Journal of Communication Studies: CommVersa
Vol. 1 No. 6 September 2025
E-ISSN: 3109-5097
Open Access: https://journals.ai-mrc.com/commversa

Students and Fake News: Exploring Digital Literacy and Information Security Among Young Adults

Dalilah Yusyifa Asfari [1]*, Diva Deviyanti Ruslan [2], Alysa Syahira [3], Andi Subhan Amir [4]
[1, 4]Hasanuddin University, Indonesia
[2]University of Indonesia, Indonesia
[3]State University of Makassar, Indonesia
[1]dalilah.syifa8@gmail.com*, [2]divadeviyantiruslan@gmail.com, [3]alysasyahira88@gmail.com, [4]asa@unhas.ac.id

Article Info

Article history:
Received 27-07-2025
Revised 19-09-2025
Accepted 24-09-2025

Keyword:
Digital Literacy, Misinformation, Fake News, Information Security, Privacy Management, Cyber Threats, University Students

ABSTRACT

In the digital age, the rapid spread of fake news, disinformation, and hoaxes poses significant challenges, particularly among young adults who are highly engaged with digital media. This study aims to explore the relationship between digital literacy and information security practices among university students in Indonesia, aged 18–19, in the context of misinformation and digital threats. A qualitative approach was employed using open-ended questionnaires to gather insights into students' experiences and strategies for handling online misinformation, securing personal data, and verifying information. Data analysis was conducted using thematic analysis, identifying key themes related to media verification, awareness of digital threats, and personal privacy management. Out of 120 respondents, 78% reported encountering fake news on social media platforms such as Instagram and TikTok at least once a week, while only 42% consistently verified the information before sharing it. Moreover, 65% admitted to having shared unverified content at least once, often driven by emotional reactions or peer influence. In terms of data security, 58% stated they used two-factor authentication, but only 37% regularly updated their passwords or reviewed privacy settings. The findings reveal that most students are aware of the importance of verifying information and safeguarding personal data, but the application of these practices varies. For instance, while 84% recognized misinformation as a major online threat, only 46% could accurately identify fake accounts or manipulated images. The rapid spread of hoaxes is often facilitated by emotional impulses, social media algorithms, and a lack of digital literacy. The study emphasizes the need for more comprehensive digital literacy education, including the integration of digital security into university curricula and creative campaigns to enhance students' ability to identify and respond to misinformation. These recommendations are supported by the finding that students who received formal digital literacy training (about 28% of participants) demonstrated 35% higher verification accuracy compared to those without prior training. The results suggest that fostering a culture of verification and privacy protection is crucial for equipping students to navigate the complexities of the digital landscape effectively and securely.

INTRODUCTION

In the digital age, the spread of disinformation and hoaxes has become a serious global concern, especially with the increasing influence of social media and online news platforms. Disinformation refers to the deliberate dissemination of false or misleading information intended to deceive, while hoaxes are fabricated narratives often designed to appear truthful to manipulate public perception. Closely related, fake news and misinformation are terms used to describe intentionally false or deceptive content that is presented as legitimate news or factual information. This phenomenon has grown rapidly due to the ease with which information—both true and false—can be circulated online.

Recent empirical studies indicate that social media platforms remain the dominant channels for misinformation exposure. For instance, a 2023 Pew Research Center report found that 64% of young

adults encountered false information on social media weekly, while a UNESCO (2024) study emphasized that digital verification skills among users aged 18–24 remain critically low, particularly in developing countries such as Indonesia. These findings highlight a growing digital divide not only in access to technology but also in the ability to critically evaluate online information.

One of the most alarming aspects of fake news and misinformation is their viral nature. False information can be shared and amplified by millions of users within minutes, often outpacing efforts to verify and correct it. This rapid spread undermines credible sources and fosters widespread belief in falsehoods, even when reliable evidence contradicts them. Beyond confusion, such misinformation has been weaponized for political and ideological purposes, including during election campaigns, where it may manipulate public opinion and damage democratic processes.

Empirical evidence from Guess et al. (2023) and Pennycook & Rand (2024) demonstrates that users with lower digital literacy are three times more likely to share misinformation, often due to heuristic processing and emotional triggers rather than deliberate intent. These studies provide a direct foundation for examining how literacy skills and information security awareness jointly influence online behavior.

The consequences of fake news and misinformation are far-reaching. On a societal level, they erode public trust in media and institutions, cause political polarization, and create uncertainty around critical issues. On a personal level, individuals can suffer reputational harm, privacy violations, and psychological distress. Moreover, misinformation in areas like health and safety can result in dangerous decision-making, further exacerbating crises and endangering public welfare. These impacts are especially pronounced among young adults, who are active digital media users and thus highly exposed to online content both accurate and deceptive.

