Jurnal Pengabdian Masyarakat: Sekolah Aman dari Phising dan Scam
Vol. 2 No. 1, May 2025, 41-53
ISSN Online: 3064 - 0415, https://doi.org/10.56447/jpmbistek
Published by LPPM, STMIK Mardira Indonesia, Bandung.

Save Your Data, Save Your Money "Schools Safe From Phishing and Scams"

Asep Ririh Riswaya[1], Suwandana Suryana Putera[2], Aep Syaripudin[3], Agni Ahmad Saripudin[4], Alfi Yudin Raihan[5], Aris Koharudin Farras[6], Muhammad Naufal[7], Sandri Arya Fikriawan[8], Septian Adiraharja[9], Sigit Aprilian[10], Sirozudin Ibnu Farhan[11]
[1,2,3,4,5,6,7,8,9,10,11] *STMIK Mardira Indonesia, Bandung*
*Email: asep.ririh@stmik-mi.ac.id**

Abstrak

In an increasingly sophisticated digital age, information security, or cybersecurity, has emerged as a significant challenge that is frequently misunderstood by the public, particularly among demographics with limited exposure to technology. An illustrative instance is evident in the Yayasan Badru environment, where participants exhibit inadequate comprehension of the perils associated with the digital realm and the measures to avert cybercrime. The primary objective of this educational activity is to impart a fundamental comprehension of cybersecurity, equipping participants to identify diverse digital threats, grasp prevalent terminology in the cybersecurity domain, and recognize applicable prevention strategies for their daily digital engagements.

This exercise employs a qualitative methodology that includes direct observation and active engagement with participants. The material is presented in an accessible manner, customized to the participants' understanding, addressing subjects including phishing, malware, personal data theft, and secure browsing practices. The findings of this activity demonstrate an enhancement in participants' awareness and attentiveness concerning diverse types of digital crime. Participants have adopted a more prudent approach to utilizing digital devices and may use fundamental cybersecurity principles in their daily lives.

In conclusion, cybersecurity education has demonstrated efficacy in enhancing digital literacy and providing preliminary protection for the community against the hazards associated with technological growth. This education must be ongoing to develop a secure, risk-conscious digital society prepared to confront future difficulties in the online realm.

Keywords: *Cybercrime, Cybersecurity, Digital World*

Introduction

The study highlighted some critical issues that impede the adequate comprehension of cybersecurity among participants. There is a considerable deficiency in audience understanding of the "dangers of the digital world." A significant number of participants lack familiarity with these dangers and are unaware of preventive measures, leading to a limited understanding of fundamental cybersecurity terminology and ideas. This lack of comprehension is a significant risk, rendering people susceptible to exploitation and digital hazards, including phishing and scamming.

Furthermore, the observations indicated that individuals often lack adequate self-protection measures in the digital domain. Many individuals utilize weak passwords and indiscriminately download links, thereby heightening their susceptibility to cybercrime. Moreover, there is a lack of systematic instructional tools; prior to the training, the material had not been presented in an organized fashion. Preliminary observations revealed the absence of structured approaches to improve participants' comprehension of cybersecurity concepts effectively.

After the intervention, the effects became apparent. Participants demonstrated heightened vigilance and effectively applied their cybersecurity expertise in practice. They acquired a deeper understanding of relevant language, the threats they encounter, and effective strategies for preventing cybercrime. This finding emphasizes that the primary obstacles were from insufficient awareness and education, underscoring the necessity for ongoing educational initiatives to enable individuals to navigate the digital realm securely.

The primary concern identified is the deficiency in fundamental digital literacy, especially regarding cybersecurity. Participants lack comprehension of hazards, fail to identify indicators of digital threats, and exhibit inadequate security practices while navigating the internet. This exposes them to possible vulnerabilities to attackers. The issue arises from three primary sources: an inadequate basic comprehension of digital ideas and cybersecurity, a deficiency in systematic and structured instruction or training, and the lack of proactive behavioral modifications prior to the intervention.

A multi-stage problem-solving technique can be created to tackle these challenges—assessment of Requirements and Preliminary Literacy Proficiency. Perform a preliminary evaluation to ascertain participants' comprehension of the digital realm and cybersecurity. Employ questionnaires, brief surveys, or basic pre-assessments. Material Design should commence with fundamental principles (such as the nature of the internet and digital footprints) and progress to more complex topics (including phishing, scams, and data protection). The information must be organized according to a contextual learning framework, including real-world case studies. Interactive Educational Methods will utilize active learning strategies, encompassing case simulations, role-playing, interactive quizzes, and gamification. Offer tangible illustrations, including the formulation of robust passwords and the enactment of phishing email scenarios.

