KALBISocio Jurnal Bisnis dan Komunikasi *Kalbisocio, Jurnal Bisnis & Komunikasi, Vol. 12, No. 3, September 2025, E-ISSN 2829-1301*

Comparative Analysis Of Digital Literacy Effects On Cybercrime Awareness: Evidence From Gen Y And Z

Aris Subagio[1)], Rahmad Syalevi[2)], Suhendra Saputra Jaya[3)]

[1,3)]Ilmu Komunikasi, Fakultas Falsafah dan Peradaban, Universitas Paramadina
Email Korespondensi: aris.subagio@paramadina.ac.id
Email: suhendra.jaya@students.paramadina.ac.id
[2)]Teknik Informatika, Fakultas Ilmu Rekayasa, Universitas Paramadina
Jl. Raya Mabes Hankam Kav 9,Setu, Cipayung, Jakarta Timur, 13880
Email: rahmad.syalevi@paramadina.ac.id

Abstract: *This study aims to examine the influence of digital literacy and its dimensions- technical, cognitive, and social-emotional - on cybercrime awareness among university students, with a comparison between Generation Y and Generation Z. Adopting a quantitative approach, data were collected from 108 respondents through an online questionnaire using purposive sampling. Regression analysis revealed that all dimensions of digital literacy significantly affect cybercrime awareness, with the technical dimension having the most substantial impact. The generational comparison revealed that digital literacy had a significant influence on Generation Z, but no significant effect on Generation Y. These findings underscore the importance of adopting a multidimensional and generation-responsive approach to developing digital literacy and enhancing cybersecurity awareness.*
Keywords: *digital literacy, cybercrime, social media, generation Z, generation Y*

Abstrak: Penelitian ini bertujuan untuk mengkaji pengaruh literasi digital dan dimensi-dimensinya—teknis, kognitif, dan sosial-emosional—terhadap kesadaran kejahatan siber di kalangan mahasiswa, dengan perbandingan antara Generasi Y dan Generasi Z. Dengan menggunakan pendekatan kuantitatif, data dikumpulkan dari 108 responden melalui kuesioner daring menggunakan purposive sampling. Analisis regresi menunjukkan bahwa semua dimensi literasi digital secara signifikan memengaruhi kesadaran kejahatan siber, dengan dimensi teknis memiliki dampak paling substansial. Perbandingan antar generasi menunjukkan bahwa literasi digital memiliki pengaruh yang signifikan terhadap Generasi Z, tetapi tidak berpengaruh signifikan terhadap Generasi Y. Temuan ini menggarisbawahi pentingnya mengadopsi pendekatan multidimensi dan responsif terhadap generasi untuk mengembangkan literasi digital dan meningkatkan kesadaran keamanan siber.
Kata kunci: literasi digital, kejahatan siber, media sosial, generasi Z, generasi Y

I. INTRODUCTION

The swift evolution of digital technologies has profoundly reshaped various aspects of human life, influencing how people communicate, retrieve information, work, and engage socially. Social media has emerged as a hallmark of this digital era, offering unparalleled convenience in networking and real-time information sharing. Recent data indicate that in 2024, Indonesia recorded over 167 million active social media users, positioning it among the nations with the highest global social media penetration (Ramadhany et al., 2025).

The Digital 2025: Indonesia report published by DataReportal and We Are Social reveals that 91.7% of internet users aged 16–64 in Indonesia use WhatsApp, making it the most popular social media platform in the country, followed by Instagram (84.6%), Facebook (83.0%), TikTok (77.4%), and Telegram (61.6%). Other platforms such as Messenger (50.5%), X/Twitter (50.3%), and Pinterest (33.6%) also contribute significantly to the Indonesian digital ecosystem (DataReportal, 2025).

While social media offers numerous advantages, its rapid growth has also introduced significant challenges, particularly the escalation of cybercrime. Threats on social media platforms include phishing, online scams, account takeovers, malware infections, and unauthorized data exploitation. These threats underscore that digital literacy today goes far beyond technical abilities and requires critical

comprehension, heightened security awareness, and ethical conduct in online contexts (Rodríguez-de-Dios et al., 2016).

Digital literacy encompasses a range of knowledge, skills, and attitudes that enable individuals to utilize digital technology safely, effectively, and critically (Ng, 2012). Specifically, in social media contexts, digital literacy encompasses the skills to assess information validity, secure personal data, detect cyber risks, and understand the legal and ethical implications of online behavior. Research suggests that, although younger groups are widely regarded as digital natives, many remain highly vulnerable to various forms of cybercrime (Wilson, 2024).

