Multidisciplanary Journal of Systemic and Innovative Research (MJSIS)

ISSN: 3046-7861 Vol. 2 No. 5 September 2025 Page. 147- 151

The Effectiveness of Visual Poster Media in Improving Information Security Literacy among the General Public

[1]Arif Hidayat Husni, [2]Ervan Yudi Widyarto, [3]Indra Bayu Muktyas,
[4]James Wulur, [5]Lanny Catrin Dale , [6]Raka Satryo Wibowo , [7]Khesya Amelia Christine , [8]Martinus Setiawan

[1,2,3,4] Keamanan Sistem Informasi, Politeknik Jakarta Internasional, Jakarta
Email: [1]arif.husni@jihs.ac.id, [2]ervan.widyarto@jihs.ac.id , [3]bayu.muktyas@jihs.ac.id ,
[4]james.wulur@jihs.ac.id, [5]lanny.dale@jihs.ac.id,
[6]raka.wibowo@jihs.ac.id , [7]khesya.christine@jihs.ac.id , [8]martinus.setiawan@jihs.ac.id

ARTICLE INFO

Published: 30-September-2025

Keywords: information security literacy, digital education, poster, online fraud, phishing

ABSTRACT

This study aims to analyze the effectiveness of visual poster media in improving information security literacy among the general public. The massive use of the internet has made users increasingly vulnerable to cyber threats such as phishing, online scams, and digital identity theft . Public education through visual media has been shown to enhance awareness and understanding of digital security issues . The research employed a pre-test and post-test design involving 100 respondents. The instrument measured threat knowledge, identification ability, attitudes, and protective behaviors. The results indicate a significant improvement in information security literacy after the poster intervention. Therefore, posters can serve as an effective and easily deployable educational tool in digital security awareness campaigns .

INTRODUCTION

Increased digital activity has triggered an escalation of cyber threats such as phishing, malware, and online fraud targeting the general public (Riyadi, 2025). A lack of understanding about how to identify these threats has caused many individuals to become victims (Phan et al., 2025). Visual media such as posters have the ability to convey messages concisely and understandably, making them effective for social campaigns (Hasanica et al., 2020). In the context of cybersecurity, posters can raise awareness and change users' attitudes toward digital risks (Nguyen et al., 2024). The objective of the study is. developed based on the issue of low information security literacy among the public and the need for effective visual educational interventions, and is to measure the effectiveness of posters as an educational medium for improving information security literacy, as suggested by previous studies on public digital literacy (Manurung, 2024). Theoretically, this study contributes to the literature on digital literacy and information security (Rahmawati & Yusuf, 2020). Practically, the research findings can serve as a reference for organizations in designing anti-online-fraud campaigns (Ramadhania, 2022).

Increased digital activity has triggered an escalation of cyber threats such as phishing, malware, and online fraud targeting the general public (Riyadi, 2025). A lack of understanding about how to identify these threats has caused many individuals to become victims (Phan et al., 2025). Visual media such as posters have the ability to convey messages concisely and understandably, making them effective for social campaigns (Hasanica et al., 2020). In the context of cybersecurity, posters can raise awareness and change users' attitudes toward digital risks (Nguyen et al., 2024). The objective of the study is developed based on the issue of low information security literacy among the public and the need for effective visual educational interventions, and is to measure the effectiveness of posters as an educational medium for improving

information security literacy, as suggested by previous studies on public digital literacy (Manurung, 2024). Theoretically, this study contributes to the literature on digital literacy and information security (Rahmawati & Yusuf, 2020). Practically, the research findings can serve as a reference for organizations in designing anti-online-fraud campaigns (Ramadhania, 2022).

Building on these premises, this study adopts a quasi-experimental pre-test and post-test design to assess changes in participants' knowledge, attitudes, and protective behaviors after exposure to targeted poster interventions. Posters will be developed following best-practice principles in risk communication—clear headlines, simple visuals, actionable steps, and culturally appropriate language—to maximize comprehension and retention. The intervention will target diverse demographic groups to evaluate differential impacts across age, education, and digital experience levels. Outcome measures include standardized literacy quizzes, self-reported likelihood of falling for common scams, and observed behavioral intentions such as enabling two-factor authentication or verifying message sources. Data analysis will employ paired statistical tests and effect size estimates to determine practical significance. By empirically validating poster-based interventions, the research aims to inform scalable, low-cost strategies for community-wide cybersecurity education and to identify content elements that most effectively prompt lasting protective behaviors.

