ITEJ
Indonesian Technology and Education Journal

E-ISSN: 2985-8216; P-ISSN: 2985-8208
Volume 3, **Number 1**, February 2025
/https://doi.org/10.61255/itej

Digital Data Security Literacy in College Students: An Analysis of Awareness and Behavior in Facing Cyber Threats in the Digital Age

Alif Alfi Takdir[1*], Devi Miftahul Jannah[2]
[1,2]Universitas Negeri Makassar

[1]alifalfi262@gmail.com, [2]devimiftahul734@email.com

ITEJ Journal
Article History:
Submitted: 20-November-2024
Accepted: 23-Desember-2024
Published: 05-January-2025
Keywords:
Cyber threats; Digital security; Security literacy; College students; Data protection
***Corresponding Author:**
Alif Alfi Takdir

ABSTRACT

Digital data security is a crucial issue in the era of modern technology, especially for students who are vulnerable to cyber threats. This study aims to analyze the effect of digital data security literacy on students' awareness and behavior in protecting personal data. The research was conducted with a quantitative method using a cross-sectional design, involving 107 students as respondents. Data were obtained through a Likert scale-based questionnaire and analyzed descriptively using Microsoft Excel and Jamovi. The results showed that the user education and awareness aspect had the highest average (3.82), reflecting students' good understanding of the importance of maintaining data confidentiality. However, the data access aspect had the lowest average score (3.60), indicating the need for improvement in controls over personal data access. These findings are relevant to previous literature, which confirms the importance of digital security education in improving literacy and awareness of cyber threats. This research provides new insights that can serve as a basis for developing more effective digital security education programs in educational institutions. By improving digital data security literacy, students are expected to be better able to protect their data from threats in the digital era.

INTRODUCTION

In the rapidly evolving digital era, Cybersecurity is increasingly becoming an important issue in today's digital era. In recent years, we have seen an increase in the number and complexity of cyberattacks that threaten computer systems and data around the world [1]. Personal data security is a human right [2]. This phenomenon occurs because fraud cases are increasingly rampant, especially through platforms such as WhatsApp and other social media. Such scams can even occur on a large scale and are difficult to detect if our level of literacy and understanding of digital security is low. This is all the more relevant given the rapid development in information and communication technology, which also increases the risk of breaches to personal data security [3]. Therefore, "Digital Security" provides an important foundation for students to understand and face challenges related to digital security, data protection, and relevant legal aspects in an increasingly digitally connected world. An understanding of these laws is essential to maintain security and privacy in an ever-changing digital environment [4].

Previous research shows that cybersecurity awareness has a significant impact on a person's cybersecurity practices [5]. In addition, research also shows that the lack of education about cybersecurity causes a decrease in the level of awareness of the threat of cybercrime that can harm individuals, groups, and companies [6]. In another study, it was shown that digital knowledge, digital trust, and digital alertness have a significant contribution to digital security literacy [3]. Literature studies also show that it is important to analyze how digital data security affects students and the impact of cyber threats that haunt them in this digital era [7].

Previous research shows that the rise of cyber threat cases that occur due to various factors, one of which is the increasing access of online users. The amount of personal data information that enters and the weak security system on the online technology makes it easy to attack the theft of data information [8]. In addition, comprehensive education is needed to increase student awareness of the importance of digital data protection. This education includes an understanding of cyber threats, basic security practices such as using strong passwords, and how to recognize phishing

ITEJ
Indonesian Technology and Education Journal
E-ISSN: 2985-8216; P-ISSN: 2985-8208
Volume 3, Number 1, February 2025
/https://doi.org/10.61255/itej

and malware attacks [9]. Increasing awareness and education about cybersecurity among students is very important. With a better understanding, students are expected to be more proactive in reporting and responding to such actions. Digital media literacy also needs to be emphasized so that students use social media wisely. This research can be the basis for intervention and training programs in educational institutions [10].

