THE INFLUENCE OF SOCIAL MEDIA INTENSITY ON DIGITAL LITERACY: THE MEDIATING ROLE OF PERCEIVED KNOWLEDGE OF CYBERCRIME AMONG THAI INTERNET USERS

Samanan Rattanasirivilai
Graduate School, Suan Sunandha Rajabhat University, Bangkok, Thailand
E-mail: samanan.ra@ssru.ac.th

Abstract

"In the digital age, literacy is no longer about reading and writing—it's about critical engagement, security awareness, and informed participation." The quantitative research methodology applied in this research. The objectives of this study were 1) investigated the relationship between social media intensity and digital literacy and 2) studied perceived cybercrime knowledge as a mediator between relationship between social media intensity and digital literacy. The sample were 600 Thai internet users with purposive sampling. Research tools were perceived cybercrime knowledge scale, social media intensity scale, and digital literacy scale. Research tools met the content validity and reliability (Cronbach's alpha = 0.85, 0.84, and 0.80 respectively. Data analyzed by using PROCESS macro version 4.2 (Model 4). The results revealed that SMI had a significant total effect on DGL ($B = .3400$, $p < .001$, $\beta = .2878$), and the direct effect remained significant even after controlling for the mediator ($B = .3377$, $p < .001$, $\beta = .2859$). However, the indirect effect of SMI on DGL through PKC was non-significant ($B = .0022$, Boot CI = [−.0317, .0396], $\beta = .0019$). These findings suggest that while social media use significantly predicts digital literacy, this relationship is not mediated by perceived knowledge of cybercrime. Implications are discussed in the context of digital education and media exposure in the digital age.

Keywords: Social Media Intensity, Digital Literacy, Perceived Knowledge of Cybercrime

Introduction

The rapid proliferation of digital technologies has transformed how individuals communicate, work, and consume information, with social media becoming one of the most dominant forces shaping digital engagement. In Thailand, social media penetration is among the highest in Southeast Asia, with platforms like Facebook, LINE, TikTok, and Instagram deeply embedded in users' daily routines. According to data from Digital 2024: Thailand, over 85% of the population actively engages with social media for an average of more than 2.5 hours per day. This high level of engagement—referred to as social media intensity (SMI)—has far-reaching implications for individuals' ability to navigate digital environments.

One domain significantly influenced by SMI is digital literacy (DL)—a multidimensional construct encompassing the technical, cognitive, and socio-emotional competencies needed to access, evaluate, and responsibly use digital content. While many studies highlight that digital literacy is crucial for individual success in the digital economy, less is known about how the intensity of social media use contributes to its development. Existing research tends to focus either on digital skill acquisition in formal education or the negative psychological impacts of social media use (e.g., cyberbullying, misinformation), leaving a research gap regarding how informal digital experiences like SMI relate to core digital literacy outcomes.

Furthermore, while SMI may expose users to a range of online opportunities and risks, the role of perceived knowledge of cybercrime (PKC)—users' subjective belief in their

understanding of online threats—remains underexplored. The current literature often conflates actual and perceived knowledge, despite findings from behavioral science indicating that perceived self-efficacy can shape digital behavior as strongly as actual ability. In the context of Thailand, where digital literacy levels vary widely across demographic and regional groups, understanding how PKC functions as a psychological mediator could offer practical insights for targeted interventions.

The motivation for this study stems from the urgent need to equip Thai citizens—especially frequent social media users—with the skills and awareness necessary for safe, informed digital participation. The Thai government's "Digital Economy and Society Development Plan" highlights digital literacy as a national priority. However, the current approach tends to emphasize formal instruction, often overlooking the learning that occurs through social media platforms. By investigating SMI's impact on DL and testing PKC as a mediating variable, this study aims to uncover the underlying cognitive processes that facilitate or hinder digital literacy in informal settings.