Generational groups, such as Millennials or Generation Y (1981–1996) and Generation Z (1997–2012), each possess distinct digital backgrounds and characteristics. Millennials matured during the internet's expansion and became early adopters of social media. Meanwhile, Generation Z grew up in an entirely digital environment, making them highly adaptive to technological innovations (Rahardyan et al., 2023).

Nevertheless, recent findings show that frequent social media or internet usage does not necessarily equate to strong digital literacy. Many in Generation Z appear to be more susceptible to manipulation, phishing schemes, and social engineering due to their excessive trust in online content and inadequate information verification skills (Rodríguez-de-Dios et al., 2016; Umeugo, 2023). Wilson (2024) also revealed that numerous Generation Z employees require additional training to enhance their digital literacy, thereby ensuring safer and more efficient performance in digital workspaces.

In Indonesia, a series of recent cyber incidents highlights the urgent need to enhance digital literacy. A prominent example is the ransomware attack on the Temporary National Data Center (PDNS) 2 in June 2024, which severely disrupted public services and resulted in the leakage of sensitive data (CNN Indonesia, 2024). Another significant breach affected Bank Syariah Indonesia (BSI), where approximately 1.5 terabytes of customer data—impacting about 15 million people—were exposed online. Likewise, major e-commerce platforms such as Tokopedia, Bukalapak, and Lazada have faced similar breaches, further highlighting the fragility of Indonesia's cybersecurity infrastructure (Ramadhany et al., 2025).

Furthermore, in May 2025, Indonesia's Ministry of Communication and Digital Affairs temporarily suspended Worldcoin (rebranded "World") and WorldID operations due to the unauthorized collection of iris biometric data, violations of electronic system provider regulations, and public concerns over transparency (Komdigi). This case highlights that the misuse of emerging digital identity tools can erode public trust and exacerbate cyber risks.

Additionally, the National Cyber and Crypto Agency (BSSN) documented over 403 million anomalous traffic incidents in 2024, revealing the magnitude of cyber threats in Indonesia. High social media penetration, coupled with inadequate digital literacy, raises users' vulnerability to cybercrime. A recent survey found that more than 60% of Indonesians lack a comprehensive understanding of how to protect personal data on social media and often share sensitive information publicly (Ramadhany et al., 2025).

Considering these realities, advancing digital literacy is crucial as a proactive measure to mitigate cybercrime risks, particularly on social media. Digital literacy equips individuals with critical thinking skills, risk identification capabilities, and the initiative to secure their digital data. Moreover, it helps build psychological resilience against manipulation and disinformation, which have become increasingly common on social media platforms (Tomczyk & Eger, 2020).

Therefore, this study aims to investigate and analyze the role of digital literacy as a pivotal factor in enhancing

cybercrime awareness on social media, with a specific focus on generational differences between Generation Y and Generation Z in Indonesia. Accordingly, the study seeks to achieve the following objectives:

1. To analyze the overall effect of digital literacy on cybercrime awareness.
2. To analyze the influence of the technical dimension of digital literacy on cybercrime awareness.
3. To analyze the effect of the cognitive dimension of digital literacy on cybercrime awareness.
4. To analyze the impact of the social-emotional dimension of digital literacy on cybercrime awareness.

To compare the influence of digital literacy on cybercrime awareness between Generation Y and Generation Z.

II. RESEARCH METHOD

A. Literature Review

1. Digital Literacy

The concept of digital literacy has evolved significantly over the past two decades, moving beyond basic technical skills to encompass a complex set of abilities necessary to function effectively in a digitally saturated society. Digital literacy encompasses a blend of technical, cognitive, and socio-emotional skills that equip individuals to engage with digital technologies in a safe, effective, and ethically responsible way (Ng, 2012).

1. Cybercrime Awareness

Cybercrime awareness refers to the level of understanding, perception, and knowledge individuals possess about online threats, as well as their ability to identify, avoid, and mitigate risks during their digital activities (Arpaci & Aslan, 2023). Cybercrime includes a broad spectrum of illegal acts such as phishing, identity theft, data breaches, scams, cyberbullying, and ransomware attacks.

According to Umeugo (2023), the lack of adequate cybercrime awareness is a significant contributing factor to individuals becoming victims in online spaces. The rapid growth of social media use has expanded the pool of targets for cybercriminals, making awareness an essential line of defense.

Additionally, cybercrime awareness is dynamic; it evolves continuously as new cyber threats and technological changes arise. For this reason, constant learning and adaptation are critical to maintaining adequate levels of protection. Increasingly, scholars and policymakers recommend embedding cybercrime awareness within broader digital literacy education frameworks.

