JURPIKAT (Jurnal Pengabdian Kepada Masyarakat)
Vol. 6 No. 4 (2025) pp. 2742-2762
https://jurnal.politeknik-kebumen.ac.id/index.php/jurpikat
p-ISSN : 2746-0398 e-ISSN : 2746-038X

Empowering Teachers in Muhammadiyah Boarding School Yogyakarta toward Safer Digital Behavior through Smartphone Security Education

Aris Rakhmadi[1,2*], Hero Wintolo[1,3], Esi Putri Silmina[1,4], Dewi Soyusiawaty[1], Sunardi[5], Abdul Fadlil[5]

[1]Department of Informatics, Universitas Ahmad Dahlan, Indonesia, 55166
[2]Department of Informatics Engineering, Universitas Muhammadiyah Surakarta, 57169
[3]Department of Informatics, Adisutjipto Institute of Aerospace Technology, Indonesia, 55198
[4]Department of Information Technology, Universitas 'Aisyiyah Yogyakarta, Indonesia, 55292
[5]Department of Electrical Engineering, Universitas Ahmad Dahlan, Indonesia, 55166

E-mail:* aris.rakhmadi@ums.ac.id
Doi : https://doi.org/10.37339/jurpikat.v6i4.2843

Info Artikel:
Diterima :
2025-11-04

Diperbaiki :
2025-11-15

Disetujui :
2025-11-17

Kata Kunci: Literasi Digital; Keamanan Smartphone; Pemberdayaan Masyarakat; Pelatihan Guru; Pendidikan Muhammadiyah

Abstrak: Program pengabdian masyarakat ini dilaksanakan melalui *Program Pemberdayaan Umat* (PRODAMAT) Universitas Ahmad Dahlan dengan tujuan meningkatkan literasi digital dan kesadaran keamanan siber bagi guru di *Muhammadiyah Boarding School (MBS)* Yogyakarta. Kegiatan difokuskan pada edukasi keamanan akun di *smartphone* melalui langkah praktis seperti pengelolaan kata sandi, aktivasi autentikasi dua faktor (2FA), dan kewaspadaan terhadap *phishing*. Pendekatan partisipatif dilakukan melalui pelatihan yang diikuti oleh 15 guru dan staf melalui diskusi interaktif, demonstrasi, serta evaluasi *pretest–posttest*. Hasil menunjukkan peningkatan rata-rata skor pengetahuan dari 4,63 menjadi 4,90, sikap dan kesadaran digital dari 4,05 menjadi 4,45, serta niat dan perilaku aman digital dari 4,35 menjadi 4,73. Peningkatan ini mencerminkan perubahan positif pada pemahaman, kesadaran, dan perilaku peserta dalam menjaga keamanan digital. Program ini menegaskan pentingnya integrasi keterampilan teknologi dengan nilai etika dan keagamaan untuk mendorong pemberdayaan digital berkelanjutan di lingkungan pendidikan Islam.

Abstract: *This community-service program was implemented through the Program Pemberdayaan Umat (PRODAMAT) of Universitas Ahmad Dahlan with the aim of enhancing digital literacy and cybersecurity awareness among teachers at*

Muhammadiyah Boarding School (MBS) Yogyakarta. The activity focused on smartphone account security education through practical steps such as password management, two-factor authentication (2FA), and phishing awareness. A participatory approach was applied through training involving 15 teachers and staff, combining interactive discussions, demonstrations, and pretest–posttest evaluation. The results showed an increase in the average knowledge score from 4.63 to 4.90, digital awareness from 4.05 to 4.45, and intention and safe digital behavior from 4.35 to 4.73. These improvements reflect positive changes in participants' understanding, awareness, and behavior toward digital security. The program highlights the importance of integrating technological skills with ethical and religious values to promote sustainable digital empowerment in Islamic educational environments.

Keywords: *Digital Literacy; Smartphone Security; Community Empowerment; Teacher Training; Muhammadiyah Education*

Introduction

The rapid digital transformation in the education sector has reshaped how teachers, students, and institutions communicate, learn, and manage information. Smartphones and digital platforms have become integral tools in teaching and administrative processes, allowing for faster access to educational materials and more efficient management systems (Bellini et al., 2022). However, this convenience comes with a growing concern over digital safety and privacy, especially among educators who serve as both technology users and role models for their students. In many educational contexts, including Islamic boarding schools (*pesantren*), awareness and competence in digital security are still developing and often remain limited to functional use rather than strategic and ethical awareness (Karayel & Saygılı, 2025).

To conceptualize the core problem addressed in this study, the gap between digital adoption and digital safety awareness among educators is presented in Figure 1. The mind map illustrates six major dimensions of the issue: existing situation, practical problem, knowledge gap, capacity gap, empowerment gap, and proposed intervention. Each component reflects how increasing technology use has not been equally matched by secure and ethical digital behavior, creating vulnerabilities that affect individuals and institutions alike. This visualization underscores the urgent need for structured digital empowerment initiatives that integrate practical, ethical, and religiously grounded approaches (Rakhmadi, Firdaus, et al., 2025).