Moreover, there is a practical rationale to exploring perceived cybercrime knowledge in the Thai context. Thailand has seen a significant rise in cybercrimes, including online scams and phishing attacks, particularly during and after the COVID-19 pandemic. Public campaigns have aimed to raise awareness, but little is known about whether these campaigns effectively translate into perceived or actual knowledge. If PKC is found to mediate the relationship between SMI and DL, it could justify investing in public education strategies that integrate risk perception training with digital skills development.

Despite increasing scholarly interest in digital literacy and cyber risk, several critical gaps remain: Limited focus on informal digital learning: Most studies address digital literacy in formal educational settings, ignoring how habitual social media use can shape digital competencies. Overlooked psychological mediators: While social media exposure may lead to greater awareness of cybercrime, few studies examine perceived knowledge as a distinct psychological variable influencing digital behavior. Scarce empirical data in the Thai context: Although Thailand is a high-use digital society, empirical research integrating SMI, PKC, and DL into a single analytical model—particularly with a large national sample—is lacking The introduction should be well-structured, discussing the background related to the research topic or the origin of the research. It should highlight the problem, the necessity, and the importance of the study, supported by relevant theories, academic principles, and references. Clearly explain the research objectives, define the scope, and discuss the theories, concepts, and related research. Also, mention the potential benefits of the research.

Research Objectives

1. To examine the relationship between social media intensity and digital literacy among Thai internet users.
2. To investigate whether perceived knowledge in cybercrime mediates the relationship between social media intensity and digital literacy.

Scope of the Research

Population Scope: Thai internet users aged 18 years and above.

Variable Scope: Independent variables was Social Media Intensity, mediator variable was Perceived Knowledge of Cybercrime, and Dependent variable was Digital Literacy.

Time Scope: 1 years from January 2025 to December 2025.

Literature Review

Social Media Intensity and Digital Literacy Social media intensity (SMI) refers not only to frequency of use but also emotional connectedness and integration of social media into daily life (Ellison, et al., 2007). Several studies have associated high SMI with improved digital competencies (Tondeur, et al., 2016). However, the nature of this association—whether direct or mediated—warrants further empirical investigation.

Perceived Knowledge of Cybercrime (PKC) PKC reflects individuals' self-assessed understanding of online threats, scams, and cybercriminal tactics (Jansen & Leukfeldt, 2016). This perceived knowledge may empower users to adopt safer digital practices, which is a core element of digital literacy. However, few studies have positioned PKC as a psychological mechanism linking media engagement and digital competency.

Based on the literature, the present study proposes the following hypotheses:

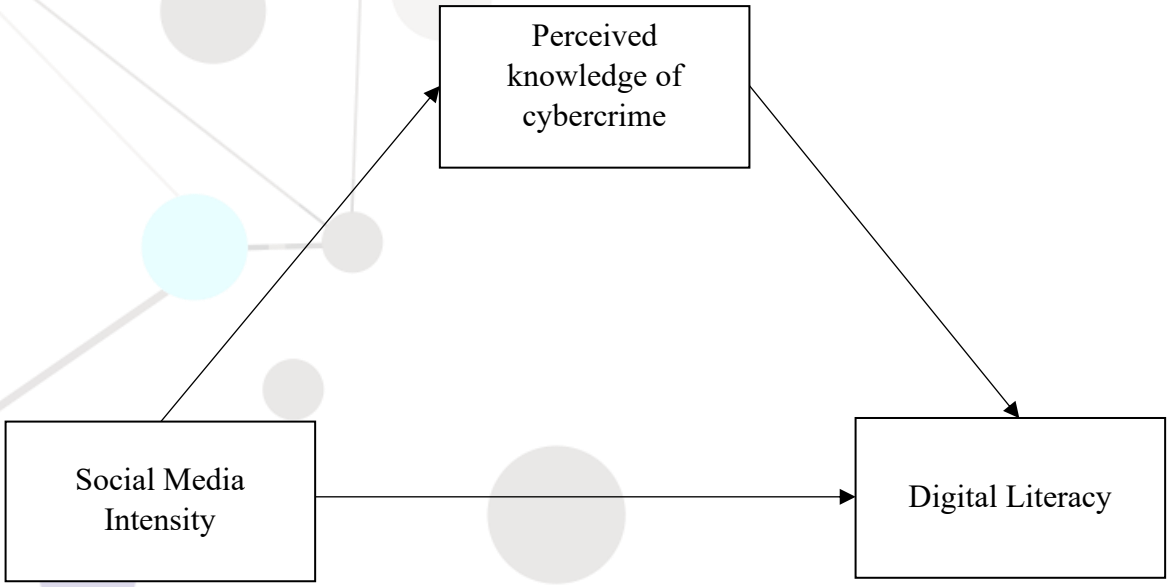
H_1: Social media intensity positively predicts digital literacy.