2. Generational Differences in Digital Behavior

The theory of generational cohorts suggests that individuals born during similar time frames share everyday experiences, values, and exposure to technology, which shape their behaviors and attitudes (Rahardyan et al., 2023). In the sphere of digital technology and social media, these generational differences significantly influence how people consume content, assess online risks, and manage their digital identities.

3. Social Media and Cybercrime

Platforms like Facebook, Instagram, Twitter, and TikTok have become deeply ingrained in everyday routines, particularly for younger generations. These platforms enable widespread information exchange, social networking, and community building. However, they also create ample opportunities for cybercriminal activities.

Existing research shows that social media users are especially susceptible to threats like phishing, online fraud, and identity theft due to the personal details they frequently share publicly (Tomczyk & Eger, 2020). Cybercriminals can exploit this publicly available data to tailor personalized attacks, thereby increasing their chances of success.

In light of the theoretical framework and previous empirical studies, this research aims to investigate the impact of digital literacy on individuals' awareness of cybercrime. Considering that digital literacy encompasses multiple dimensions—technical, cognitive, and social-emotional—this study aims to

explore both the overall and dimensional impacts of digital literacy on awareness of cybercrime. Moreover, the role of generational differences is considered by comparing the effects across Generation Y and Generation Z. The following hypotheses are proposed:

H_1 : Digital literacy significantly influences cybercrime awareness.
H_{1a} : The technical dimension of digital literacy significantly influences cybercrime awareness.
H_{1b} : The cognitive dimension of digital literacy significantly influences cybercrime awareness.
H_{1c} : The social-emotional dimension of digital literacy significantly. influences cybercrime awareness.
H_2 : There is a difference in the effect of digital literacy on cybercrime awareness between Generation Y and Generation Z.

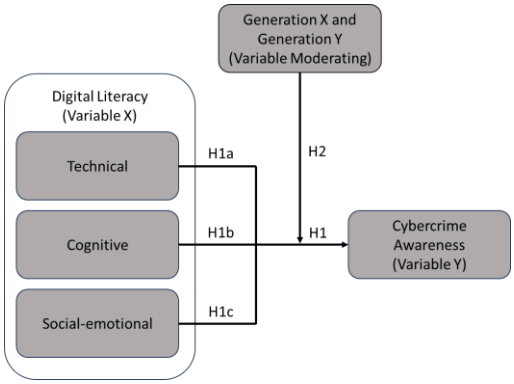

Figure 1: Theoretical Framework
Source: Processed by researchers

B. Data Collection Method

This study utilized purposive sampling, focusing on students at Universitas Paramadina. Data were gathered through an online questionnaire distributed via Google Forms during the research period from June to July 2025. A total of 108 valid responses were collected.

III. RESULTS AND DISCUSSION

The mean analysis, as shown in Table 1, reveals varying levels of respondent perception across the dimensions and indicators of the studied variables. Within the Digital Literacy variable, the Cognitive dimension recorded the highest average score (4.10), reflecting respondents' confidence in their ability to process and understand digital information. In contrast, the Social-Emotional dimension received the lowest mean score (3.81), indicating that respondents may place less emphasis on emotional and social competencies in digital environments.

Within the Technical dimension, the indicator "I can easily learn new technologies" (X_{12}) achieved the highest mean score of 4.23, showing that respondents strongly recognize adaptability to new digital tools. Meanwhile, the indicator "I have good ICT skills to secure my social media account" (X_{15}) received the lowest in this dimension, with a mean of 3.82, indicating a potential gap in cybersecurity practices.

In the Social-Emotional dimension, the indicator "I often seek help through online communication to solve technical issues" (X_{31}) recorded the lowest mean (3.32). At the same time, "I understand critical digital issues such as cyber security and fake news" (X_{32}) reached the highest mean (4.29), showing that although awareness exists, confidence in social interaction via digital tools remains relatively low.