Although various studies have discussed the importance of digital security literacy, there are still a number of questions that have not been fully answered. One of them is how the level of digital security literacy affects students' behavior in protecting their personal data practically, especially in the midst of increasingly complex cyberattacks. In addition, although education about data security is increasingly socialized, there are still few studies that explore the effectiveness of cybersecurity education programs among university students. Questions that need further research include: To what extent can cybersecurity education increase awareness and preventive measures among university students? And what factors are most influential in improving their digital security literacy?

In the context of students, this research is important considering the increasing number of data breach cases and cyber threats that occur among students. Students are one of the most active groups of internet users, both for academic and social purposes, so they are potential targets for cyber crime. The high level of online activity among students also demands extra protection of their personal data. By understanding the influence of digital data security and increasing literacy in this area, it is hoped that students can be more vigilant and able to protect their data from the threats that haunt the digital era. This research is expected to be the basis for developing more effective educational programs to improve digital security literacy in educational institutions.

The purpose of this study is to analyze the effect of digital data security literacy on students' awareness and behavior in protecting their personal data from cyber threats. This study also aims to identify the level of student awareness related to cybersecurity and evaluate the effectiveness of educational programs that have been implemented on campus. Thus, this research is expected to provide recommendations for educational institutions in improving digital security literacy and awareness among students, so that they can be better prepared to face challenges in the digital era.

METHODOLOGY

This study uses a quantitative design [11] with a cross-sectional approach [12] to analyze the effect of digital data security literacy on college students' awareness and behavior in protecting their personal data from cyber threats. The research sample consisted of 107 respondents selected through a Google Form Questionnaire, which is effective for collecting data from university students. Data was collected by sharing a link to a Google Form questionnaire containing closed questions, using a Likert scale to measure perceptions by respondents, The research was conducted on the campus of "Makassar State University" in November of 2024 [13]. with the aim of knowing how much the level of digital data security literacy of students in protecting their personal data. This method allows replication of research in the future.

Table 1. Instrument Grid

No	Aspects / Sub-factors	Statement	Statement Number	References (Can be from 1 article only or from 2 articles)
1	Data Security	I feel comfortable storing my important data on a digital platform that has a good reputation for security	1	
		I feel confident that my data will not be lost or corrupted when stored in the organization's digital system	2	
		I trust that the company where I store my digital	3	

E-ISSN: 2985-8216; P-ISSN: 2985-8208
Volume 3, **Number 1**, February 2025
/https://doi.org/10.61255/itej

		data regularly updates their security systems		[14] "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education"
		The organization that manages my data has adequate security measures in place to protect my data from theft	4	
		I feel my personal data is kept safe by the organization that collects it	5	
2	Data Access	I feel I have control over who can access my personal data in digital systems	6	[14] "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education"
		The company or platform I use gives me the option to set my data access permissions	7	
		I am confident that only those I authorize can access my personal data	8	
		I trust that my personal data will not be shared with third parties without my permission	9	
		I believe that the company provides clear information about who can access my personal data	10	

E-ISSN: 2985-8216; P-ISSN: 2985-8208
Volume 3, **Number 1**, February 2025
/https://doi.org/10.61255/itej

3	Kontrol Privasi	I am aware of my privacy rights when it comes to the use and storage of personal data	11	[14] "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education"
		I can make a request to delete my personal data if necessary	12	
		The digital platform I use provides options for users to review and manage stored data	13	
		I am comfortable with how the organization manages and controls my personal data	14	
		I feel I have full control to retrieve my personal data from the platforms I use	15	

E-ISSN: 2985-8216; P-ISSN: 2985-8208
Volume 3, **Number 1**, February 2025
/https://doi.org/10.61255/itej

