/article/view/2180

4. Eliza F, Fadli R, Ramadhan MA, Sutrisno VLP, Hidayah Y, Hakiki M, et al. Assessing student readiness for mobile learning from a cybersecurity perspective. Online J Commun Media Technol. 2024 Oct 1;14(4):e202452. Available from: https://doi.org/10.30935/OJCMT/15017

5. Fadli R, Surjono HD, Sari RC, Hidayah Y, Eliza F. Assessing Cybersecurity Awareness Among Vocational Students in Office Administration. Int J Saf Secur Eng. 2024 Aug 1;14(4):1115-23. Available from: https://doi.org/10.18280/IJSSE.140410

6. Amer TB, Al-Omar MIA. The Impact of Cyber Security on Preventing and Mitigating Electronic Crimes in the Jordanian Banking Sector. Int J Adv Comput Sci Appl. 2023;14(8):371-80. Available from: https://doi.org/10.14569/IJACSA.2023.0140841

7. Grody AD. Addressing cyber risk in financial institutions and in the financial system. J Risk Manag Financ Institutions. 2020 Mar 1;13(2):155-62. Available from: https://doi.org/10.69554/LCUN5985

8. Eling M. Cyber risk research in business and actuarial science. Eur Actuar J. 2020 Dec 1;10(2):303-33. Available from: https://doi.org/10.1007/S13385-020-00250-1

9. Hart S, Margheri A, Paci F, Sassone V. Riskio: A Serious Game for Cyber Security Awareness and Education. Comput Secur [Internet]. 2020;95. Available from: https://www.sciencedirect.com/science/article/pii/S0167404820301012

10. Hobbs J. Cybersecurity awareness in higher education: a comparative analysis of faculty and staff. Issues Inf Syst. 2023;24(1):159-69. Available from: https://doi.org/10.48009/1_iis_2023_114

11. Karayel T, Aktaş B, Akbıyık A. Human factors in remote work: examining cyber hygiene practices. Inf Comput Secur. 2024; Available from: https://doi.org/10.1108/ICS-11-2023-0215

12. Ngo FT, Agarwal A, Holman K. Cyber Hygiene and Cyber Victimization Among Limited English Proficiency (LEP) Internet Users: A Mixed-Method Study. Vict Offenders. 2024; Available from: https://doi.org/10.1080/15564886.2024.2329765

13. Salem MA, Sobaih AEE. A Quadruple "E" Approach for Effective Cyber-Hygiene Behaviour and Attitude toward Online Learning among Higher-Education Students in Saudi Arabia amid COVID-19 Pandemic. Electron. 2023 May 1;12(10). Available from: https://doi.org/10.3390/ELECTRONICS12102268

14. Gyaisey AP, Owusu A. Multi-Contextual Analysis of Internet Security Perception and Behavior: Perspectives of Anglophone and Francophone Internet Users. Int J Cyber Warf Terror. 2022;12(1). Available from: https://doi.org/10.4018/IJCWT.305243

15. Wilner AS, Luce H, Ouellet E, Williams O, Costa N. From public health to cyber hygiene: Cybersecurity and Canada's healthcare sector. Int J. 2021 Dec 1;76(4):522–43. Available from: https://doi.org/10.1177/00207020211067946

16. Vishwanath A, Neo LS, Goh P, Lee S, Khader M, Ong G, et al. Cyber hygiene: The concept, its measure, and its initial tests. Decis Support Syst. 2020 Jan 1;128. Available from: https://doi.org/10.1016/J.DSS.2019.113160

17. Baraković S, Baraković Husić J. Cyber hygiene knowledge, awareness, and behavioral practices of university students. Inf Secur J. 2023;32(5):347–70. Available from: https://doi.org/10.1080/19393555.2022.2088428

18. Kioskli K, Fotis T, Nifakos S, Mouratidis H. The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. Appl Sci. 2023 Mar 1;13(6). Available from: https://doi.org/10.3390/APP13063410