Table 1. Mean Test Results

Dimension	Indicator	Mean	Mean Dimension	Mean Variable
Digital Literacy (X)				
Technical (X_1)	X_{11}	4.09		
	X_{12}	**4.23**		
	X_{13}	4.07	4.05	
	X_{14}	4.19		4.01
	X_{15}	**3.82**		
	X_{16}	3.90		
Cognitive (X_2)	X_{21}	**4.10**	**4.10**	
	X_{22}	**4.10**		
Social-emotional (X_3)	X_{31}	**3.32**	**3.81**	
	X_{32}	**4.29**		
Cybercrime Awa	Y_1	**4.87**		
	Y_2	4.81		
	Y_3	4.61		
	Y_4	4.66		
	Y_5	4.78		
	Y_6	**4.19**		
	Y_7	4.72		
	Y_8	4.70		
	Y_9	4.81		
	Y_{10}	4.57		
	Y_{11}	4.44	**4.60**	**4.60**
	Y_{12}	4.40		
	Y_{13}	4.44		
	Y_{14}	4.43		
	Y_{15}	4.74		
	Y_{16}	4.70		
	Y_{17}	4.63		
	Y_{18}	4.29		
	Y_{19}	4.68		
	Y_{20}	4.56		
	Y_{21}	4.68		
	Y_{22}	4.40		

Source: Processed by researchers with SPSS 23, 2025

Turning to the Cybercrime Awareness variable, the overall mean score was relatively high (4.60), reflecting strong awareness among respondents regarding digital threats. Among the 22 indicators, the item "I am aware of the risk of cybercrime when using social media" (Y_1) achieved the highest mean (4.87), indicating strong baseline awareness. Other indicators such as "Sharing personal data with third parties without the owner's knowledge is a crime" (Y_2), "I know that posting support for terrorist organizations on social media is a criminal act" (Y_5), and "Conducting illegal gambling/betting activities on social media is a crime" (Y_9) also scored above 4.70. On the other hand, indicators such as "Posting unverified political or military content on social media is a legal violation" (Y_6) (mean = 4.19), "Sharing violent images on social media is a crime" (Y_{18}) (mean = 4.29), and "Sharing unlicensed software on social media is a legal offense" (Y_{22}) (mean = 4.40) showed comparatively lower perceptions, which may point to areas where digital crime prevention messaging could be improved.

These descriptive results not only highlight the dimensions that are perceived positively but also reveal areas requiring further attention.

Table 2. Correlation Between Digital Literacy and Cybercrime Awareness

		Digital Literacy	Cybercrime Awareness
Digital Literacy	Pearson Correlation	1	.271**
	Sig. (2-tailed)		.005
	N	108	108
Cybercrime Awareness	Pearson Correlation	.271**	1
	Sig. (2-tailed)	.005	
	N	108	108

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Processed by researchers with SPSS 23, 2025

The Pearson correlation test yielded a coefficient value of 0.271, with a significance level of $p = 0.005$ ($p < 0.01$), as shown in Table 2. This result indicates a positive and statistically significant relationship between overall Digital Literacy (X) and Cybercrime Awareness (Y) scores. While the correlation is categorized as weak, it remains meaningful in suggesting that as individuals' digital literacy improves, so does their level of awareness regarding cybercrime.

This finding supports the argument that digital literacy—comprising technical, cognitive, and social-emotional competencies—plays a foundational role in helping individuals identify, interpret, and respond to various forms of online threats. Although the effect size is modest, it highlights the potential of even basic improvements in digital literacy to enhance one's vigilance against cybercrime.

Table 3. Determination Coefficient of the Digital Literacy Variable on Cybercrime Awareness

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	76.739	8.440		9.092	.000
	Digital Literacy	.607	.209	.271	2.900	.005

a. Dependent Variable: Cybercrime Awareness

Source: Processed by researchers using SPSS version 23, 2025

The results of the data analysis show that the unstandardized regression coefficient (B) for the Digital Literacy variable is 0.607, with a standard error of 0.209, and a standardized coefficient (Beta) of 0.271. The t-value is 2.900, and the significance level is 0.005. The result indicates that Digital Literacy has a significant influence on Cybercrime Awareness, as presented in Table 3.

To test the influence of the independent variable on the dependent variable, a t-test was conducted. The hypothesis tested in this study is as follows:

H_1: Digital literacy significantly influences cybercrime awareness.

Based on the distribution table with a significance level (α) of 5%, the critical t-value is approximately 1.982. Since the calculated t-value (2.900) is greater than the t-table value and the significance level is less than 0.05 (p = 0.005), the hypothesis is accepted. Therefore, it can be concluded that Digital Literacy has a statistically significant influence on Cybercrime Awareness.

Furthermore, the constant value in the regression model is 76.739, representing the predicted value of Cybercrime Awareness when Digital Literacy equals zero. Thus, the simple linear regression equation can be estimated as follows:

$$Y = 76.739 + 0.607X$$

where Y is Cybercrime Awareness and X is Digital Literacy. This result implies that for every one-unit increase in Digital Literacy, Cybercrime Awareness increases by 0.607 units, assuming other factors remain constant.

