International Journal of Science Education and Cultural Studies

Cybersecurity Education Strategies Based on Open-Source Intelligence (OSINT) to Enhance Public Awareness

Taufik Hidayat
Department of Computer Engineering, Universitas Wiralodra, Indramayu, Indonesia

Budi Wibowo
Department of Informatics Engineering, Institut Teknologi Budi Utomo Jakarta, Indonesia

Andrie Yuswanto
Department of Informatics Engineering, Institut Teknologi Budi Utomo Jakarta, Indonesia

Annisa Fathul Jannah
Department of Informatics Engineering, Institut Teknologi Budi Utomo Jakarta, Indonesia

Abstract: In today's rapidly evolving digital landscape, cybersecurity threats are escalating in both frequency and complexity, which points to the urgent need for effective educational approaches to enhance public awareness. Open-Source Intelligence (OSINT), which leverages publicly available information, offers a practical framework for identifying and understanding cyber risks. This study proposes the design, implementation, and evaluation of an OSINT-based cybersecurity education strategy aimed at non-technical audiences. Employing a mixed-methods approach including literature review, module development, and surveys, this research measures the strategy's effectiveness in improving cybersecurity comprehension. The results indicate that the OSINT-based educational approach significantly enhances participants' understanding of cyber risks, yielding an average increase of 35% in comprehension scores. Furthermore, the integration of real-world OSINT demonstrations makes cybersecurity threats more tangible and personally relevant, thereby motivating proactive preventive behavior. In conclusion, incorporating OSINT into cybersecurity education provides an effective and scalable strategy for improving public awareness and resilience against modern digital threats.

Keywords: OSINT, cybersecurity education, public awareness, threat mitigation.

Correspondents Author:
Budi Wibowo, Department of Informatics Engineering, Institut Teknologi Budi Utomo Jakarta, Indonesia
Email: budiwibowo1993@gmail.com

Received September 26 2025; Revised October 17, 2025; Accepted October 18, 2025; Published October 19, 2025.

Introduction

The rapid advancement of digital technologies has transformed modern society, providing significant convenience and efficiency in communication, business, and daily life. However, this digital dependency has also amplified vulnerabilities in the cyber domain. Cyberattacks such as phishing, malware infections, and identity theft are increasingly targeting individuals often the weakest link in the cybersecurity chain due to limited awareness and inadequate security practices (Addison et al., 2025). Recent surveys indicate that nearly 65% of global internet users remain unaware of the cybersecurity threats they face daily (Ainslie et al., 2023). This lack of understanding underscores the urgent need for effective public cybersecurity education.

While various cybersecurity education initiatives have been introduced, most existing programs are designed primarily for technical audiences, such as IT specialists and cybersecurity professionals (Baltuttis & Teubner, 2024). As a result, individuals with limited technical backgrounds are often neglected and remain vulnerable to cyber threats. Furthermore, traditional educational approaches, such as one-way seminars and theoretical lectures, have proven insufficient in promoting long-term behavioral change, as they often fail to engage participants or demonstrate real-world cyber risks effectively (Beu et al., 2023).

In contrast, Open-Source Intelligence (OSINT) has emerged as a powerful tool within professional cybersecurity practice (Budi Wibowo & MT, 2025). OSINT refers to the systematic collection and analysis of publicly available information from sources such as social media, websites, and online forums (Cheng & Wang, 2022). It enables cybersecurity professionals to detect potential threats, identify vulnerabilities, and monitor malicious activities (Dupont et al., 2023). Tools such as Shodan, Maltego, and Google Dorking have become standard instruments in threat intelligence and digital forensics (Fenech et al., 2024). However, despite its extensive use in professional settings, the educational potential of OSINT for non-technical audiences remains largely unexplored (De Arroyabe et al., 2023).