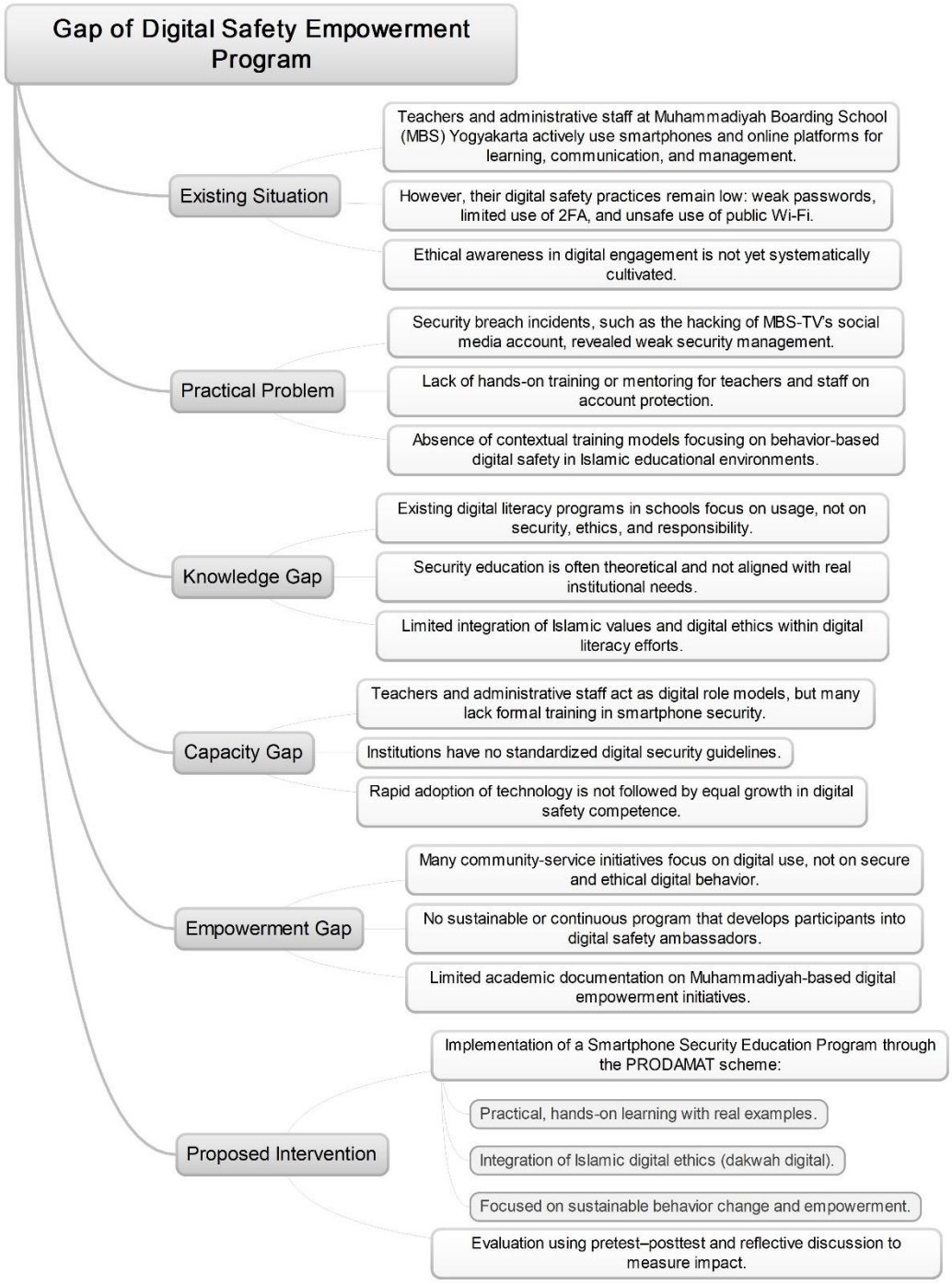

Figure 1. Mind Map of the Gap in Digital Safety Empowerment at Muhammadiyah Boarding School (MBS) Yogyakarta.

The proliferation of online learning, communication platforms, and digital administration systems has heightened teachers' dependence on mobile devices. In the context of Islamic boarding schools, smartphones are commonly used not only for academic purposes but also for communication, social media management, and

coordination of religious programs (Shuwandy et al., 2025). However, this increased reliance has not been followed by adequate training on security measures. Many teachers and staff use weak passwords, do not update their devices regularly, and remain unaware of the importance of two-factor authentication (2FA) or phishing awareness. As a result, they become vulnerable to data breaches, identity theft, and unauthorized access to institutional accounts.

One notable example of this vulnerability occurred when the official MBS-TV social-media account was compromised by external actors. The incident exposed weaknesses in account management and highlighted the need for comprehensive digital safety education. Such cases are not unique to one institution but reflect a broader trend across many educational settings where digital adoption outpaces the development of cybersecurity literacy (Riadi et al., 2023). This imbalance indicates that technology integration in education must be accompanied by structured efforts to enhance digital ethics and protection awareness among educators.

