SOCIETA
Journal of Society and Change

Volume 1, Issue 1, January–June 2026

Toward a secure digital society: The influence of digital security awareness on students' personal data protection behavior

Lucia Apria[1]*, Darwis Robinson Manalu[2]

[1 2] Universitas Methodist Indonesia, Medan, Indonesia

*Corresponding Author: luciaapria@gmail.com

Submission: 26 June 2026 Revision: 9 July 2026 Accepted: 15 July 2026

Abstract

The growth of the digital society has increased technology use while simultaneously amplifying the risk of personal data breaches, yet the relationship between digital security awareness and personal data protection behavior among university students remains underexplored. This study aimed to examine the influence of digital security awareness on the personal data protection behavior of students at Universitas Methodist Indonesia. A quantitative causal-associative approach was employed involving 102 respondents selected through convenience sampling, with data collected using questionnaires and analyzed through simple linear regression. The findings revealed that digital security awareness had a positive and significant effect on personal data protection behavior ($B = 0.621$; $t = 9.876$; $p < 0.001$) and explained 49.4% of the behavioral variance ($R^2 = 0.494$). These findings highlight that strengthening digital security awareness is fundamental to fostering personal data protection behavior and provides empirical support for enhancing cybersecurity literacy initiatives within the digital society.

Keywords: Digital security awareness; Personal data protection behavior; Digital society; Cybersecurity; University students.

Abstrak

Perkembangan masyarakat digital meningkatkan intensitas penggunaan teknologi sekaligus memperbesar risiko kebocoran data pribadi. Namun, hubungan antara kesadaran keamanan digital dan perilaku perlindungan data pribadi mahasiswa masih belum banyak dikaji secara empiris. Penelitian ini bertujuan untuk menganalisis pengaruh kesadaran keamanan digital terhadap perilaku perlindungan data pribadi mahasiswa Universitas Methodist Indonesia. Penelitian ini menggunakan pendekatan kuantitatif dengan desain asosiatif kausal terhadap 102 responden yang dipilih melalui teknik *convenience sampling*. Data dikumpulkan menggunakan kuesioner dan dianalisis menggunakan regresi linear sederhana. Hasil penelitian menunjukkan bahwa kesadaran keamanan digital berpengaruh positif dan signifikan terhadap perilaku perlindungan data pribadi ($B = 0{,}621$; $t = 9{,}876$; $p < 0{,}001$), dengan kemampuan menjelaskan 49,4% variasi perilaku ($R^2 = 0{,}494$). Temuan ini menegaskan bahwa peningkatan kesadaran keamanan digital merupakan fondasi penting dalam membentuk perilaku perlindungan data pribadi serta memperkuat upaya pengembangan literasi keamanan siber di era masyarakat digital.

Kata Kunci: Kesadaran keamanan digital; Perilaku perlindungan data pribadi; Masyarakat digital; Keamanan siber; Mahasiswa.

Introduction

Digital transformation has fundamentally reshaped the ways people communicate, learn, work, and conduct financial transactions through a wide range of internet-based platforms (Kraus et al., 2021). Within higher education, university students represent one of the most active user groups of digital technologies, utilizing learning management systems, social media, digital wallets, cloud storage, and various applications that support academic activities (Cohen et al., 2022). The increasing intensity of technology use has resulted in a substantial growth in the volume of personal data stored and exchanged electronically (Shah & Khan, 2020). At the same time, the expansion of digital activities has been accompanied by a rise in cybersecurity threats, including phishing, identity theft, account misuse, and personal data breaches (Aslan et al., 2023). These developments indicate that personal data protection is no longer merely a technical concern but has become a fundamental component of building a secure, responsible, and sustainable digital society.