A 2024 ASEAN Digital Trust Index report revealed that Indonesian youth ranked among the lowest in Southeast Asia for online information verification confidence, suggesting an urgent need for targeted educational interventions. This aligns with findings from Susanto et al. (2023), who observed that only 41% of university students could correctly distinguish between credible and manipulated online sources.

To address these challenges, digital literacy and information security have become increasingly essential. Digital literacy is the ability to locate, evaluate, and use digital content critically and responsibly. It empowers users to identify trustworthy sources, detect bias or manipulation, and make informed decisions in the digital landscape. Equally important is information security awareness, which involves understanding how to protect personal data, maintain privacy, and guard against threats like phishing or identity theft. These two concepts are deeply interconnected and are necessary for building a generation of informed and cautious digital citizens.

However, the intersection between digital literacy and information security remains underexplored in the Southeast Asian context. Previous studies (e.g., Rahmawati & Taufiq, 2023; Al-Fadhli, 2024) tend to examine these domains separately, focusing either on misinformation resilience or cybersecurity behavior. This lack of integration presents a clear research gap, particularly regarding how young adults apply literacy and security practices simultaneously in real-world digital interactions.

This study seeks to examine the relationship between digital literacy and information security practices among young adults in the context of fake news, disinformation, and hoaxes. By focusing on university students, the research aims to assess how well-equipped they are to identify and respond to misinformation in their digital environments. The findings are expected to highlight gaps in awareness and digital education while offering insights for developing stronger media literacy and cybersecurity strategies within academic and societal contexts.

RESEARCH METHODS

This study employed a qualitative research approach to explore how young adults perceive and respond to fake news, disinformation, and digital information security threats. Data were collected using open-ended questionnaires designed to elicit detailed responses regarding students' experiences,

attitudes, and strategies in navigating digital media. The research population consisted of university students aged 18 to 19 years from various institutions in Indonesia, with participants selected through purposive sampling.

The rationale for choosing this sampling technique was to ensure the inclusion of participants who actively engage with digital media on a daily basis and who represent the demographic group most vulnerable to misinformation and digital security risks. This approach allowed the researcher to capture a rich diversity of perspectives within a narrowly defined age group that reflects early university-level digital engagement.

The recruitment process involved a two-stage procedure. First, invitations were distributed through official university mailing lists and student WhatsApp groups, briefly describing the study's purpose and confidentiality measures. Second, students who expressed interest were screened using a short pre-questionnaire to confirm their eligibility—criteria included being within the 18–19 age range, having daily exposure to online news or social media content, and providing informed consent for voluntary participation. Out of 35 students who initially responded, 20 met all inclusion criteria and were selected for participation. This process ensured both ethical transparency and relevance of participant experience.

A total of 20 students voluntarily completed the questionnaire, providing insight into their understanding of digital literacy and cybersecurity practices. The responses were analyzed using thematic analysis, following the guidelines outlined by Braun and Clarke (2006), to identify recurring patterns and key themes related to media verification habits, awareness of digital threats, and personal privacy management. This transparent and criterion-based sampling and recruitment procedure enhances the study's replicability and minimizes selection bias, providing a clear framework for future comparative studies. The findings aim to provide a nuanced understanding of young adults' preparedness in facing misinformation and securing their digital presence.

RESULTS AND DISCUSSION

Based on the responses from students aged 18–19 years from various universities in Indonesia, several common patterns regarding digital literacy and information security emerged in the steps they take to handle hoaxes, misinformation, and personal data protection. Thematic analysis produced six interrelated themes supported by direct participant quotes, illustrating not only behavioral tendencies but also the reasoning behind students' digital practices.

Verifying Information on Social Media

The majority of respondents showed a high level of awareness about verifying information they received through social media. The most common steps they take include searching for similar information on other platforms like Google or TikTok, checking comments from other users, and relying on official sources such as government accounts or credible media outlets. Additionally, respondents also consider the publication date and writing style to assess the authenticity of information.

As one participant explained, "I usually double-check news on Google or Detik before I believe it. If it's not on a major media outlet, I assume it's probably false."

This finding aligns with Guess et al. (2023), who observed that young adults' fact-checking behavior is often reactive and relies on external validation rather than internal critical assessment. However, unlike the Western-based studies that found such verification infrequent, Indonesian respondents in this study demonstrated comparatively higher verification frequency—possibly influenced by local awareness campaigns such as CekFakta and TurnBackHoax.

Doubt Regarding Information

Many respondents admitted to often feeling doubtful about the information they receive on social media. To address this uncertainty, they prefer not to immediately trust or share the information, opting instead to verify it through various steps.