Continuous Monitoring and Evaluation must incorporate a post-test to evaluate enhancements in comprehension and behavioral modifications. Further sessions or advanced modules may supplement this to enhance long-term understanding.

Literature and contemporary studies suggest that improving digital literacy and cybersecurity is a strategic measure to combat the growing complexity of digital threats. In Indonesia, this necessity is amplified by the substantial rise in internet users, which is not paralleled by an equivalent enhancement in digital awareness.

The UNESCO Digital Literacy worldwide Framework (2018)** underscores the significance of digital security education within the worldwide educational curriculum, notably in safeguarding individuals against threats such as phishing, data theft, and online manipulation. Data from the **Kominfo–Katadata Insight Center (2022)** indicates that merely 24.1% of Indonesian internet users can identify phishing emails, while 34.3% are unaware of how to report personal data misuse. More than 50% of users use inadequate data protection measures.

Field findings at Yayasan Badru indicate a substantial deficiency in fundamental digital literacy, since participants lack familiarity with concepts such as phishing, fraud, and malware. Global research underscores the importance of literacy as a fundamental requirement, necessitating effective literacy interventions. Self-protective behaviors, such as employing weak passwords and engaging with arbitrary links, underscore the significance of daily preventive measures. There is a necessity for direct and practical training, together with organized educational methodologies. According to UNESCO, a digital citizenship curriculum is needed, in conjunction with a suitable educational medium. The intended audience, comprising religious groups, has not yet been engaged by formal initiatives. Global research frequently emphasizes students in formal industries, underscoring the necessity for contextual and value-oriented methodologies.

Impact Evaluation Following the seminar, participants exhibited enhanced comprehension and awareness. The study advocates for continuous monitoring; nevertheless, a long-term evaluation has yet to be performed.

Growing Internet User Base and Escalating Cyber Threats: The number of internet users in Indonesia has surged from 110 million in 2015 to over 216 million in 2023. A poll conducted by **Kominfo–Katadata (2022)** reveals that merely 24.1% of consumers can identify phishing emails or viruses; 32.3% are unaware of how to utilize antivirus software; and 34.3% lack knowledge on reporting online data misuse. Public knowledge is deficient, with over 75% failing to identify phishing attempts and more than 50% employing insufficient data protection methods. The amalgamation of inadequate digital literacy and hazardous behaviors heightens dangers for individuals and the community, rendering those unfamiliar with phishing or data protection vulnerable to identity theft, financial detriment, and even psychological repercussions.

Proposed Solutions: The solution entails educating participants via a lecture aimed at fostering a secure school environment against phishing and scams. The seminar will consist of two sessions: the initial session will address cybercrime, followed by a Q&A session to debate the offered content. To evaluate participants' knowledge, we will implement a rating exercise in which they respond to questions derived from the information presented during the seminar. This evaluation employs a qualitative method.

Primary Limitations: The population comprises participants (volunteers/staff) at Yayasan Badru in Bandung. The employed approaches include observation and descriptive interviews, devoid of complicated statistical analysis. The material emphasizes awareness and fundamental cybersecurity measures (including terminology, hazard identification, and prevention), excluding sophisticated technical details.

Expected Outcomes: The projected results encompass an enhancement in knowledge and awareness, a measurable effect assessment, and modifications in digital behaviors and routines. This paper's originality lies in its capacity to elucidate cybercrime among individuals primarily engaged in religious issues during a time of advanced digital threats. Furthermore, it incorporates a complementary assessment via a rating exercise derived from questions posed during the session.

Research Objective: This study seeks to fulfill the genuine requirements of Yayasan Badru by developing quantifiable techniques to improve fundamental cybersecurity literacy and safeguarding.

Method

This community service project employs a qualitative descriptive study design. This study seeks to thoroughly and accurately delineate participants' understanding, awareness, and behavioral modifications about digital risks, including phishing and fraud. The researcher engages in all tasks, from preparing and executing the seminar to assessing the outcomes. This research primarily focuses on the process of educational engagement and the concrete effects of the activities on participants.

The study population comprises all seminar attendees, encompassing middle and high school students at Yayasan Badru in Cimahi. The sample is chosen using purposive sampling, predicated on the active engagement of participants in the seminar. The primary sample comprises 25 people who actively attended and participated in the Q&A session and interactive quiz. The sampling emphasizes people exhibiting significant passion and engagement in the events.

Data gathering is performed via direct observation during events, unstructured interviews with various participants and foundation staff, and the administration of pre-tests and post-tests via an interactive quiz titled "Ranking 1." The tools created consist of inquiries derived from the content delivered in the educational session. These inquiries aim to assess participants' comprehension of fundamental cybersecurity principles, categories of digital dangers, and the preventive measures they can implement.