The growing threats to personal data security suggest that technological advancement has not been fully accompanied by adequate personal data protection behavior. Many users continue to reuse the same passwords across multiple accounts, neglect two-factor authentication, and pay insufficient attention to privacy settings when using digital services (Marky et al., 2022). This issue is particularly critical among university students, as they belong to a generation that has grown up with digital technology and engages intensively with a wide range of internet-based services. Inadequate personal data protection behavior may lead to serious consequences, including identity theft, misuse of personal information, and loss of access to digital accounts (Herath et al., 2024). Therefore, greater efforts are needed to encourage students not only to understand digital threats but also to consistently adopt appropriate personal data protection practices in their daily lives.

One of the key factors believed to shape such behavior is digital security awareness. Digital security awareness extends beyond the ability to recognize various forms of cyber threats; it also encompasses an understanding of potential risks, concern for information security, and individuals' readiness to implement protective measures when using digital technologies (Zwilling et al., 2022). The higher an individual's level of digital security awareness, the greater the likelihood of making safer decisions when managing personal data. Consequently, digital security awareness is not confined to knowledge alone but evolves into attitudes and tangible actions aimed at safeguarding personal information. This relationship provides an important foundation for understanding how personal data protection behavior is developed within the evolving digital society.

Studies examining digital security awareness and personal data protection behavior have been conducted across various groups of technology users. Mamonov and

Benbunan-Fich (2018) demonstrated that digital security awareness positively influences personal data protection behavior, enabling individuals to better anticipate cyber threats. Saritepeci et al. (2024) found that digital literacy enhances individuals' ability to recognize information security risks; however, increased knowledge does not necessarily translate into consistent personal data protection behavior. Furnell et al. (2022) reported that students in technology-related disciplines generally exhibit higher levels of security awareness than those in non-technology fields, although weaknesses remain in password management, privacy settings, and account authentication practices. Likewise, Hassandoust and Techatassanasoontorn (2020) argued that digital security awareness explains only part of personal data protection behavior, as other factors beyond awareness also play important roles. These findings suggest that the relationship between digital security awareness and personal data protection behavior requires further empirical investigation across different higher education contexts.

Based on this research gap, this study aims to examine the influence of digital security awareness on the personal data protection behavior of students at Universitas Methodist Indonesia. This study is important because university students represent a population with intensive digital technology usage while simultaneously facing increasing threats to personal information security. Unlike previous studies, which have primarily focused on general levels of digital awareness or digital literacy, the present study specifically investigates the direct relationship between digital security awareness and personal data protection behavior using simple linear regression analysis. The findings are expected to provide empirical evidence that enriches the literature on digital security in higher education while offering a practical foundation for universities to design educational programs that foster sustainable personal data protection behavior in the era of the digital society.

Method

This study employed a quantitative approach with a causal-associative research design to examine the influence of digital security awareness on university students' personal data protection behavior (Creswell, 2014). The study was conducted at Universitas Methodist Indonesia during the 2025/2026 academic year, with all enrolled undergraduate students constituting the target population. A total of 102 respondents were selected using a non-probability sampling technique through convenience sampling. Data were collected using an online questionnaire administered via Google Forms. In this study, digital security awareness (X) served as the independent variable, while personal data protection behavior (Y) was the dependent variable.

The research instrument consisted of a questionnaire employing a five-point Likert scale (1 = strongly disagree to 5 = strongly agree), comprising 10 statements, with five items measuring each variable. The instrument was adapted from the *Human Aspects*

of Information Security Questionnaire (HAIS-Q) developed by Parsons et al. (2014). Digital security awareness was measured using indicators including the ability to recognize suspicious messages or links, understanding the risks of personal data breaches, knowledge of account security practices, awareness of the importance of personal data protection, and attentiveness to information regarding data breach incidents. Meanwhile, personal data protection behavior was assessed through the use of unique passwords for important accounts, activation of two-factor authentication (2FA), management of social media privacy settings, verification of message senders before opening links, and caution when sharing personal information.