4	Regulatory Compliance	I trust that the organization that holds my data complies with applicable data protection regulations (such as GDPR)	16	[14] "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education"
		I feel secure that the organizations I trust follow government-mandated data security standards.	17	
		It is important to me that the organization that holds my data adheres to data privacy rules and regulations.	18	
		I trust that the company will notify me in the event of a data breach or leak involving my personal data	19	
		I am confident that the digital platforms I use adhere to privacy policies properly and transparently	20	
5	User Education and Awareness	I understand the importance of keeping my personal data confidential on digital platforms	21	[14] "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education"
		I feel that the company provides adequate education on how to protect my personal data	22	
		I know how to set privacy settings on the digital platforms I use	23	
		I feel the company or platform provides information on how to report data security issues	24	
		I actively seek information on how to protect my personal data in a digital environment	25	

ITEJ
Indonesian Technology and Education Journal
E-ISSN: 2985-8216; P-ISSN: 2985-8208
Volume 3, Number 1, February 2025
/https://doi.org/10.61255/itej

RESULT & DISCUSSION

The data was assessed quantitatively using a Likert Scale with the aim of providing a score in the form of a scale on each statement in the questionnaire. Table 2 below shows the Likert Scale Levels used as follows:

Table 2. Likert scale

Scale	Type
5	Strongly Agree
4	Agree
3	Neutral
2	Disagree
1	Strongly Disagree

After the average value of the answers is known, then the results are interpreted based on table 1 then the researcher makes a continuum line:

NJI (Interval Level Value) = Max-Value Min-Value Number of Statement Criteria
Scale Width = 5-15
= 0,8

It can be concluded that:

. Index Minimum: 1
a. Index Minimum: 1
b. Index Maximum: 5
c. Interval: 5-1 = 4
d. Interval Distance: (4-1) ÷ 4 = 0.8

To support data analysis, this study used a Likert scale to measure respondents' perceptions and psychological impact. This scale helps convert qualitative responses into quantitative data that can be analyzed. Table 3 below shows the Likert scale intervals used.

Table 3. Interval Scale Likert

Scale		Ket
1,00	1,80	Strongly Disagree
1,81	2,60	Disagree
2,61	3,40	Neutral
3,41	4,20	Agree
4,21	5,00	Strongly Agree

Table 4 below shows the gender distribution of respondents involved in this study. This data provides an overview of the gender composition that can affect respondents' perceptions and experiences related to Digital Security, and supports further analysis in discussing the results of the study.

Table 4. Demographics Respondents

Gender	N	Percentage (%)
Male	48	44,86%
Female	59	55,14%
Total	107	

ITEJ
Indonesian Technology and Education Journal
E-ISSN: 2985-8216; P-ISSN: 2985-8208
Volume 3, Number 1, February 2025
/https://doi.org/10.61255/itej

Selanjutnya, Pada Tabel 5 di bawah ini menyajikan hasil analisis deskriptif [15], Analisis ini memberikan ga An overview of students' perceptions and experiences of Digital Security, which forms the basis for further discussion. This study uses descriptive analysis, descriptive analysis is a form of research data analysis to test the generalization of research results based on one sample. The analysis is used to describe quantitative data collected through a Google Form questionnaire on privacy security in digital data storage, there are 5 variables measured, namely, Data Security (AK), Data Access (AD), Privacy Control (AP), Regulatory Compliance (AKP), User Education and Awareness (AE). Once the data was collected, irrelevant information was removed and answers were coded into numbers to facilitate analysis. Microsoft Excel was used to average the results per variable, calculate the mean (average) value of each variable, while Jamovi was used to calculate the median, mode, sum (total number), max (maximum value), and min (minimum value), as well as to conduct further descriptive analysis. The results of the analysis are presented in tables that visualize the distribution of data and facilitate understanding of the relationship between the variables studied.