Table 4. Correlation Between the Technical Dimension of Digital Literacy and Cybercrime Awareness

		Technical	Cybercrime Awareness
Technical	Pearson Correlation	1	.221*
	Sig. (2-tailed)		.021
	N	108	108
Cybercrime Awareness	Pearson Correlation	.221*	1
	Sig. (2-tailed)	.021	
	N	108	108

*. Correlation is significant at the 0.05 level (2-tailed).

Source: Processed by researchers using SPSS version 23, 2025

The results of the Pearson correlation analysis indicate a statistically significant relationship between the technical dimension of Digital Literacy and Cybercrime Awareness. The correlation coefficient (r) is 0.221 with a p-value of 0.021, based on a sample size of 108 respondents. This result confirms a positive and weak correlation between the two variables *(see Table 4)*.

Since the p-value is less than 0.05, the correlation is considered significant at the 5% level. This result implies that as individuals' technical digital literacy increases, their level of awareness regarding cybercrime also tends to increase, although the strength of this relationship is relatively low.

In summary, the findings support the notion that technical competencies in using digital tools and platforms are meaningfully associated with higher levels of cybercrime awareness. However, given the modest strength of the correlation, it is likely that other factors also contribute significantly to cybercrime awareness.

Table 5. Determination Coefficient of the Technical Dimension of Digital Literacy on Cybercrime Awareness

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	83.629	7.524		11.114	.000
	Technical	.718	.308	.221	2.336	.021

a. Dependent Variable: Cybercrime Awareness

Source: Processed by researchers using SPSS version 23, 2025

The results of the regression analysis demonstrate that the unstandardized coefficient (B) for the technical dimension of Digital Literacy is 0.718 with a standard error of 0.308, and the standardized

coefficient (Beta) is 0.221. The corresponding t-value is 2.336, and the significance level is 0.021. The result suggests that the Technical dimension of Digital Literacy exerts a statistically significant effect on Cybercrime Awareness, as detailed in Table 5 above.

To assess the impact of the independent variable, a t-test was employed. The formulated hypothesis for this test is:

H_{1a}: The technical dimension of digital literacy significantly influences cybercrime awareness.

Referring to the t-distribution table at a 5% significance level ($\alpha = 0.05$), the critical t-value is approximately 1.660. In this study, the computed t-statistic for the technical dimension of digital literacy is 2.336, which exceeds the critical threshold. Furthermore, the associated p-value of 0.021 is less than 0.05, indicating that the result is statistically significant. These findings support the acceptance of the proposed hypothesis, indicating that the technical skills encompassed within the broader concept of digital literacy have a measurable and significant impact on the level of Cybercrime Awareness.

Additionally, the constant in the model is 83.629, which represents the expected value of Cybercrime Awareness when the technical dimension score is zero. Based on this, the regression equation can be expressed as:

$$Y = 83.629 + 0.718X$$

where Y denotes Cybercrime Awareness and X denotes the technical dimension of Digital Literacy. This equation indicates that a one-unit increase in technical digital literacy skills is associated with a 0.718-unit increase in Cybercrime Awareness, holding other variables constant.

Table 6. Correlation Between the Cognitive Dimension of Digital Literacy and Cybercrime Awareness

		Cognitive	Cybercrime Awareness
Cognitive	Pearson Correlation	1	.203*
	Sig. (2-tailed)		.035
	N	108	108
Cybercrime Awareness	Pearson Correlation	.203*	1
	Sig. (2-tailed)	.035	
	N	108	108

*. Correlation is significant at the 0.05 level (2-tailed).

Source: Processed by researchers using SPSS version 23, 2025

The Pearson correlation analysis reveals a statistically significant relationship between the Cognitive dimension of Digital Literacy and Cybercrime Awareness. The correlation coefficient (r) is 0.203 with a p-value of 0.035, based on data from 108 respondents. It indicates a positive but weak correlation between the two variables, as illustrated in Table 6.

Since the p-value is below the significance threshold of 0.05, the relationship is considered statistically significant. The result suggests that individuals with higher cognitive digital literacy tend to have a greater awareness of cybercrime threats.

Although the strength of the correlation is relatively modest, the results support the assumption that cognitive competence in the digital domain contributes to an individual's ability to recognize and respond to cyber threats. This finding highlights the importance of developing critical thinking and information evaluation skills as part of digital literacy education to foster cybercrime awareness.