Data were analyzed using IBM SPSS Statistics version 22. The initial stage involved assessing instrument quality through validity testing using the Product Moment correlation and reliability testing using Cronbach's alpha. Assumption testing was subsequently conducted, including the Kolmogorov–Smirnov normality test and the linearity test, before hypothesis testing. The research hypothesis was examined using simple linear regression based on the equation $Y = a + bX$. The statistical significance of the effect of the independent variable on the dependent variable was evaluated using the *t*-test, while the coefficient of determination (R^2) was used to determine the extent to which digital security awareness explained the variation in university students' personal data protection behavior (Ghozali, 2006).

Results and Discussion

Respondent characteristics and preliminary assumption tests

This study involved 102 active students at Universitas Methodist Indonesia from various study programs and academic semesters. The respondent characteristics are presented to illustrate the composition of the sample and demonstrate that the study included students from diverse academic backgrounds. This diversity is important because the use of digital technologies is not limited to students in information technology disciplines but also extends to those from other fields of study. The distribution of respondents by study program and semester is presented in Table 1. This information provides important context for interpreting the findings, as respondent characteristics may influence both the level of digital security awareness and the personal data protection behavior observed throughout the study.

Table 1. Respondent characteristics

Characteristic	Category	n	%
Study program	Information Systems	51	50.0
	Informatics Engineering	31	30.4
	Accounting	7	6.9
	Management	4	3.9

	Agrotechnology	3	2.9
	Information Technology Education	3	2.9
	Agribusiness	2	2.0
	English Literature	1	1.0
Semester	Semester 2	20	19.6
	Semester 4	16	15.7
	Semester 6	50	49.0
	Semester 8	16	15.7

Source: Processed research data (2026).

As shown in Table 1, most respondents were enrolled in the Information Systems program (51 students, 50.0%), followed by Informatics Engineering (31 students, 30.4%), while the remaining respondents were distributed across six other study programs with smaller proportions. In terms of academic level, nearly half of the respondents were in Semester 6 (49.0%), followed by Semester 2 (19.6%), whereas Semester 4 and Semester 8 each accounted for 15.7% of the sample. This composition indicates that most respondents had substantial experience using various digital services in both academic and everyday contexts. Therefore, their responses are expected to reflect real-world experiences in managing account security, maintaining privacy, and protecting personal data, making the collected data highly relevant to the objectives of this study.

Before testing the research hypothesis, the measurement instrument had to meet established quality standards to ensure the reliability of the collected data. Therefore, validity testing was conducted to verify that each questionnaire item adequately measured the intended construct, while reliability testing was performed to assess the internal consistency of respondents' answers. A summary of these instrument quality assessments is presented in Table 2. An instrument that satisfies both validity and reliability requirements indicates that each indicator appropriately measures its corresponding variable and consistently captures the intended construct. Having established the quality of the instrument, the subsequent statistical analyses could be conducted with confidence in the adequacy of the measurement tool.

Table 2. Instrument quality test results

Variable	**Number of Items**	**Range of Calculated *r***	**Cronbach's Alpha**	**Interpretation**
Digital security awareness	5	0.649–0.790	0.768	Valid and reliable
Personal data protection behavior	5	0.520–0.728	0.699	Valid and reliable

Source: Processed using IBM SPSS Statistics 22 (2026).

The results presented in Table 2 indicate that all questionnaire items exceeded the minimum correlation threshold of 0.30, confirming that every indicator was statistically valid. This finding demonstrates that each questionnaire item effectively represented the constructs of digital security awareness and personal data protection behavior in accordance with the intended measurement objectives. Furthermore, Cronbach's alpha coefficients of 0.768 for digital security awareness and 0.699 for personal data protection behavior indicate satisfactory internal consistency for both variables. Accordingly, the research instrument demonstrated adequate measurement quality, and the resulting data were considered suitable for regression analysis to examine the relationship between the two study variables.

The next stage involved testing the preliminary assumptions of the regression model through normality and linearity tests, as presented in Table 3. Normality was assessed using the Kolmogorov–Smirnov test on the regression residuals to determine whether they followed a normal distribution. Meanwhile, the linearity test was conducted to examine whether the relationship between digital security awareness and personal data protection behavior followed a linear pattern, thereby justifying the application of simple linear regression analysis. These assumption tests are essential because the validity of the regression model depends on the extent to which these underlying assumptions are satisfied.