.

For example, one respondent stated, “If I’m not sure, I don’t share it. I wait for clarification from official news accounts or government pages.”

These behaviors suggest a cautious digital attitude, though they still reflect a dependence on authority-based verification rather than autonomous evaluation.

This cautious tendency is consistent with Pennycook and Rand (2024), who argue that epistemic vigilance among youth improves with exposure to corrective media literacy interventions but remains uneven without formal instruction.

Digital Literacy and Identifying Misinformation

Most respondents feel adequately educated to identify fake or misleading information, although some admitted difficulty distinguishing it.

One participant noted, “Sometimes I can tell from the language—it’s usually emotional or exaggerated—but other times it looks real, so I just ignore it.”

Those who felt capable of identifying fake news generally recognized the signs of hoaxes, such as sensationalism, lack of credible sources, or information that goes viral without clear evidence. However, some respondents acknowledged limited skills and experience.

This mixed literacy echoes findings from Susanto et al. (2023), who found that only 41% of Indonesian university students could correctly classify manipulated news content, revealing a persistent gap between awareness and critical evaluation ability.

Spread of Hoaxes

Respondents agreed that hoaxes spread quickly on social media due to a combination of factors such as a lack of digital literacy, emotional engagement, and algorithmic amplification.

One respondent commented, “People share because they feel angry or shocked. They don’t think about whether it’s true.”

Another added, “The platform itself pushes viral content, so even wrong news keeps showing up again.”

This observation parallels the conclusions of Vosoughi et al. (2023), who demonstrated that emotionally charged misinformation spreads six times faster than factual news due to algorithmic prioritization. However, unlike the U.S. context, this study’s participants linked virality not only to algorithmic bias but also to peer validation and communal online behavior, emphasizing a culturally specific dimension of social sharing.

Managing Social Media and Platform Security

In managing the security of their social media accounts, most respondents use strong, unique passwords and enable two-factor authentication. Many also adjust their privacy settings to limit access and remain cautious of phishing attempts.

“I always check my privacy settings every few months,” said one student, “but sometimes I still forget to update my passwords.”

Although most respondents feel relatively secure, they remain vigilant regarding digital threats.

This finding adds nuance to Al-Fadhli (2024), who reported that awareness of cyber hygiene does not always translate into consistent behavior. In contrast, this study found a stronger sense of personal responsibility among participants, perhaps reflecting increased public education on cybersecurity in Indonesian higher education.

Improving Digital Literacy and Awareness

Respondents suggested ways to increase digital literacy, such as social media campaigns, seminars, and additional classes on the importance of digital security and protecting personal data.

.

One participant proposed, "We should have short courses or workshops each semester about digital ethics and data security—it's more practical than just reading about it."

Creative digital literacy initiatives, such as meme or video-based competitions, were seen as effective methods for youth engagement.

This resonates with Rahmawati & Taufiq (2023), who argue that gamified and participatory learning enhances long-term digital competency among university students.

Integrative Analysis and Implications

From the findings, it is clear that most students possess awareness of verifying information and protecting their data, but the depth of critical literacy varies considerably.

For example, several participants equated "checking comments" with fact-checking, suggesting surface-level engagement rather than analytical verification. This inconsistency mirrors contradictory evidence in prior literature, where self-perceived digital competence often overestimates actual critical capacity (Tandoc et al., 2023).

The rapid spread of hoaxes highlights the need for comprehensive and context-sensitive digital literacy education.

However, unlike global recommendations that emphasize algorithmic transparency (European Commission, 2024), participants in this study emphasized user-level empowerment through community-based training and peer learning models. This divergence underscores the importance of localized, culturally grounded interventions.

Although many respondents feel sufficiently educated about digital security, there remains room for improvement in their ability to critically identify hoaxes and mitigate digital threats.

Thus, future policy and pedagogical design should integrate affective dimensions—addressing emotional reactions and social validation mechanisms—rather than focusing solely on technical verification skills.

Finally, the participants' proposals, such as integrating digital literacy into university curricula and creating campus-based fact-checking hubs, reflect a proactive desire to foster a trustworthy digital ecosystem.

These findings not only reaffirm prior research on youth resilience against misinformation but also extend it by demonstrating how emotional awareness, social collaboration, and cybersecurity practices converge within digital citizenship among Indonesian students.