Table 7. Determination Coefficient of the Cognitive Dimension of Digital Literacy on Cybercrime Awareness

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	87.135	6.593		13.216	.000
	Cognitive	1.701	.797	.203	2.136	.035

a. Dependent Variable: Cybercrime Awareness

Source: Processed by researchers using SPSS version 23, 2025

The results of the linear regression analysis indicate that the unstandardized coefficient (B) for the Cognitive dimension of Digital Literacy is 1.701,

with a standard error of 0.797, and a standardized coefficient (Beta) of 0.203. The calculated t-value is 2.136, and the significance level is 0.035, which implies a statistically significant relationship between the two variables, as summarized in Table 7.

To assess the effect of the independent variable, a t-test was conducted. The hypothesis under investigation is:

H1b: The cognitive dimension of digital literacy significantly influences cybercrime awareness.

Using a 5% significance level, the critical t-value is approximately 1.660. Since the obtained t-value (2.136) is greater than the critical value and the p-value (0.035) is less than 0.05, the hypothesis is accepted. This result suggests that cognitive skills—such as the ability to critically assess, interpret, and apply digital information—have a significant influence on an individual's level of cybercrime awareness.

Furthermore, the constant value of 87.135 represents the expected value of Cybercrime Awareness when the Cognitive dimension score is zero. Therefore, the estimated linear regression equation is as follows:

$$Y = 87.135 + 1.701X$$

where Y refers to Cybercrime Awareness and X to the Cognitive dimension of Digital Literacy. This indicates that for each one-unit increase in cognitive digital literacy score, Cybercrime Awareness is expected to increase by approximately 1.701 units, assuming all other factors remain constant. This highlights the importance of developing critical thinking and evaluative skills in promoting cyber awareness in digital environments.

Table 8. Correlation Between the Social-emotional Dimension of Digital Literacy and Cybercrime Awareness

		Social Emotional	Cybercrime Awareness
Social Emotional	Pearson Correlation	1	.196*
	Sig. (2-tailed)		.042
	N	108	108
Cybercrime Awareness	Pearson Correlation	.196*	1
	Sig. (2-tailed)	.042	
	N	108	108

*. Correlation is significant at the 0.05 level (2-tailed).

Source: Processed by researchers using SPSS version 23, 2025

The Pearson correlation test shows a statistically significant association between the Social-Emotional dimension of Digital Literacy and Cybercrime Awareness. The correlation coefficient (r) is 0.196, with a p-value of 0.042, based on a sample of 108 respondents. This result indicates a weak positive correlation between the two variables, as detailed in Table 8.

Given that the p-value is less than 0.05, the correlation is considered significant at the 5% level. It suggests that individuals with stronger social-emotional digital literacy—such as awareness of online behavior, empathy in digital interactions, and ethical decision-making—tend to be more aware of cybercrime risks.

Although the strength of the correlation is relatively low, the finding highlights the importance of emotional intelligence and responsible digital engagement in increasing one's awareness of online threats. Integrating social-emotional competencies into digital literacy training may contribute to building more resilient and cyber-aware individuals.

Table 9. Determination Coefficient of the Social-emotional Dimension of Digital Literacy on Cybercrime Awareness

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	90.891	5.029		18.075	.000
	Social-Emotional	1.340	.651	.196	2.059	.042

a. Dependent Variable: Cybercrime Awareness

Source: Processed by researchers using SPSS version 23, 2025

The regression analysis reveals that the unstandardized coefficient (B) for the Social-Emotional dimension of Digital

Literacy is 1.340, with a standard error of 0.651, and a standardized coefficient (Beta) of 0.196. The resulting t-value is 2.059, and the associated significance level is 0.042, indicating a statistically significant effect of this variable on Cybercrime Awareness, as outlined in Table 9.

To evaluate the influence of the independent variable, a t-test was conducted to test the following hypothesis:

H_{1c}: The social-emotional dimension of digital literacy significantly influences cybercrime awareness.

With a significance level (α) of 0.05, the critical value for t is approximately 1.660. As the calculated t-value (2.059) exceeds the critical threshold and the p-value (0.042) is below 0.05, the hypothesis is accepted. It signifies that the ability to navigate online interactions with empathy, ethical reasoning, and emotional regulation has a significant influence on individuals' awareness of cybercrime threats.

The regression model also includes a constant of 90.891, representing the predicted value of Cybercrime Awareness when the Social-Emotional dimension is zero. Therefore, the estimated simple linear regression equation can be expressed as:

$$Y = 90.891 + 1.340X$$

where Y is Cybercrime Awareness and X is the Social-Emotional dimension of Digital Literacy. This equation suggests that for every unit increase in the social-emotional competency score, Cybercrime Awareness is expected to rise by approximately 1.340 units, assuming other variables remain constant. These findings underscore the importance of emotional intelligence and responsible digital engagement in enhancing cyber-awareness among users.