Table 3. Preliminary assumption test results

Test	Value	Sig.	Interpretation
Normality (Kolmogorov–Smirnov)	–	0.200	Residuals are normally distributed
Linearity	124.774	0.000	Significant linear relationship
Deviation from Linearity	2.862	0.001	Significant deviation from linearity

Source: Processed using IBM SPSS Statistics 22 (2026).

As presented in Table 3, the normality test produced a significance value of 0.200 (> 0.05), indicating that the residuals were normally distributed. This result confirms that one of the fundamental assumptions of regression analysis was satisfied. Furthermore, the linearity test yielded a significance value of 0.000 for the Linearity component, indicating a statistically significant linear relationship between digital security awareness and personal data protection behavior. However, the significance value for the Deviation from Linearity component was 0.001, suggesting the presence of a statistically significant departure from an ideal linear relationship. Therefore, the results of the linearity test should be interpreted with caution when evaluating the regression model.

Overall, the respondent characteristics indicate that the study was dominated by students with substantial experience in using digital technologies, while the instrument quality assessment confirmed that all indicators satisfied the required

validity and reliability criteria. Moreover, the preliminary assumption tests demonstrated that the residuals were normally distributed and that the relationship between the variables generally followed a linear pattern, although a significant deviation from linearity was also identified and should be taken into consideration when interpreting the findings. Having satisfied most of the required analytical assumptions, the study proceeded to simple linear regression analysis to examine the influence of digital security awareness on university students' personal data protection behavior.

Regression analysis and hypothesis testing

Simple linear regression analysis was conducted to examine the influence of digital security awareness on the personal data protection behavior of students at Universitas Methodist Indonesia. This analysis aimed to determine the direction, magnitude, and statistical significance of the relationship between the independent and dependent variables. In addition, hypothesis testing was performed using the *t*-test to determine whether the observed effect was statistically significant. A summary of the regression analysis is presented in Table 4. These results indicate whether an increase in digital security awareness is accompanied by an improvement in personal data protection behavior, as proposed in the research hypothesis. Therefore, the regression analysis serves as the primary basis for addressing the research objectives established at the outset of the study.

Table 4. Simple linear regression analysis results

Variable	**B**	***t***	**Sig.**
Constant	8.302	6.825	0.000
Digital security awareness	0.621	9.876	0.000

Source: Processed using IBM SPSS Statistics 22 (2026).

As presented in Table 4, the regression equation was $Y = 8.302 + 0.621X$. The regression coefficient of 0.621 indicates that each one-unit increase in digital security awareness is associated with a 0.621-unit increase in personal data protection behavior, assuming all other factors remain constant. The positive coefficient confirms a positive relationship between the two variables, indicating that higher levels of digital security awareness are associated with better personal data protection behavior among university students. Furthermore, the *t*-test yielded a value of 9.876 with a significance level of 0.000 (< 0.05). These findings demonstrate that digital security awareness has a positive and statistically significant effect on personal data protection behavior. Therefore, the alternative hypothesis (H_1) was accepted, while the null hypothesis (H_0) was rejected.

To determine the explanatory power of the independent variable in predicting the dependent variable, the coefficient of determination (R^2) was calculated. The results

are presented in Table 5. This analysis provides information regarding the proportion of variance in personal data protection behavior explained by digital security awareness through the proposed regression model. A higher coefficient of determination indicates a greater contribution of the independent variable in explaining changes in the dependent variable. Conversely, the unexplained proportion suggests the presence of additional factors outside the scope of the present study that may also influence university students' personal data protection behavior.

Table 5. Hypothesis testing and coefficient of determination results

Model	*R*	*R* Square	Adjusted *R* Square	Decision
1	0.703	0.494	0.489	H_1 accepted

Source: Processed using IBM SPSS Statistics 22 (2026).