A review of the current state of the art reveals a clear research gap at the intersection of OSINT and public cybersecurity education. Existing studies have yet to establish (1) a structured pedagogical framework for translating OSINT concepts into accessible learning for non-technical users (Kemp, 2023); (2) methods to make cybersecurity risks feel tangible and personally relevant to the general public; and (3) ethical guidelines for teaching potentially dual-use OSINT tools in an educational context (Mahmood et al., 2024). Addressing these gaps requires a paradigm shift in how OSINT is perceived—not merely as a professional intelligence tool, but as a public education and digital self-defense mechanism.

Therefore, this study introduces a novel framework that integrates OSINT into public cybersecurity education. The primary contribution of this research is the development and empirical evaluation of an OSINT-based educational strategy designed to increase cybersecurity awareness and understanding among non-technical audiences. Specifically, this study aims to:

1. Design a structured OSINT-based cybersecurity education model for the public,
2. Implement this model through interactive and context-driven educational modules, and
3. Evaluate its effectiveness in improving public awareness and comprehension of cybersecurity threats.

By bridging the gap between professional intelligence practices and public digital literacy, this study contributes to the advancement of inclusive and practical cybersecurity education.

Research Method

This section describes the systematic steps undertaken to achieve the research objectives and the methods used for data collection and analysis. The study adopts a mixed-methods approach, integrating both qualitative and quantitative techniques with an emphasis on the application of Open-Source Intelligence (OSINT) to support cybersecurity education (McIntosh et al., 2024). The research began with problem identification, which focused on determining the public's knowledge gap in cybersecurity and exploring the potential of OSINT as an educational tool to bridge this gap (Naseer et al., 2023). This was followed by a literature review that analyzed previous studies, scientific journals, and institutional reports to establish a strong theoretical foundation. The review also covered the effectiveness of cyber education programs and the technical applications of OSINT tools such as Shodan, Maltego, and Google Dorking (Hafiz & Hidayat, 2025; Popoola et al., 2024). Based on these findings, an educational strategy was designed through the development of OSINT-based modules tailored to different levels of public understanding from beginner to intermediate. These modules included real-world case studies and live demonstrations to enhance engagement and practical comprehension (Prümmer et al., 2024). The overall research process was structured into several stages as illustrated in Figure 1.

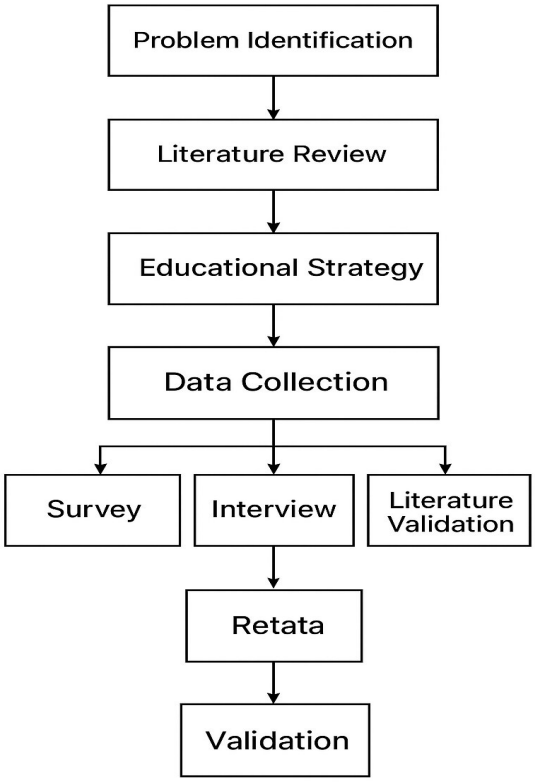

Figure 1 Research framework of the OSINT-based cybersecurity education strategy

The framework illustrates the sequential stages of the research process, beginning with problem identification and literature review, followed by educational strategy design, data collection (surveys, interviews, and literature validation), and data analysis using both quantitative and qualitative approaches. The process concludes with validation through the t-test and effectiveness evaluation of the OSINT-based educational modules.