Table 5. Descriptive Analysis Results

	Total AK	Total AD	Total AP	Total AKP	Total AE
N	107	107	107	107	107
Missing	0	0	0	0	0
Mean	3.65	3.60	3.73	3.71	3.82
Median	3.60	3.60	3.80	3.80	4.00
Mode	3.60	3.00	4.00	3.00	4.00
Sum	390	386	399	397	409
Standard deviation	0.749	0.785	0.748	0.749	0.792
Minimum	1.00	1.00	1.00	1.60	1.00
Maximum	5.00	5.00	5.00	5.00	5.00

Table 5 presents the descriptive analysis for the five variables measured on 107 respondents. The User Education and Awareness (AE) aspect has the highest average (3.82) and the Data Access (AD) aspect the lowest (3.60). The median was highest for the User Education and Awareness Aspect (AE) at (4.00), while the most frequent mode was 3.00 for AK, AD, and AKP, and 4.00 for AP and AE. The standard deviation shows the largest variation in AE (0.792) and the smallest in AP (0.748). The range of values (minimum 1.00 and maximum 5.00) was almost the same for most of the variables, but there were some differences in the mean and dispersion of the variables.

Table 6 below presents descriptive data regarding Data Security on Digital Security. The following is a table of descriptive data on Data Security:

Table 6. Descriptive Data of Data Security

No	Item/Statement/ Question						
		Mean	Median	Modus	Minimum	Maximum	Sum
Data Security							
1.	**AK 1**	**3.96**	**4**	**4.00**	**1**	**5**	**424**
2.	**AK 2**	**3.43**	**3**	**3.00**	**1**	**5**	**367**
3.	**AK 3**	**3.64**	**4**	**3.00**	**1**	**5**	**390**
4.	**AK 4**	**3.64**	**4**	**4.00**	**1**	**5**	**390**
5.	**AK 5**	**3.56**	**3**	**3.00**	**1**	**5**	**381**

ITEJ
Indonesian Technology and Education Journal
E-ISSN: 2985-8216; P-ISSN: 2985-8208
Volume 3, Number 1, February 2025
/https://doi.org/10.61255/itej

Table 7 below illustrates the descriptive data for Data Access at Digital Security. The following is a table of descriptive data for Data Access:

Table 7. Descriptive Data of Data Access

No	Item/Statement/ Question						
		Mean	Median	Modus	Minimum	Maximum	Sum
Data Access							
1.	AD 1	3.54	4	3.00	1	5	379
2.	AD 2	3.67	4	4.00	1	5	393
3.	AD 3	3.61	4	4.00	1	5	386
4.	AD 4	3.57	4	4.00	1	5	382
5.	AD 5	3.63	4	4.00	1	5	388

Table 8 below presents descriptive data regarding Privacy Control on Digital Security. The following is a table of descriptive data for Privacy Control:

Table 8. Privacy Control Descriptive Data

No	Item/Statement/ Question						
		Mean	Median	Modus	Minimum	Maximum	Sum
Privacy Controls							
1.	AP 1	3.74	4	4.00	1	5	400
2.	AP 2	3.87	4	4.00	1	5	414
3.	AP 3	3.76	4	4.00	1	5	402
4.	AP 4	3.57	4	4.00	1	5	382
5.	AP 5	3.73	4	4.00	1	5	399

Table 9 below shows descriptive data for the Regulatory Compliance aspect of Digital Security. The following is a descriptive data table for Regulatory Compliance:

Table 9. Descriptive Data of Regulatory Compliance

No	Item/Statement/ Question						
		Mean	Median	Modus	Minimum	Maximum	Sum
Regulatory Compliance							
1.	AKP 1	3.55	4	3.00	2	5	380
2.	AKP 2	3.69	4	3.00	1	5	395
3.	AKP 3	3.86	4	4.00	2	5	413
4.	AKP 4	3.71	4	4.00	2	5	397
5.	AKP 5	3.76	4	4.00	1	5	402

Table 10 below provides a descriptive overview of User Education and Awareness on Digital Security. The following is a descriptive data table of User Education and Awareness:

Table 10. Descriptive Data of User Education and Awareness

ITEJ
Indonesian Technology and Education Journal
E-ISSN: 2985-8216; P-ISSN: 2985-8208
Volume 3, Number 1, February 2025
/https://doi.org/10.61255/itej

No	Item/Statement/ Question						
		Mean	Median	Modus	Minimum	Maximum	Sum
User Education and Awareness							
1.	AE 1	3.96	4	5.00	1	5	424
2.	AE 2	3.74	4	4.00	1	5	400
3.	AE 3	3.79	4	4.00	1	5	405
4.	AE 4	3.87	4	4.00	1	5	414
5.	AE 5	3.75	4	4.00	1	5	401

Based on the analysis results in Table 6 to Table 10, it was found that although the level of student awareness of digital data security is quite high, there are disparities in the mastery of various aspects. User education and awareness has the highest average (3.82), reflecting a good understanding of the importance of maintaining data security. However, data access has the lowest average (3.60), indicating that students face challenges in controlling who can access their data. Students are generally aware of the importance of aspects of data security, such as regulatory compliance, privacy controls, and digital security education. However, the low average on data access indicates the need for increased literacy regarding personal data access permission settings. This is relevant to previous research [3] which emphasizes the importance of digital education to mitigate the risk of cyber threats.

This finding indicates that students understand the dangers of cyber threats, but do not fully have the experience or practical ability to overcome real challenges, especially in terms of managing data access. This phenomenon reflects good conceptual awareness, but limited implementation.

The results of this study support the findings of Sanjaya (2024) [3] and Kairupan & Rahman (2022) [7], which show the importance of comprehensive education to improve digital security literacy. However, there is an important difference that is not addressed in both studies, which is that this study underscores the need for a more specific educational approach at the campus level to strengthen personal data access control. This includes practical training and cyber threat simulations that can help students deal with potential risks in their digital lives. Thus, this study highlights the importance of strengthening digital security education programs in educational institutions. These programs should focus not only on raising awareness, but also on practical skills to protect personal data from increasingly complex cyber threats.

CONCLUSION

This research reveals that digital data security literacy plays an important role in influencing students' awareness and behavior in protecting personal data from cyber threats. The results showed that the user education and awareness aspect had the highest score, reflecting students' good understanding of the importance of keeping personal data private. However, the data access aspect had the lowest average score, indicating the need to strengthen control over personal data access.

The findings emphasize the need for strategic measures to improve digital security education among students, including simulations of real cyber threats and hands-on curriculum. In addition, campuses also need to provide support in the form of prevention programs and more effective data protection policies. The psychological and academic impact of data security breaches should also be a major concern in these efforts.

As a follow-up to this research, several suggestions can be made:

1. Engage a wider sample of institutions in Indonesia to get a more representative picture of digital security literacy and threats at the national level.
2. Implement more varied data collection methods, such as in-depth interviews or case studies, to better understand students' individual experiences with cyber threats.
3. Improve the evaluation of campus prevention policies, including in providing digital security education, psychological support, and cyber threat simulations aimed at increasing students' readiness to face threats.

With these measures, it is hoped that students will not only have an awareness of the importance of digital data security, but also be more practically prepared to protect themselves from risks in the digital age. Further research is also needed

E-ISSN: 2985-8216; P-ISSN: 2985-8208
Volume 3, **Number 1**, February 2025
/https://doi.org/10.61255/itej

to identify the effectiveness of existing policies and programs, as well as monitor changes in students' awareness levels over time.

REFERENCES

[1] Nofri Yudi Arifin, Okta Veza, Albertus Laurensius Setyabudhi, and Atman Lucky Fernandes, "Sosialisasi Pentingnya Cyber Security untuk Menjaga Keamanan Online Studi Fakultas Teknik Informatika Universitas Ibnu Sina," *KaryaNyata*, vol. 1, no. 3, pp. 46–51, Aug. 2024, doi: 10.62951/karyanyata.v1i3.451.