As shown in Table 5, the correlation coefficient (*R*) of 0.703 indicates a strong positive relationship between digital security awareness and personal data protection behavior. Meanwhile, the *R* Square value of 0.494 indicates that digital security awareness accounts for 49.4% of the variance in university students' personal data protection behavior. The remaining 50.6% is attributable to factors beyond the scope of the present model, such as digital literacy, previous experience with cyber threats, patterns of technology use, and social environmental influences. Overall, the regression analysis and hypothesis testing demonstrate that digital security awareness is a key factor influencing students' personal data protection behavior. These findings provide the foundation for the subsequent discussion by linking the empirical results with the theoretical framework and previous research findings.

The influence of digital security awareness on university students' personal data protection behavior

Digital transformation has fundamentally reshaped students' academic activities, ranging from learning processes to the online management of personal data. However, the increasing intensity of technology use has not always been accompanied by stronger personal data protection behavior. Although many students recognize the importance of digital security, they continue to overlook essential security practices, such as using strong passwords, enabling two-factor authentication, and configuring account privacy settings appropriately. This raises an important question as to whether digital security awareness genuinely translates into improved personal data protection behavior. The findings of this study demonstrate that digital security awareness has a positive and statistically significant influence on students' personal data protection behavior, with a regression coefficient of 0.621, $t = 9.876$, a significance level of 0.000, and a coefficient of determination of 49.4%. These findings indicate that digital security awareness is a key determinant of students' personal data protection behavior, although it is not the sole factor influencing such behavior.

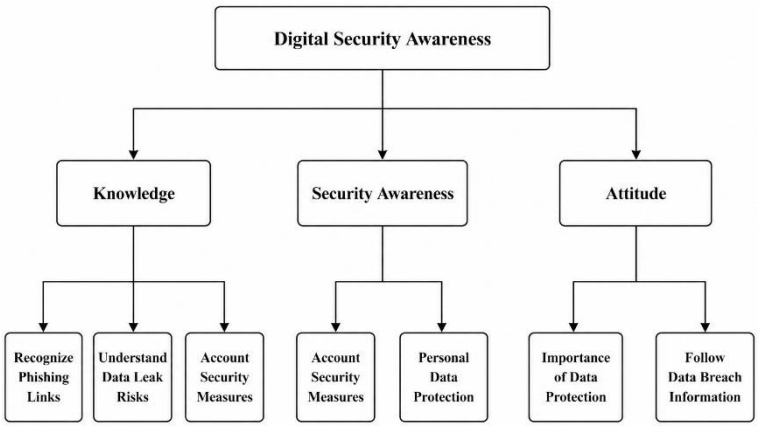

Figure 1. Conceptual interpretation of the influence of digital security awareness on personal data protection behavior

Source: Developed by the authors based on the findings of this study (2026).

Figure 1 was developed to illustrate the conceptual mechanism underlying the relationship between digital security awareness and personal data protection behavior. Although the regression analysis confirmed a statistically significant relationship, the statistical results alone do not explain how this influence is formed. Therefore, Figure 1 integrates the findings of this study into three core components—knowledge, security awareness, and attitude—which collectively constitute digital security awareness. These components subsequently influence how students make decisions when interacting with digital services, ultimately shaping their personal data protection behavior. Accordingly, the figure serves as an interpretive framework that links the empirical findings with the underlying conceptual mechanism.

The first component underlying digital security awareness is knowledge. The regression analysis produced a coefficient of 0.621 with a *t* value of 9.876 and a significance level of 0.000, confirming that higher levels of digital security awareness are associated with stronger personal data protection behavior. These findings suggest that students who are able to recognize phishing links, understand the risks of personal data breaches, and possess knowledge of account security practices are more likely to engage in appropriate personal data protection behavior. Such knowledge provides the foundation for evaluating potential risks before making decisions when using digital services. These findings are consistent with those of Maalem Lahcen et al. (2020), who concluded that an understanding of cyber threats constitutes the initial factor shaping information security behavior. Similarly, Ogbodo et al. (2025) demonstrated that the ability to recognize digital risks enhances individuals' preparedness to adopt personal data protection practices. Therefore, the findings of the present study reinforce the view that knowledge is the primary foundation for developing digital security awareness.