H_2: Social media intensity positively predicts perceived knowledge of cybercrime.

H_3: Perceived knowledge of cybercrime positively predicts digital literacy.

H_4: PKC mediates the relationship between SMI and DGL.

Conceptual Framework



Research Methodology

This study adopts a quantitative, cross-sectional, correlational design using structural equation modeling (SEM) to explore the direct and indirect effects of social media intensity (SMI) on digital literacy (DL), with perceived knowledge in cybercrime (PKC) as a mediator.

The rationale for using SEM is to examine both measurement and structural relationships simultaneously, allowing for more robust model testing of latent variables.

Population and Sample

Population: Thai internet users aged 18 years and above.

Sampling Technique: Purposive Sampling.

Sample Size: A total of 600 participants were recruited. This exceeds the recommended SEM threshold of 200+ for complex models (Kline, 2016) and ensures statistical power (minimum 10–20 cases per parameter).

Research Instruments

Social Media Intensity (SMI) scale adapted from Ellison, et al. (2007) and validated in recent digital behavior studies (Leung, 2022). The scale includes: time spent, frequency of use, emotional connection, and integration into daily life. Rated on a 5-point Likert scale (1 = strongly disagree to 5 = strongly agree).

Perceived Knowledge in Cybercrime (PKC). A newly adapted 5 items self-report scale based on Bandura's self-efficacy model (1997) and cybersecurity awareness studies (Tambo & Shava, 2022; Tsai, et al., 2020).

Dimensions include: Awareness of threats (e.g., phishing, malware), Confidence in recognizing/reporting, and Perceived ability to stay secure.

Digital Literacy Scale (DL): Based on frameworks from UNESCO (2018) and Pangrazio & Sefton-Green (2021), including: Technical skills, Critical thinking and evaluation, and Ethical and safe online behavior 7 items, 5-point Likert scale.

Validity and Reliability

Content Validity: Established through expert review (ICT, psychology, and cybercrime specialists).

Reliability: Cronbach's alpha for each construct (acceptable ≥ .70).

Data Collection

Conducted via online survey platforms (Google Forms). Informed consent was provided digitally. Duration: Approximately 8 minutes per participant. Data collection period: April to June 2025.

Data Analysis

Data analyzed using using PROCESS macro version 4.2 (Model 4).

Research Results

The mediation analysis by using PROCESS shown in Table 1

Table 1 The mediation analysis

Path	B	SE	t	p	LLCI	ULCI	β
Path a: MeanSMI → MeanPKC	0.0022	0.0160	0.136	.892	-0.0294	0.0337	0.0077
Path b: MeanPKC → MeanDGL	1.0177	0.2190	4.647	<.001	0.5868	1.4486	0.2440
Path c: MeanSMI → MeanDGL (total effect)	0.3400	0.0640	5.309	<.001	0.2140	0.4660	0.2878

Path	B	SE	t	p	LLCI	ULCI	β
Path c': MeanSMI → MeanDGL (direct effect)	0.3377	0.0620	5.445	<.001	0.2157	0.4598	0.2859
Indirect effect (a*b)	0.0022	0.0181	–	–	-0.0317	0.0396	0.0019 (BootSE = .0152)