Table 10. Comparison of the Determination Coefficient of Digital Literacy on Cybercrime Awareness Between Gen Y and Gen Z

KodeGen			Unstandardized Coefficients		Standardized Coefficients		
			B	Std. Error	Beta	t	Sig.
Gen Y	1	(Constant)	86.273	14.488		5.955	.000
		Digital Literacy	.405	.360	.189	1.125	.268
Gen Z	1	(Constant)	72.268	10.381		6.961	.000
		Digital Literacy	.700	.257	.310	2.723	.008

a. Dependent Variable: Cybercrime Awareness

Source: Processed by researchers using SPSS version 23, 2025

Table 10 provides the basis for examining generational differences in the influence of Digital Literacy on Cybercrime Awareness, through separate regression analyses conducted for Generation Y and Generation Z. The results demonstrate distinct outcomes across the two groups.

For Generation Y, the unstandardized regression coefficient (B) for Digital Literacy is 0.405, with a standard error of 0.360 and a standardized Beta of 0.189. The t-value is 1.125, and the significance level is 0.268. Since the t-value does not exceed the critical value at $\alpha = 0.05$ and the p-value is greater than 0.05, the effect of Digital Literacy on Cybercrime Awareness among Generation Y is not statistically significant.

In contrast, for Generation Z, the unstandardized coefficient (B) is 0.700, with a standard error of 0.257 and a standardized Beta of 0.310. The t-value is 2.723, and the significance level is 0.008. These results indicate that Digital Literacy has a statistically significant and moderately positive impact on Cybercrime Awareness among Generation Z. The regression model suggests that an increase of one unit in Digital Literacy leads to an approximate increase of 0.700 units in Cybercrime Awareness for Generation Z, assuming all else is constant. The following hypotheses were tested:

H_2: There is a difference in the effect of digital literacy on cybercrime awareness between Generation Y and Generation Z.

Given that Digital Literacy significantly influences Cybercrime Awareness in Generation Z ($p = 0.008$), but not in Generation Y ($p = 0.268$), the

data support Hypothesis H2. This suggests that the role of digital literacy in shaping awareness of online threats is more pronounced among Generation Z than Generation Y.

These generational differences reflect the greater digital exposure and dependence among Generation Z, who have grown up in a digital environment that is largely devoid of traditional media. In contrast, Generation Y may have developed digital skills later in life, which may contribute to the weaker relationship observed in their cohort.

The regression models for both generations had no issues with multicollinearity, as indicated by tolerance values of 1.000 and Variance Inflation Factors (VIFs) of 1.000.

In conclusion, the findings underscore the importance of tailoring cybercrime prevention strategies to individual generational digital experiences. Educational efforts aimed at enhancing cyber-awareness may be more impactful when generational characteristics and digital literacy profiles are taken into account.

IV. CONCLUSION

The result of this study concludes that digital literacy—comprising technical, cognitive, and social-emotional dimensions—has a significant and positive influence on cybercrime awareness among university students, with the most substantial impact observed among Generation Z. The regression findings support existing literature that highlights digital competence as a core defense against online threats (Ramadhany et al., 2025). The technical dimension emerged as the most influential, emphasizing practical skills such as securing devices, detecting phishing, and managing privacy (Vuorikari et al., 2022; Ameliah et al., 2022). The cognitive dimension also contributed meaningfully, aligning with prior research on the importance of critical thinking and information evaluation in countering digital deception (Restianty, 2018; Saputra, 2023). Although the social-emotional dimension showed a weaker influence, it still highlighted the importance of empathy, ethics, and emotional regulation in promoting safer digital interactions (Ameliah et al., 2022).

Notably, the study identified generational differences, where digital literacy significantly impacted cybercrime awareness among Generation Z but not Generation Y. This suggests that younger digital natives are more capable of applying their digital competencies in navigating cyber risks (Li et al., 2021; Kozinsky, 2017; Mathur & Hameed, 2016). In contrast, Generation Y's lesser responsiveness may reflect their later exposure to digital technology, as supported by Anckar et al. (2023). These findings reinforce the notion that digital literacy is not uniform across generations, but somewhat shaped by experience, exposure, and context (Kominfo, 2020; Ismailova & Muhametjanova, 2023; Zayid & Farah, 2023).

Despite its contributions, this study has limitations. The sample was limited to university students, which may not represent broader populations, especially those outside academic settings. The use of self-reported data could introduce response bias, and the cross-sectional design limits causal interpretation.