The data collection process was conducted through three main channels. First, surveys were distributed to 100 respondents from diverse backgrounds, including students, professionals, and the general public, to measure their initial and final understanding of cybersecurity (Taherdoost, 2024). Second, in-depth interviews with OSINT practitioners were carried out to gain insights into the effective and ethical implementation of OSINT-based educational strategies (Taherdoost, 2024). Third, a continuous literature review was used to triangulate and validate findings. In the data analysis phase, quantitative data from the surveys were statistically analyzed to assess the change in participants' understanding, while qualitative data from interviews were examined to provide contextual interpretation (Dioubate et al., 2022). The overall effectiveness of the OSINT-based education strategy was determined using a mathematical effectiveness model, which measured the percentage of improvement in cybersecurity comprehension. The model is expressed as:

$$E = \frac{\Delta K}{t} \times 100\% \quad (1)$$

where E represents the effectiveness of the educational strategy (in percentage), ΔK is the average change in cybersecurity comprehension scores before and after the program, and t denotes the duration of the educational intervention (in hours). The results were subsequently validated using a statistical t-test to determine whether the observed improvement in comprehension scores was statistically significant. This validation process ensured that the OSINT-based educational strategy yielded measurable enhancements in public cybersecurity awareness and understanding (Yadav et al., 2024).

Result and Discussion

This section presents and discusses the main results of the study in relation to the research objectives. The findings confirm that the proposed OSINT-based cybersecurity education strategy significantly enhances public understanding of cyber threats. Based on a survey of 100 respondents from various backgrounds, the results indicate an average increase of 35% in cybersecurity comprehension scores after participation in the educational program. Among all groups, the general public recorded the highest improvement of 33.3%, suggesting that non-technical users benefit most from interactive and practical learning approaches. The educational modules utilizing OSINT tools such as Shodan, Maltego, and Google Dorking effectively captured participants' interest, particularly among students and IT professionals, as shown in Fig. 1 which illustrates the respondent demographics by age group.

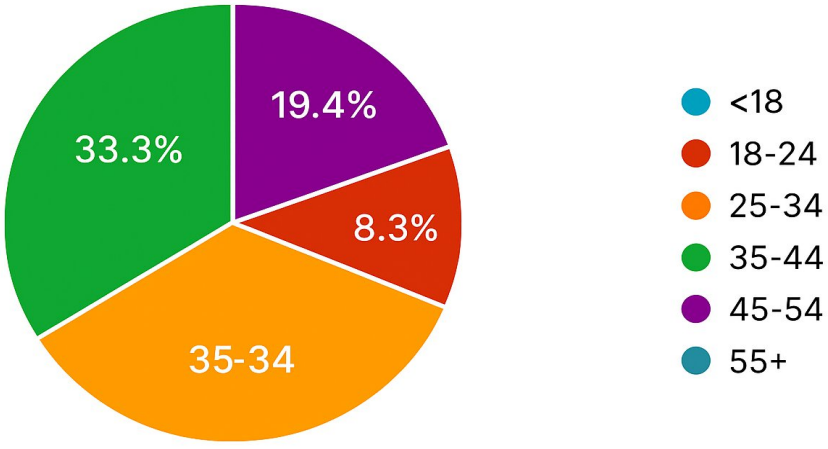

Figure 1 Respondent Demographics by Age Grou

The results strongly support the hypothesis that an OSINT-based learning approach has a positive and measurable impact on raising cybersecurity awareness. Compared to traditional

methods such as lectures or seminars, the experiential learning format of OSINT-based training proved more effective. For instance, using Shodan to visualize exposed Internet of Things (IoT) devices allowed participants to recognize real-time vulnerabilities and understand personal risk exposure. This finding aligns with previous studies reporting that hands-on or experiential learning improves comprehension by up to 30% compared with passive learning methods (Yadav et al., 2024). Such real-world demonstrations make cybersecurity threats tangible and personal, reinforcing behavioral change rather than theoretical awareness.