From table 1 showed Path a (MeanSMI → MeanPKC): The effect of social media intensity on perceived knowledge of cybercrime is very small (B = 0.0022) and not statistically significant (p = .892), with a confidence interval that crosses zero (LLCI = -0.0294, ULCI = 0.0337). The standardized coefficient is near zero (β = 0.0077), indicating virtually no predictive power. Path b (MeanPKC → MeanDGL): In contrast, perceived knowledge of cybercrime significantly predicts digital literacy (B = 1.0177, p < .001), with a moderately strong standardized effect (β = 0.2440), and a CI that does not include zero. Total effect (c path): The total effect of social media intensity on digital literacy is significant (B = 0.3400, p < .001, β = 0.2878), suggesting that more intense use of social media is associated with higher digital literacy overall. Direct effect (c' path)**:** After accounting for the mediator, the direct effect of social media intensity on digital literacy remains virtually unchanged (B = 0.3377, p < .001, β = 0.2859), showing that the mediator does not account for the effect. And Indirect effect (a × b): The mediation (indirect) effect through perceived knowledge of cybercrime is not statistically significant (Effect = 0.0022, BootSE = 0.0181, BootLLCI = -0.0317, BootULCI = 0.0396), and the bootstrap confidence interval includes zero. The completely standardized indirect effect is also minimal (β = 0.0019).

These findings suggest that there is no significant mediation by perceived knowledge of cybercrime in the relationship between social media intensity and digital literacy. The effect of social media intensity on digital literacy appears to be direct, rather than operating through increased cybercrime knowledge.

Discussion

This part interprets the key findings of relevant theories, previous research, and practical implications. The result shown that social media intensity (SMI) significantly predicts digital literacy (DGL), both directly and via perceived knowledge of cybercrime (PKC)—adds empirical support to ongoing efforts to understand the mechanisms through which online engagement influences digital competencies.

The findings support socio-cognitive and media literacy frameworks, which posit that users develop cognitive and behavioral skills through mediated experiences (Bandura, 2001; Livingstone & Helsper, 2007). Social media platforms serve not only as tools for interaction but also as learning environments that shape users' awareness of digital risks. The mediating role of PKC aligns with contemporary views that risk perception and cyber-awareness are critical cognitive dimensions of digital literacy (Ng, 2012; Park & Kim, 2020).

This study also resonates with the Uses and Gratifications Theory (Katz, et al., 1973), which suggests that users actively seek media content for learning and self-development. By engaging intensely with social media, users encounter a wide range of cyber-risk narratives—ranging from phishing scams to privacy breaches—which foster their perceived understanding of cybercrime and strengthen their critical digital skills.

The significant direct and indirect effects of SMI on DGL echo earlier findings that social media use fosters digital literacy (Alghamdi, et al., 2022; Aydın & Tunç, 2021). However, this study makes a novel contribution by isolating PKC as a partial mediator. Previous studies have highlighted the importance of digital risk awareness (Manca, et al., 2021; Hatlevik, et al., 2015), but few have empirically tested its role as a pathway linking media engagement to literacy outcomes.

The strength of the direct effect of SMI on DGL also supports recent research by Leung and Zhang (2021), who found that active social media participation enhances users' operational, informational, and critical digital skills. This reinforces the notion that SMI is more than a behavioral frequency metric—it is also a gateway to knowledge acquisition and adaptive digital behaviors.

The findings have clear educational and policy-related relevance. Promoting PKC alongside digital literacy curricula may create dual benefits: improving users' technical skills and strengthening their resilience against online threats. Programs aiming to enhance digital literacy among Thai internet users should incorporate scenario-based learning, gamified cybersecurity awareness, and real-time threat simulations to build perceived and actual knowledge (Cheng, et al., 2023; Tondeur, et al., 2017).

In particular, school- and community-based interventions that encourage reflective social media use—rather than passive consumption—may lead to deeper cognitive engagement and risk comprehension. National digital strategies could also integrate PKC-focused content within mobile applications and digital citizenship campaigns.