The data is examined qualitatively and descriptively through a comparison method between pre-test and post-test findings to evaluate changes in participants' knowledge and awareness. Furthermore, the data from observations and interviews are examined by synthesizing answer patterns, participant actions throughout activities, and perceptions recorded by the facilitators. The findings of this research are utilized to assess the efficacy of the implemented instructional methodologies and to formulate improved educational methods for the future.

Results and Discussion

On June 14, 2025, the initial phase of community service activities involved securing authorization and submitting a notification letter from STMIK Mardira Indonesia to the Badru Foundation for an event aimed at junior high and high school students. The notification permit letter was delivered by student representatives to the Badru Foundation, which received it positively.

Figure 1. Submission of Notification Letter to the Badru Foundation

On June 22, 2025, a community service team of academics and students from STMIK Mardira Indonesia conducted a Community Service (PKM) program. This initiative was conducted to benefit the broader community by offering educational outreach on Cyber Security and contemporary digital security to junior and senior high school students at the Badru Foundation, Jl. Budi No. 58, Pasirkaliki, North Cimahi District, Cimahi City, West Java 40514.

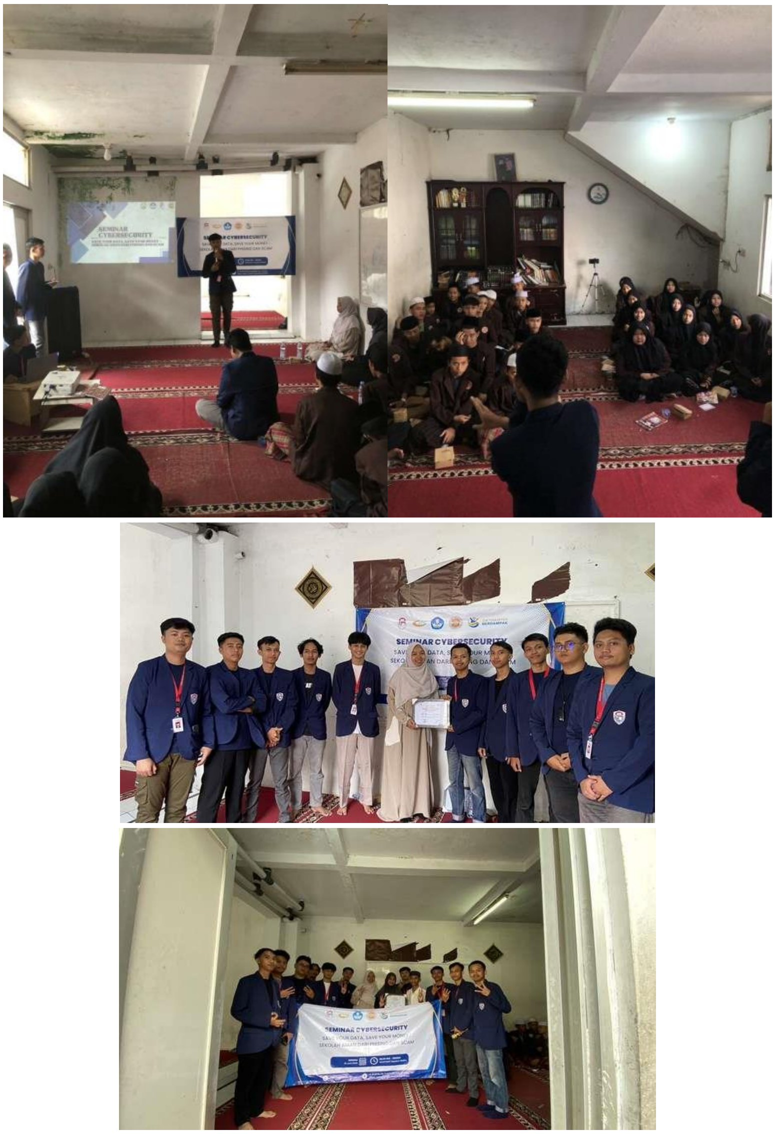

Figure 2. Community Service Activities

The findings of this community project, particularly concerning the students of the Badru Foundation, suggest that they should exercise caution when interacting with social media (e.g., clicking on unfamiliar links). The children were highly engaged during the event, facilitating a seamless transition. This document outlines the execution of the Community Service Program (PKM) at the Badru Foundation.