In addition to its effectiveness, this approach fostered community engagement by encouraging participants to actively explore OSINT tools to assess their own digital exposure, such as identifying leaked credentials or unsecured devices. As depicted in Fig. 2, the most preferred media for learning about cybersecurity included interactive workshops, online simulations, and discussion forums. These findings emphasize the potential of OSINT-based training to stimulate collective awareness and active participation in cyber hygiene practices.

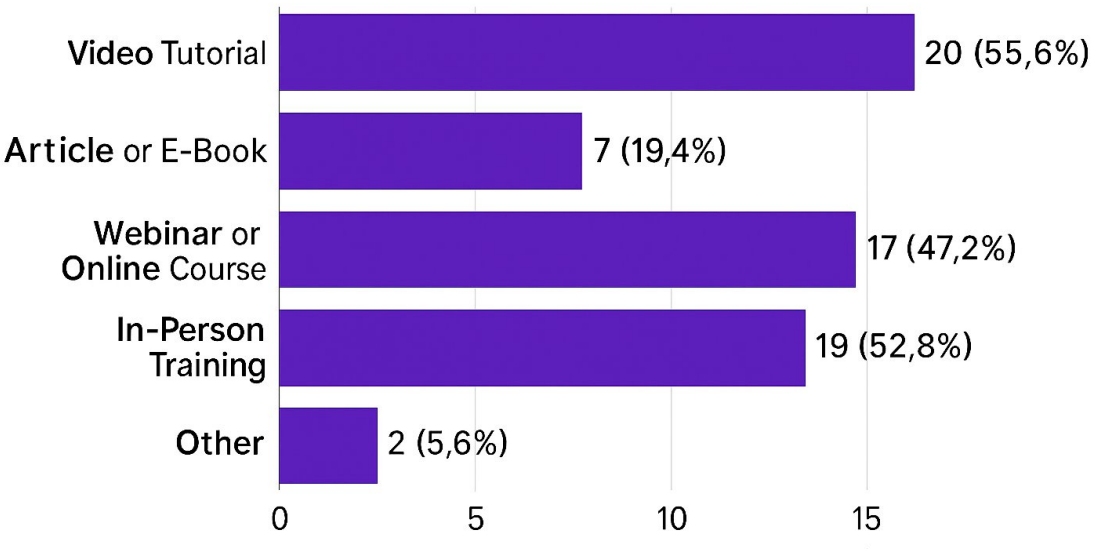

Figure 2 Most Preferred Media to Learn About Cybersecurity

However, several challenges were also identified during implementation. Differences in participants' initial understanding levels and limited training time reduced learning consistency across groups. Moreover, inherent issues with OSINT persist, including the risk of information misuse, ethical concerns, and the difficulty of filtering relevant data from vast open sources. To address these limitations, the study recommends the incorporation of ethical frameworks and data privacy guidelines into OSINT-based training programs. Furthermore,

future developments could explore augmented reality (AR) or simulation-based environments to enhance interactivity and efficiency in training delivery.

The implications of this research are significant for academia, policymakers, and the cybersecurity community. Integrating OSINT into formal cybersecurity curricula—from schools to professional certification programs can help bridge the knowledge gap for non-technical audiences. Community-driven initiatives such as hackathons, awareness campaigns, and live attack simulations are also recommended to sustain engagement and promote long-term awareness. Finally, ongoing evaluation mechanisms such as periodic surveys and longitudinal studies should be implemented to measure the sustained impact of OSINT-based education on reducing cyber incidents caused by human error.

In summary, the findings demonstrate that OSINT-based cybersecurity education effectively increases public understanding and engagement by making cyber risks more tangible and relatable. The 35% increase in comprehension validates the strategy's success, confirming that contextual and experiential learning represents a superior model for public cybersecurity awareness compared to traditional educational methods.