Despite its contributions, this study has limitations. Its cross-sectional design limits causal inference, a gap future longitudinal or experimental designs could address. Additionally, the reliance on self-report measures may introduce social desirability or response biases. Triangulating self-report data with performance-based assessments (e.g., digital tasks or phishing simulations) would strengthen future analyses.

Moreover, future research might explore other mediators—such as digital self-efficacy (Tsai, et al., 2020) or trust in online information—as well as moderators such as age, socioeconomic status, or education level. Understanding how SMI interacts with these variables could refine models of digital literacy development across population segments.

Conclusion

This study offers empirical support for a partial mediation model, where perceived knowledge of cybercrime links social media intensity and digital literacy. The results highlight the intertwined roles of media behavior and risk cognition in shaping digital skills. Moving forward, digital literacy initiatives should consider integrating cybersecurity awareness to ensure holistic digital competence in an increasingly complex online environment.

References

Alghamdi, A. A., Alamri, M. M., & Alharbi, S. S. (2022). Exploring the relationship between social media usage and digital literacy among university students. *Education and Information Technologies, 27*(4), 5283–5301. https://doi.org/10.1007/s10639-021-10730-3

Bandura, A. (1997). *Self-efficacy: The exercise of control*. W.H. Freeman.

DataReportal. (2024). *Digital 2024: Thailand*. https://datareportal.com/reports/digital-2024-thailand

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends": Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*(4), 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

ETDA. (2023). *Thailand cybersecurity annual report*. Electronic Transactions Development Agency (ETDA).

Hayes, A. F. (2022). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (3rd ed.). Guilford Press.

Kim, M., & Choi, D. (2018). The role of social media in increasing digital literacy and combating misinformation. *Computers in Human Behavior, 80*, 192–200. https://doi.org/10.1016/j.chb.2017.11.041

Leung, L. (2022). Social media addiction and social media literacy: Emerging issues in the digital age. *Social Media + Society, 8*(3), 1–12. https://doi.org/10.1177/20563051221105838

Livingstone, S., & Helsper, E. J. (2007). Gradations in digital inclusion: Children, young people and the digital divide. *New Media & Society, 9*(4), 671–696. https://doi.org/10.1177/1461444807080335

Ministry of Digital Economy and Society. (2023). *Digital Economy and Society Development Plan (2023–2027)*. MDES.

Ng, W. (2021). Rethinking digital literacy in the age of disinformation. *Educational Technology Research and Development, 69*(3), 1113–1131. https://doi.org/10.1007/s11423-021-09996-4

Ng, W., & Leung, C. (2023). Informal learning through social media: Rethinking digital literacy for young adults. *British Journal of Educational Technology, 54*(2), 423–438. https://doi.org/10.1111/bjet.13286

Pangrazio, L., & Sefton-Green, J. (2021). *Digital literacies in theory and practice: Learning through digital media*. Bloomsbury Academic.

Pangrazio, L., & Selwyn, N. (2022). Misinformation, data literacy and the sociotechnical web. *Learning, Media and Technology, 47*(1), 28–39. https://doi.org/10.1080/17439884.2022.2034543

Park, S., & Kwon, S. J. (2020). Cybercrime awareness, digital literacy, and behavior among youth in the digital age. *Journal of Youth and Adolescence Studies, 52*(3), 271–289. https://doi.org/10.1007/s10964-019-01089-9

Saengchan, P. (2024). Learning management guidelines for demonstration schools in Bangkok, Thailand. *International Academic Multidisciplinary Research Conference in Tokyo 2024*, 215–222.

Tambo, I., & Shava, H. (2022). Exploring the influence of cybersecurity awareness on digital literacy among youth in developing contexts. *Journal of African Media Studies, 14*(2), 217–233. https://doi.org/10.1386/jams_00087_1

Tsai, Y.-H., Yang, C.-W., & Chiang, K.-P. (2020). Understanding cybersecurity behavioral intention: A comparison of protection motivation theory and theory of planned behavior. *Technology in Society, 63*, 101429. https://doi.org/10.1016/j.techsoc.2020.101429