[2] B. A. Saputra, E. Kurnia, M. Rahmah, and T. Sumarni, "PENERAPAN PRIVASI DAN ETIKA DI ERA DIGITAL DALAM PERLINDUNGAN DATA PRIBADI," vol. 5, no. 9, 2024.

[3] S. Sanjaya, L. R. Fitriati, M. A. Hakim, M. Y. Yasin, and S. S. Maesaroh, "Analisis Literasi Keamanan Digital Bagi Mahasiswa Universitas Pendidikan Indonesia Kampus Tasikmalaya: Tingkat Pengetahuan, Kepercayaan, dan Kewaspadaan".

[4] S. P. Berutu, "BUKU DIGITAL SECURITY".

[5] N. R. P. Chairisda, "OPTIMALISASI SATGAS CYBERPATROL POLRES BANYUMAS DALAM MENGHADAPI PEMILU 2019".

[6] H. R. Nurdin and A. A. Rahman, "PENGUKURAN TINGKAT KESADARAN KEAMANAN SIBER PADA PENGGUNA MEDIA SOSIAL DI LINGKUNGAN MAHASISWA TEKNIK INFORMATIKA UNIVERSITAS WIDYATAMA," *JUDA*, vol. 31, no. 3, p. 94, Jun. 2023, doi: 10.46930/ojsuda.v31i3.3374.

[7] V. A. Kairupan and A. A. Rahman, "ANALISIS KESADARAN CYBERSECURITY PADA PENGGUNA MEDIA SOSIAL DI KALANGAN MAHASISWA KOTA BANDUNG," *JUDA*, vol. 30, no. 1, p. 1164, Apr. 2022, doi: 10.46930/ojsuda.v30i1.3167.

[8] S. Parulian, D. A. Pratiwi, and M. C. Yustina, "Ancaman dan Solusi Serangan Siber di Indonesia".

[9] A. F. Azizi *et al.*, "Esensi Pendidikan Inspiratif," vol. 6, no. 2, 2024.

[10] A. A. Witjaksono, I. M. Hanika, and S. I. Pratiwi, "Fenomena Cyberbullying pada Mahasiswa di DKI Jakarta," vol. 2, 2021.

[11] M. Yasin, S. Garancang, and A. A. Hamzah, "Metode dan Instrumen Pengumpulan Data (Kualitatif dan Kuantitatif)," vol. 2, no. 3, 2024.

[12] M. Abduh, T. Alawiyah, G. Apriansyah, R. A. Sirodj, and M. W. Afgani, "Survey Design: Cross Sectional dalam Penelitian Kualitatif," *JPSK*, vol. 3, no. 01, pp. 31–39, Dec. 2022, doi: 10.47709/jpsk.v3i01.1955.

[13] I. P. Sesana, "Efektifitas Penggunaan Aplikasi Google Form Dalam Pelaksanaan PAT Berbasis Online Di SMKN 1 Tembuku: Effectiveness Of The Use Of Google Form Applications In The Implementation Of PAT Based Online At SMKN 1 Tembuku," *Widyadewata*, vol. 3, no. 1, pp. 1–11, Dec. 2022, doi: 10.47655/widyadewata.v3i1.4.

[14] M. Rajab and A. Eydgahi, "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education," *Computers & Security*, vol. 80, pp. 211–223, Jan. 2019, doi: 10.1016/j.cose.2018.09.016.

[15] F. Habaora, J. R. Riwukore, and T. Yustini, "Analisis Deskriptif tentang Tampilan Kinerja Aparatur Sipil Negara di Sekretariat Pemerintah Kota Kupang Nusa Tenggara Timur Indonesia," *JIEGMK*, vol. 12, no. 1, pp. 31–41, Jul. 2021, doi: 10.36982/jiegmk.v12i1.1123.