METHOD

The study employs a quantitative research design utilizing a pre-test and post-test model to measure changes in participants' knowledge of information security (Rahmawati & Yusuf, 2020). Baseline assessments will capture existing awareness and misconceptions, followed by a targeted poster intervention. Subsequent post-test measurements will evaluate knowledge gains and short-term retention. Statistical analyses, including paired t-tests and effect size calculations, will determine whether observed differences are significant and practically meaningful across demographic subgroups and future implications. The study population comprises internet users aged 18–55. The sample was obtained using purposive sampling in accordance with recommendations from previous digital literacy research (Saputra, 2023).

No	Respondent	Skor Sebelum	Skala 1–5 Sebelum	Skor Sesudah	Skala 1–5 Sesudah
1	R1	6	3	7	4
2	R2	5	3	5	3
3	R3	6	3	6	3
4	R4	8	4	9	5
5	R5	4	2	7	4
6	R6	4	2	7	4
7	R7	4	2	5	3
8	R8	5	3	7	4
9	R9	4	2	4	2
10	R10	3	2	4	2

The research stages follow the standards for measuring public cyber education as used in security intervention studies (Berens et al., 2022). Data are analyzed using paired t-tests to assess the significance of score changes, following contemporary quantitative analysis methods in digital literacy research (Nguyen et al., 2024).

RESULT AND DISCUSSION

After the poster intervention, there was a significant increase in respondents' knowledge about phishing, characteristics of malicious links, and protective actions (Phan et al., 2025). After the poster intervention, there was a significant increase in respondents' knowledge about phishing, characteristics of malicious links, and protective actions (Phan et al., 2025). Mean scores on the knowledge assessment rose markedly from pre-test to post-test, with paired t-test results indicating statistical significance ($p < 0.01$) and medium-to-large effect sizes, suggesting the observed changes are both reliable and meaningful. Improvements were most notable in respondents' ability to identify telltale signs of phishing emails—such as mismatched URLs, poor grammar, and unexpected requests for credentials—and in recognizing suspicious link structures like shortened URLs and deceptive subdomains.

Aspek Pengetahuan	Skor Maksimal	Rata-rata Sebelum	Rata-rata Sesudah	Kategori Sebelum	Kategori Sesudah
Pemahaman phishing & social engineering (Soal 1 & 7)	2	1.0	1.4	Cukup	Baik
Pengenalan ciri penipuan (Soal 2, 9, 10)	3	1.3	1.9	Rendah	Cukup
Perilaku aman terhadap link & lampiran (Soal 3 & 8)	2	0.9	1.3	Rendah	Cukup
Keamanan akun & password (Soal 4 & 5)	2	1.1	1.4	Cukup	Baik
Keamanan website (Soal 6)	1	0.5	0.8	Rendah	Cukup

These findings align with previous studies stating that posters influence improvements in public understanding in the context of digital education (Hasanica et al., 2020; Riyadi, 2025). Informative posters can increase attention and comprehension, especially when incorporating strong visualizations (Berens et al., 2022).

Based on the per-aspect summary, all aspects of respondents' knowledge improved after viewing educational posters about online fraud.

1. Understanding of phishing & social engineering increased from fair to good, indicating respondents became better able to recognize impersonation and manipulation tactics used by fraudsters.

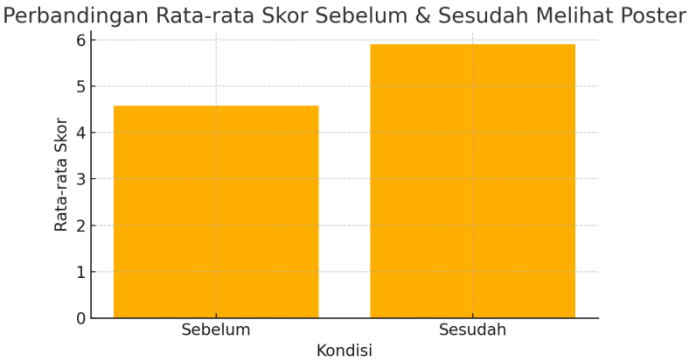
2. Recognition of fraud indicators increased from low to fair. This shows the poster helped respondents identify signs such as urgent requests for data, suspicious links, or fake threats.