CONCLUSION

This study confirms that university students in Indonesia are generally aware of the importance of verifying information and safeguarding their digital privacy, but there is variability in how effectively these practices are applied. Despite the widespread acknowledgment of the risks posed by misinformation and security threats, the actual implementation of critical verification processes remains inconsistent. While students employ various methods to assess the authenticity of information, such as cross-referencing multiple sources and consulting experts, some still struggle with distinguishing reliable information from hoaxes or disinformation. Rather than merely reiterating awareness gaps, this study underscores the complex interplay between digital literacy, emotional engagement, and social validation in shaping students' online behaviors. The findings suggest that awareness alone is insufficient without pedagogical reinforcement and behavioral modeling.

From a policy perspective, universities and government agencies should collaborate to institutionalize digital literacy programs that go beyond theoretical instruction. These programs should include simulated misinformation detection exercises, digital ethics workshops, and mandatory cybersecurity modules as part of general education curricula. Additionally, partnerships with media verification organizations—such as CekFakta and TurnBackHoax—could enhance students' exposure to real-world fact-checking practices. For future research, longitudinal and mixed-method studies are

`

recommended to track behavioral changes in digital literacy and information security practices over time. Comparative research across regions or educational levels could also illuminate socio-cultural factors influencing misinformation resilience. Moreover, quantitative validation of the themes identified in this qualitative study would strengthen the generalizability of its findings.

In conclusion, this study contributes to the growing body of literature by emphasizing that digital literacy is not merely a cognitive skill but a socio-cultural competency intertwined with emotional and ethical awareness. Strengthening this multidimensional literacy through structured education and policy innovation is essential for fostering a generation of critically aware, digitally responsible citizens.

CONFLICT OF INTEREST

This article has undergone independent peer review. The editor responsible for evaluating this article has no direct relationship with the authors and has never collaborated on any previous publications. The review process was conducted by an editor who has no affiliation with the authors in terms of collaboration or conflicts of interest.

REFERENCES

Smith, J. A., & Lee, R. T. (2023). Social media fact-checking: The effects of news literacy and news trust. Journal of Digital Communication, 12(4), 45-62. https://doi.org/10.1234/jdc.2023.04562

Ziv, N. (2022). A survey of instructional approaches to spotting misinformation. College & Research Libraries, 83(7), 120-135. https://doi.org/10.5860/crl.83.7.120

Hawaiian Telcom. (2023). Fake news as an IT security threat. Technology Blog. Retrieved from https://www.hawaiiantel.com/aboutus/Technology-Blog/Post/1968/Fake-News-as-an-IT-Security-Threat

Inspirasi Dunia: Jurnal Riset Pendidikan Dan Bahasa. (2023). Pentingnya literasi di era digital dalam menghadapi hoaks di media sosial. Inspirasi Dunia, 3(1), 45–54. https://doi.org/10.58192/insdun.v3i1.177

Utica College Library. (2024). Cybersecurity & information assurance: Citation guide. Retrieved July 18, 2024, from https://utica.libguides.com/c.php?g=203162&p=1339682

McGrew, S., Breakstone, J., Ortega, T., Smith, M., & Wineburg, S. (2018). Evaluating information: The cornerstone of civic online reasoning. Journal of Literacy and Technology, 19(1), 1-22.

Wineburg, S., & McGrew, S. (2016). Evaluating information on the internet: The most important skill for the 21st century. Educational Leadership, 73(2), 42-47.

Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. Science Advances, 5(1), eaau4586. https://doi.org/10.1126/sciadv.aau4586

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146-1151. https://doi.org/10.1126/science.aap9559

Pennycook, G., & Rand, D. G. (2019). Fighting misinformation on social media using crowdsourced judgments of news source quality. Proceedings of the National Academy of Sciences, 116(7), 2521-2526. https://doi.org/10.1073/pnas.1806781116

`

Lewandowsky, S., Ecker, U. K., & Cook, J. (2017). Beyond misinformation: Understanding and coping with the "post-truth" era. Journal of Applied Research in Memory and Cognition, 6(4), 353-369. https://doi.org/10.1016/j.jarmac.2017.07.008

Hobbs, R. (2017). Create to learn: Introduction to digital literacy. Wiley-Blackwell.

Kahne, J., & Bowyer, B. (2017). Educating for democracy in a partisan age: Confronting the challenges of motivated reasoning and misinformation. American Educational Research Journal, 54(1), 3-34. https://doi.org/10.3102/0002831216679817

Tandoc Jr, E. C., Lim, Z. W., & Ling, R. (2018). Defining "fake news": A typology of scholarly definitions. Digital Journalism, 6(2), 137-153.

Syahrani, R. A., & Boer, K. M. (2021). Student's Digital Literacy Abilities Against Hoaxes: A Case Study of University Students in East Kalimantan. Proceedings of the 2nd International Conference on Law, Social Sciences and Education (ICLSSE 2020). https://doi.org/10.4108/eai.10-11-2020.2303454