19. Cain AA, Edwards ME, Still JD. An exploratory study of cyber hygiene behaviors and knowledge. J Inf Secur Appl. 2018 Oct 1;42:36–45. Available from: https://doi.org/10.1016/J.JISA.2018.08.002

20. Alsobeh AMR, Alazzam I, Shatnawi AMJ, Khasawneh I. Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. Online J Commun Media Technol [Internet]. 2023;13(2). Available from: https://www.ojcmt.net/article/cybersecurity-awareness-factors-among-adolescents-in-jordan-mediation-effect-of-cyber-scale-and-12942

21. Huraj L, Lengyelfalusy T, Hurajová A, Lajčin D. Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students. TEM J. 2023 May 1;12(2):623–33. Available from: https://doi.org/10.18421/TEM122-05

22. Taha N, Dahabiyeh L. College students information security awareness: a comparison between smartphones and computers. Educ Inf Technol [Internet]. 2021 Mar 1 [cited 2023 Jun 20];26(2):1721–36. Available from: https://link.springer.com/article/10.1007/s10639-020-10330-0

23. Alharbi T, Tassaddiq A. Assessment of cybersecurity awareness among students of Majmaah University. Big Data Cogn Comput [Internet]. 2021 May 10 [cited 2023 Jun 20];5(2):23. Available from: https://www.mdpi.com/2504-2289/5/2/23/htm

24. Pratama AR, Firmansyah FM, Rahma F. Security awareness of single sign-on account in the academic community: the roles of demographics, privacy concerns, and Big-Five personality. PeerJ Comput Sci [Internet]. 2022;8. Available from: https://doi.org/10.7717/peerj-cs.918

25. Kruger HA, Kearney WD. A prototype for assessing information security awareness. Comput Secur. 2006 Jun 1;25(4):289–96. Available from: https://doi.org/10.1016/j.cose.2006.02.008

26. Mohanty SN, Singh T, Goel R, Baral SK, Kumar R. A study on building awareness in cyber security for educational system in India using interpretive structural modellings. Int J Syst Assur Eng Manag. 2024 Jun 1;15(6):2518–28. Available from: https://doi.org/10.1007/S13198-024-02273-3

27. Rahim NHA, Hamid S, Kiah MLM. Enhancement of cybersecurity awareness program on personal data protection among youngsters in Malaysia: An assessment. Malaysian J Comput Sci [Internet]. 2019;32(3):221–45. Available from: https://doi.org/10.22452/mjcs.vol32no3.4

28. Okokpujie K, Kennedy CG, Nnodu K, Noma-Osagha E. Cybersecurity Awareness: Investigating Students'

Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University). Int J Sustain Dev Plan. 2023 Jan 1;18(1):255–63. Available from: https://doi.org/10.18280/IJSDP.180127

29. Al-Janabi S, Al-Shourbaji I. A Study of Cyber Security Awareness in Educational Environment in the Middle East. J Inf Knowl Manag [Internet]. 2016;15(1). Available from: https://doi.org/10.1142/S0219649216500076

30. Salem Y, Moreb M, Rabayah KS. Evaluation of Information Security Awareness among Palestinian Learners. In: 2021 International Conference on Information Technology (ICIT) [Internet]. IEEE; 2021 [cited 2023 Jun 20]. p. 21–6. Available from: https://ieeexplore.ieee.org/document/9491639/

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Fivia Eliza, Radinal Fadli.
Data curation: Fivia Eliza, Radinal Fadli.
Formal analysis: Fivia Eliza, Radinal Fadli.
Research: Radinal Fadli.
Methodology: Fivia Eliza, Yayuk Hidayah.
Project management: Yayuk hidayah.
Resources: Fivia Eliza.
Software: Radinal Fadli.
Supervision: M. Aghpin Ramadhan.
Validation: Abdulnassir Yassin, Muhammad Banu Setyawan, and Sutrisno.
Display: Radinal Fadli.
Drafting - original draft: Fivia Eliza, Radinal Fadli.
Writing - proofreading and editing: Fivia Eliza, Radinal Fadli.