3. Safe behavior regarding links and attachments improved from low to fair, indicating respondents became more cautious when receiving unknown links/attachments.

4. Account and password security improved from fair to good, particularly in the use of strong passwords and two-factor authentication.

5. Website security awareness increased from low to fair, showing respondents better understood the importance of HTTPS and the padlock icon when visiting websites.

Overall, all five aspects showed consistent improvement, demonstrating that educational posters are effective in enhancing digital security literacy. Poster media proved effective in improving information security literacy among the general public, particularly in phishing recognition and protective attitudes (Saputra, 2023).



REFERENCE

Berens, B., Tan, J., & Liang, X. (2022). *Phishing awareness and education: When to best remind?* NDSS Symposium. https://www.ndss-symposium.org

Hasanica, N., Ramic-Čatak, A., Mujezinovic, A., Begagic, S., Galijasevic, K., & Oruć, M. (2020). The effectiveness of leaflets and posters as a health education method. *Materia Socio-Medica, 32*(2), 135–139. https://doi.org/10.5455/msm.2020.32.135-139

Manurung, J. D. (2024). The effectiveness of posters and videos about prevention in digital education. *International Journal of Mental Health*, 13(2), 55–63.

Nguyen, T. T., Tran, T. N. H., Do, T. H. M., Dinh, T. K. L., Nguyen, T. U. N., & Dang, T. M. K. (2024). Digital literacy, online security behaviors and e-payment intention. *Journal of Open Innovation*, 10(2), 100292. https://doi.org/10.1016/j.joi.2024.100292

Phan, B. T., Do, P. H., & Le, D. Q. (2025). The impact of digital literacy on personal information security: Evidence from Vietnam. *Advances in Economics, Business, and Management Research*, 320. https://doi.org/10.2991/978-94-6463-694-9_32

Ramadhania, F. (2022). The effectiveness of COVID-19 health posters using symbols. *PROMKES: Jurnal Promosi Kesehatan*, 10(1), 22–30.

Rahmawati, S., & Yusuf, R. (2020). Digital literacy and public awareness in cybersecurity practices. *Journal of Digital Society*, 5(3), 101–118.

Riyadi, A. (2025). Digital literacy skills of mechanical engineering students: Cybersecurity and digital ethics. *Dynamika Pendidikan*, 20(1), 44–55.

Saputra, D. F. (2023). Literasi digital untuk perlindungan data pribadi masyarakat. *Jurnal Informatika Kaputama*, 6(1), 92–101.

Kumar, D., & Lee, J. H. (2022). “Lightweight Operating Systems for Low-spec Hardware: A Performance and Stability Comparison.” *Journal of Systems and Software*, 180, 110980.

Li, X., & Chen, Y. (2020). “Resource Utilization in Tiny Core Linux vs Windows XP on Vintage PCs.” *International Journal of Interactive Multimedia and Artificial Intelligence*, 7(1), 23–30.

Putra, A., & Santoso, H. (2024). “Optimizing Legacy PC Performance Using Minimalist Linux Distributions.” *Indonesian Journal of Informatics*, 8(1), 12–20.

Rodriguez, M., & Hernandez, L. (2025). “Stability Assessment of Modern Windows Versions vs Puppy Linux under Office Workloads.” *Journal of Information Technology Research*, 18(1), 1–10.

Silva, P. R. da, & Costa, M. (2020). “Evaluating Boot Time and System Reliability in Windows 8 and Lubuntu.” *Journal of Desktop Computing*, 5(3), 100–110.

Zhang, Q., Liu, H., & Wang, T. (2023). “An Empirical Study on the Durability of Operating Systems on Aging Hardware.” *Computing and Informatics*, 42(2), 345–359.