Beyond knowledge, security awareness transforms understanding into vigilance toward a wide range of digital threats. This is reflected in the *R* Square value of 0.494,

indicating that digital security awareness explains 49.4% of the variation in students' personal data protection behavior. This represents a substantial contribution for behavioral research, suggesting that awareness extends beyond theoretical understanding to influence how students secure their accounts, protect personal information, and evaluate potential risks before engaging with digital platforms. Nevertheless, the remaining 50.6% of the behavioral variation is explained by factors outside the proposed model, such as digital literacy, previous experience with cybersecurity incidents, and social environmental influences. These findings support the conclusions of Alqarni (2025), who identified digital security awareness as an important predictor of data protection behavior. However, unlike Hrp and Guntur Utomo (2025), who reported a greater explanatory contribution, the present findings suggest that although digital security awareness exerts a strong influence, additional factors are necessary to foster optimal personal data protection behavior.

The final component is attitude, which refers to students' tendency to regard personal data protection as an integral part of their everyday digital practices. The positive relationship between the two variables, reflected by the correlation coefficient (R) of 0.703, indicates that more positive attitudes toward digital security are associated with stronger personal data protection behavior. These attitudes are reflected in practices such as using unique passwords for important accounts, enabling two-factor authentication, verifying the sources of links before opening them, configuring social media privacy settings, and exercising greater caution when sharing personal information. Thus, digital security awareness extends beyond knowledge and develops into a commitment expressed through concrete protective actions in everyday digital activities. These findings are consistent with Pollini et al. (2022), who argued that attitudes play a crucial role in shaping information security behavior. Conversely, Hong and Furnell (2021) found that positive attitudes do not necessarily lead to consistent security behavior unless they are reinforced through continuous digital security practices. The present study demonstrates that attitude makes a meaningful contribution to the development of students' personal data protection behavior.

Overall, Figure 1 illustrates that the influence of digital security awareness on personal data protection behavior is established through the interaction of knowledge, security awareness, and attitude. These three components complement one another in shaping how students understand digital threats, assess potential risks, and make decisions when interacting with digital technologies. These findings are consistent with the regression analysis, which demonstrated a positive and statistically significant effect, with digital security awareness explaining 49.4% of the variance in personal data protection behavior. This confirms that digital security awareness constitutes a fundamental basis for fostering students' personal data protection behavior. Nevertheless, 50.6% of the behavioral variation remains attributable to factors beyond

the scope of the present model. Therefore, Figure 1 serves not only as a conceptual synthesis of the empirical findings but also as a framework for future research aimed at identifying additional factors that contribute to the development of personal data protection behavior within higher education institutions.

Conclusion

This study demonstrates that digital security awareness has a positive and statistically significant influence on the personal data protection behavior of students at Universitas Methodist Indonesia. The regression analysis produced the equation $Y = 8.302 + 0.621X$, with a t value of 9.876, a significance level of 0.000, and an R^2 value of 0.494, indicating that digital security awareness explains 49.4% of the variance in students' personal data protection behavior. These findings confirm that greater knowledge of cyber threats, heightened awareness of digital security risks, and positive attitudes toward the importance of data protection encourage students to adopt safer practices, such as using strong passwords, enabling two-factor authentication, verifying the source of links before accessing them, and exercising greater caution when sharing personal information. In the context of a digital society that is increasingly dependent on technology and data-driven services, digital security awareness is no longer merely an additional competency but has evolved into a fundamental competency that determines individuals' ability to safeguard the security and privacy of their personal data.