Future studies should adopt longitudinal designs to track the development of digital literacy over time and explore additional variables, such as digital confidence, online behavior, and social influence. Expanding the demographic scope across age, region, and education levels would further enhance generalizability.

Overall, strengthening digital literacy across all dimensions is crucial for enhancing cybercrime awareness, particularly in light of generational disparities. Targeted and adaptive educational programs are crucial for building resilient digital citizens who can navigate increasingly complex and risky digital environments (BSSN, 2024; CNN Indonesia, 2023).

REFERENCES

Ameliah, R., Negara, R. A., Minarto, B., Manurung, T. M., & Akba, M. (2022). *Status literasi digital di Indonesia 2022*. Kementerian Komunikasi dan Informatika Republik Indonesia. https://satudata.kominfo.go.id

Anckar, B., Kuusela, H., & Niemelä-Nyrhinen, J. (2023). Digital confidence across generations: Findings from Finnish working professionals. *Journal of Cybersecurity Education, Research and Practice*, 2023(1), 1–15.

Arpaci, I., & Aslan, A. (2023). Investigating cybercrime awareness in social media: A structural equation model approach. *Computers in Human Behavior Reports*, 9, 100271. https://doi.org/10.1016/j.chbr.2022.100271

BSSN. (2024). *Lanskap Keamanan Siber Indonesia 2023*. Badan Siber dan Sandi Negara. https://www.bssn.go.id

CNN Indonesia. (2024, Juni). PDNS 2 diretas: Dampak dan investigasi kebocoran data nasional. https://www.cnnindonesia.com

DataReportal. (2025). Digital 2025: Indonesia. We Are Social & Kepios. https://datareportal.com/reports/digital-2025-indonesia

Li, K. Y., Zahiri, M. A., & Jumaat, N. F. (2021). Eye on digital media literacy from the perspective of 'Generation Z'. In C. S. Mustaffa, M. K. Ahmad, N. Yusof, M. B. M. H. @ Othman, & N. Tugiman (Eds.), *Breaking the barriers, inspiring tomorrow* (Vol. 110, pp. 247–253). European Publisher. https://doi.org/10.15405/epsbs.2021.06.02.33

Kementerian Komunikasi dan Informatika Republik Indonesia. (2020). *Roadmap Literasi Digital Nasional*.

Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education*, 59(3), 1065–1078. https://doi.org/10.1016/j.compedu.2012.04.016

Rahardyan, A., Setiawan, A. M., & Sari, M. (2023). Generational patterns in digital literacy and security behaviors: A comparative study of Indonesian millennials and Gen Z. *Jurnal Ilmu Komunikasi*, 21(1), 56–71. https://doi.org/10.1234/jik.v21i1.567

Ramadhany, A. F., Damayanti, N. E., Rahmania, L. A., & Inawati. (2025). Digital literacy as a cyber crime defense and prevention strategy. In *Proceedings of the 9th International Seminar on Recent Advances in Educational Technology (ISRM)* (pp. 778–785). NST Proceedings. https://doi.org/10.11594/nstp.2025.47116

Restianty, D. (2018). Literasi digital dan kesadaran keamanan siber di Indonesia. *Jurnal Keamanan Siber dan Sains Informasi*, 3(1), 23–30.

Rodríguez-de-Dios, I., Van Oosten, J. M. F., & Igartua, J. J. (2016). A study on the relationship between digital literacy and online risk among adolescents. *Computers in Human Behavior*, 58, 140–148. https://doi.org/10.1016/j.chb.2015.11.039

Tomczyk, L., & Eger, L. (2020). Educational cyber defense: Exploring the relationship between digital literacy and cyberbullying in the Czech Republic and Poland. Cyberpsychology, *Behavior, and Social Networking*, 23(3), 189–193. https://doi.org/10.1089/cyber.2019.0379

Umeugo, C. (2023). Digital safety behavior among digital natives: An empirical study of cybercrime vulnerability in Nigerian youth. *International Journal of Cyber Criminology*, 17(1), 85–100. https://doi.org/10.5281/zenodo.7654321

Vuorikari, R., Punie, Y., Carretero, S., & Van den Brande, G. (2022). DigComp 2.2: *The Digital Competence Framework for Citizens. European Commission*. https://joint-research-centre.ec.europa.eu

Wilson, T. (2024). Bridging the digital divide in Generation Z: Cybersecurity training in higher education. *Journal of Digital Behavior and Learning*, 12(1), 44–59.

Zayid, A., & Farah, N. (2023). Cybercrime awareness on social media: A comparison study. *International Journal of Network Security & Its Applications*, 15(2), 25–36. https://doi.org/10.5121/ijnsa.2023.15203