Conclusions

This study demonstrated that integrating OSINT into cybersecurity education significantly enhances public understanding and awareness of digital threats. By combining theoretical and practical learning components, the proposed OSINT-based educational strategy achieved an average 35% increase in comprehension scores, confirming its effectiveness for non-technical audiences. The application of real-world OSINT tools such as Shodan, Maltego, and Google Dorking provided participants with direct, experiential insights into cyber risks, making the learning process more tangible and engaging. The findings validate that hands-on, context-driven approaches outperform traditional lecture-based methods in promoting behavioral change and improving digital literacy.

Beyond increasing awareness, this research introduces a structured framework for employing OSINT as a public digital self-defense tool, effectively bridging the gap between professional cybersecurity practices and community education. Nevertheless, several challenges remain, including variations in participants' prior knowledge, limited training time, and potential ethical concerns regarding OSINT misuse. To mitigate these challenges, future work should explore adaptive learning technologies, such as augmented and virtual reality simulations, and establish clear ethical and legal guidelines for safe OSINT education. In conclusion, OSINT-based cybersecurity education provides a scalable and impactful approach to strengthening public resilience against evolving cyber threats. Collaboration among

educational institutions, government agencies, and cybersecurity organizations is crucial to expanding its implementation, ensuring that cybersecurity literacy becomes an accessible, practical, and ethical foundation of modern digital citizenship.

References

Addison, S. K., Tahir, M., & Isoaho, J. (2025). Experimental Implementation of a Low Cost Real-Time Threat Intelligence Solution for Smart Home Security. *Procedia Computer Science, 257*, 575-582.

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security, 132*, 103352.

Baltuttis, D., & Teubner, T. (2024). Effects of visual risk indicators on phishing detection behavior: An eye-tracking experiment. *Computers & Security, 144*, 103940.

Beu, N., Jayatilaka, A., Zahedi, M., Babar, M. A., Hartley, L., Lewinsmith, W., & Baetu, I. (2023). Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation. *Computers & Security, 131*, 103313.

Budi Wibowo, S., & MT, T. H. (2025). *OSINT FOR DUMMIES: Jurus Ninja Digital dalam Menguak Rahasia Internet!* PENERBIT KBM INDONESIA.

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information, 13*(4), 192.

De Arroyabe, I. F., Arranz, C. F., Arroyabe, M. F., & de Arroyabe, J. C. F. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers & Security, 124*, 102954.

Dioubate, B. M., Daud, W., & Norhayate, W. (2022). Cyber security risk management frameworks implementation in Malaysian higher education institutions. *International journal of academic research in business and social sciences, 12*(4), 1356-1371.

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security, 132*, 103372.

Fenech, J., Richards, D., & Formosa, P. (2024). Ethical principles shaping values-based cybersecurity decision-making. *Computers & Security, 140*, 103795.

Hafiz, L., & Hidayat, T. (2025). Unveiling the Cybercrime Ecosystem: Impact of Ransomware-as-a-Service (RaaS) in Indonesia. *International Journal of Science Education and Cultural Studies, 4*(1), 11-21.

Kemp, S. (2023). Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. *Computers & Security, 127*, 103089.

Mahmood, S., Chadhar, M., & Firmin, S. (2024). Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector. *Journal of Contingencies and Crisis Management, 32*(1), e12549.

McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From cobit to iso 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Computers & Security, 144*, 103964.

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. *Computers & Security, 135*, 103525.

Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions. *Blockchain: Research and Applications, 5*(2), 100178.

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136*, 103585.

Taherdoost, H. (2024). A critical review on cybersecurity awareness frameworks and training models. *Procedia Computer Science, 235*, 1649-1663.

Yadav, P., Kumar, A., Mishra, S. K., & Kochhar, K. (2024). Financial equality through technology: Do perceived risks deter Indian women from sustained use of mobile payment services? *International Journal of Information Management Data Insights, 4*(2), 100266.