This study contributes empirically by strengthening the understanding of the mechanisms through which knowledge, security awareness, and attitude interact to shape university students' personal data protection behavior. It also demonstrates that digital security awareness is a critical factor in fostering a culture of information security within higher education institutions. Nevertheless, the proposed model explains only 49.4% of the variance in personal data protection behavior, indicating that the remaining 50.6% is influenced by factors beyond the scope of the present study, such as digital literacy, previous experience with cyber incidents, self-efficacy, and social environmental influences. Furthermore, the use of convenience sampling within a single higher education institution limits the generalizability of the findings. Therefore, future research is encouraged to include respondents from a broader range of institutions and geographical regions, employ more representative sampling techniques, and expand the research model by incorporating additional explanatory variables to develop a more comprehensive understanding of personal data protection behavior in the era of the digital society.

References

Alqarni, A. (2025). The relationship between cybersecurity awareness and data protection behaviors among Saudi secondary school students: The mediating role of cyber threat perception and the moderating role of internet usage duration.

Humanities and Social Sciences Communications, *12*(1), 1837. https://doi.org/10.1057/s41599-025-06122-x

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333. https://doi.org/10.3390/electronics12061333

Cohen, A., Soffer, T., & Henderson, M. (2022). Students' use of technology and their perceptions of its usefulness in higher education: International comparison. *Journal of Computer Assisted Learning*, *38*(5), 1321–1331. https://doi.org/10.1111/jcal.12678

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage Publications.

Furnell, S., Langner, G., Tokola, T., Andriessen, J., Quirchmayr, G., & Luciano, C. (2022). Collaborative cybersecurity learning: Establishing educator and learner expectations and requirements (pp. 46–59). https://doi.org/10.1007/978-3-031-08172-9_4

Ghozali, I. (2006). *Aplikasi analisis multivariate dengan program SPSS*. Badan Penerbit Universitas Diponegoro.

Hassandoust, F., & Techatassanasoontorn, A. A. (2020). Understanding users' information security awareness and intentions. In *Cyber influence and cognitive threats* (pp. 129–143). Elsevier. https://doi.org/10.1016/B978-0-12-819204-7.00007-5

Herath, H. M. S. S., Herath, H. M. K. K. M. B., Madhusanka, B. G. D. A., & Guruge, L. G. P. K. (2024). Data protection challenges in the processing of sensitive data. In *Data protection* (pp. 155–179). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-76473-8_8

Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, *57*, 102710. https://doi.org/10.1016/j.jisa.2020.102710

Hrp, T. A. S., & Guntur Utomo, R. (2025). Assessing the impact of information security and privacy awareness on privacy protection behavior among college students: A structural equation modeling approach. *2025 International Conference on Data Science and Its Applications (ICoDSA)*, 127–132. https://doi.org/10.1109/ICoDSA67155.2025.11157025

Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital transformation: An overview of the current state of the art of research. *Sage Open*, *11*(3). https://doi.org/10.1177/21582440211047576

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(1), 10. https://doi.org/10.1186/s42400-020-00050-w

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32–44. https://doi.org/10.1016/j.chb.2018.01.028

Marky, K., Ragozin, K., Chernyshov, G., Matviienko, A., Schmitz, M., Mühlhäuser, M., Eghtebas, C., & Kunze, K. (2022). "Nah, it's just annoying!" A deep dive into user perceptions of two-factor authentication. *ACM Transactions on Computer-Human Interaction*, *29*(5), 1–32. https://doi.org/10.1145/3503514

Ogbodo, D. C., Awan, I.-U., Cullen, A., & Zahrah, F. (2025). From regulation to reality: A framework to bridge the gap in digital health data protection. *Electronics*, *14*(13), 2629. https://doi.org/10.3390/electronics14132629

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Saritepeci, M., Yildiz Durak, H., Özüdoğru, G., & Atman Uslu, N. (2024). The role of digital literacy and digital data security awareness in online privacy concerns: A multi-group analysis with gender. *Online Information Review*, *48*(5), 983–1001. https://doi.org/10.1108/OIR-03-2023-0122

Shah, S. M., & Khan, R. A. (2020). Secondary use of electronic health record: Opportunities and challenges. *IEEE Access*, *8*, 136947–136965. https://doi.org/10.1109/ACCESS.2020.3011099

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