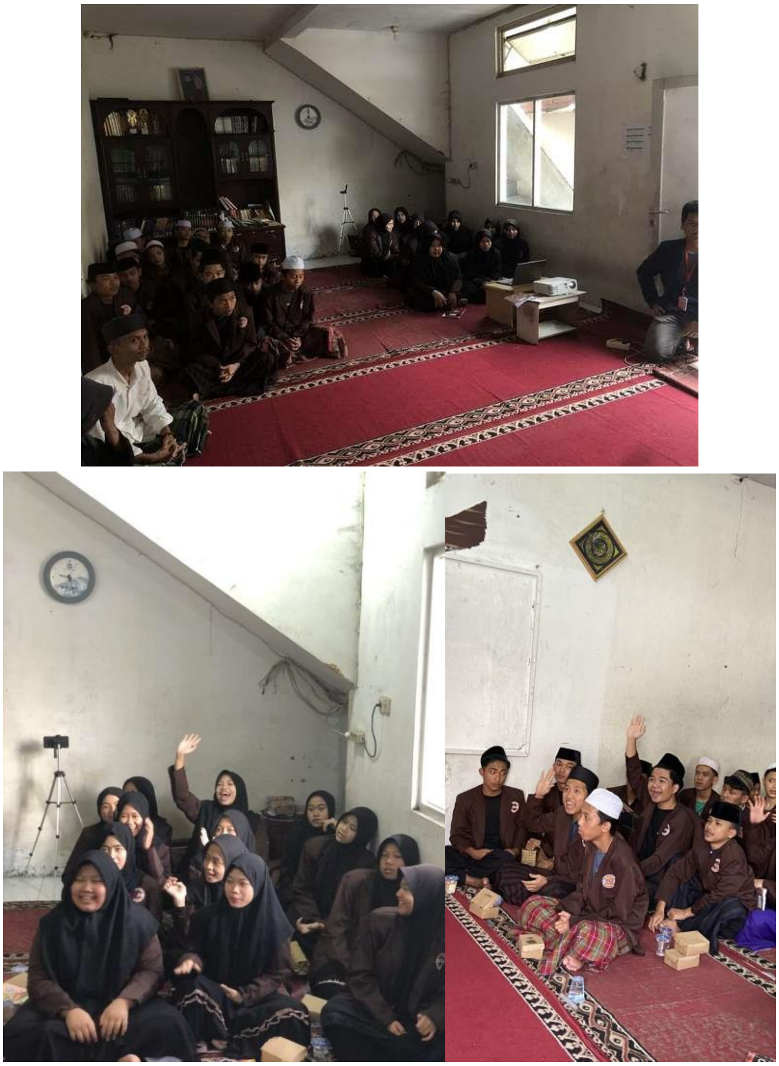

Figure 3. Implementation of Joint Activities with the Badru Foundation

SEMINAR CYBERSECURITY
SAVE YOUR DATA, SAVE YOUR MONEY :
SEKOLAH AMAN DARI PHISING DAN SCAM
BIKIN GADUH SE-INDONESIA, SIAPA "HACKER" BJORKA?

Figure 4. Implementation of Material Presentation

The findings of this community project, particularly concerning the students of the Badru Foundation, suggest that they should exercise caution when interacting with social media (e.g., clicking on unfamiliar links). The children were highly engaged during the event, facilitating a seamless transition. This document outlines the execution of the Community Service Program (PKM) at the Badru Foundation.

Conclusion

The execution of the educational initiative "Safe School from Phishing and Scam" at Yayasan Badru has yielded highly favorable outcomes. Through the application of relatable methodologies and engaging pedagogical techniques, such as case simulations and games, participants have gained a deeper understanding of digital threats, including phishing and fraud. They have begun to exhibit more prudent habits while utilizing the internet.

This initiative effectively engaged community groups that have historically had limited exposure to technology training, especially those with religious affiliations. This illustrates that digital security education may be efficiently imparted using a comprehensible method adapted to practical circumstances, without dependence on intricate technical jargon. The employed strategies can exemplify effective instruction in analogous places.

This initiative must be extended to areas with analogous requirements. Educational material should be developed, including movies, animations, or applications that facilitate comprehension. The curriculum could incorporate subjects such as safeguarding personal data, utilizing VPNs, and identifying progressively intricate internet hoaxes.

Crucially, education on digital security must extend beyond a singular encounter. Cooperation among educational institutions, communities, and governmental bodies is essential for the sustainability and lasting impact of programs like this. The objective is to foster a generation that is adept in technology usage while also being equipped to safeguard themselves against cyber risks.

References

UNESCO. (2018). *A global framework of reference on digital literacy skills*. https://unesdoc.unesco.org/ark:/48223/pf0000265403

Katadata Insight Center & Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). *Status literasi digital Indonesia 2022*. https://literasidigital.id/pustaka/status-literasi-digital-indonesia-2022

APJII. (2023). *Laporan Survei Internet APJII 2023: Penetrasi & Perilaku Pengguna Internet Indonesia*. Asosiasi Penyelenggara Jasa Internet Indonesia. https://apjii.or.id/survei2023

Katadata Insight Center & Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). *Status literasi digital Indonesia 2022*. https://literasidigital.id/pustaka/status-literasi-digital-indonesia-2022