Another layer of the problem lies in the fact that most digital literacy programs in educational institutions focus on the use of technology—how to operate tools, access learning platforms, and manage data—rather than on secure and ethical use (Gunawan et al., 2022). Training modules typically stop at the level of technical proficiency without addressing the behavioral aspects of safe digital engagement (Firdonsyah et al., 2025). As a result, educators may know how to use digital applications but remain unaware of the ethical implications and security responsibilities associated with them. This represents a critical knowledge gap in current digital education initiatives.

In Islamic boarding schools, this gap is compounded by the limited integration of Islamic values and ethical principles within digital literacy frameworks. While the institutions emphasize moral education and discipline in daily life, these values are often not explicitly linked to digital behavior. Muhammadiyah, as a reformist Islamic movement that promotes modern education, upholds the idea that technology should serve as a medium for *dakwah* and social good (Maimun et al., 2022). Therefore, bridging the gap between technical knowledge and ethical application becomes essential for sustaining responsible digital citizenship in Muhammadiyah's educational environment.

From the perspective of capacity building, teachers and administrative staff in boarding schools play dual roles as educators and digital users. They are expected to set examples for their students in both moral conduct and responsible technology use

(Irsyadi et al., 2024). However, many lack access to structured capacity-building programs focusing on digital safety. Without such training, they face challenges in protecting their own data as well as institutional assets. Furthermore, most schools do not yet have internal policies or security guidelines, leaving the protection of digital resources to individual practices, which vary greatly in awareness and discipline.

The empowerment dimension of this issue highlights that most community-service and digital literacy initiatives remain project-based and short-term. They often emphasize technological adoption rather than behavioral empowerment (Khatib Sulaiman et al., 2024). Once the activity concludes, the knowledge transfer tends to fade without long-term sustainability. Consequently, there is a pressing need for an empowerment model that transforms teachers and staff into digital safety ambassadors, capable of promoting safe practices beyond the duration of a single program. This transformation requires a shift from training as an event to empowerment as a continuous process (Rakhmadi, Fravy Qanza, et al., 2025).

The *Program Pemberdayaan Umat* (PRODAMAT) of Universitas Ahmad Dahlan (UAD) seeks to address this empowerment gap by promoting sustained community engagement grounded in Islamic ethics and technological literacy. The initiative represents a unique model of collaboration between academia and local communities, focusing on practical education and reflective learning (Wintolo et al., 2025). In the context of MBS Yogyakarta, PRODAMAT offers a framework that combines technological skill development with moral and ethical guidance, aligning with Muhammadiyah's vision of *dakwah digital*—digital preaching through responsible technology use.

This article reports on the implementation and outcomes of the PRODAMAT community-service program, which focuses on enhancing the digital literacy and smartphone security awareness of educators at MBS Yogyakarta. Rather than an experimental research study, the initiative serves as a community engagement activity designed to empower local educators with essential skills to improve both their personal and professional digital safety practices. The focus of this paper is to present the methodology, findings, and implications of this empowerment initiative.

Empowerment theory emphasizes the process of increasing individuals' control over their lives and decisions, often through education, skill-building, and community engagement. However, when applied to digital environments, empowerment must also integrate ethical principles to ensure that knowledge is used responsibly. Ethics-based empowerment combines digital literacy with values of

integrity, accountability, and social responsibility, ensuring that participants not only acquire technical skills but also recognize their ethical obligations in using technology. This framework aligns with Jalil et al., 2021) theory of *digital ethics*, which stresses the importance of moral responsibility in an increasingly interconnected world. In the context of Islamic education, this empowerment approach is further reinforced by Islamic values of *amanah* (trust), *akhlaq* (ethics), and collective responsibility. By embedding these principles into digital literacy programs, PRODAMAT ensures that participants view digital safety not just as a technical skill, but as a moral duty to protect both personal and communal digital spaces. This ethical approach enhances the sustainability of the program by fostering responsible digital citizenship that extends beyond individual practices and impacts the broader educational community.

It was observed that many teachers and administrative staff, despite their frequent use of smartphones for professional tasks, had limited knowledge regarding essential digital security practices. A significant number of participants expressed concerns over weak password practices and lacked awareness of advanced security measures, such as two-factor authentication (2FA) and app permission management. This gap in knowledge was particularly evident when discussing incidents like the hacking of the MBS-TV social media account, which served as a catalyst for this training. The lack of structured security education and awareness led to vulnerabilities in both personal and institutional digital assets. These findings underscore the necessity of a tailored training program that not only addresses the technical aspects of digital security but also instills a deeper understanding of personal responsibility in maintaining safe digital environments.

The purpose of the present program is to empower teachers and administrative staff at MBS Yogyakarta to adopt safer digital behaviors through smartphone security education. The training aims to enhance participants' knowledge of security risks, strengthen their ability to implement protection measures, and encourage them to share these practices within their community. By fostering awareness and accountability, the program seeks to build not only digital competence but also ethical consciousness in technology use, ensuring that participants understand both the technical and moral dimensions of digital engagement.

This initiative contributes to the broader discourse on digital ethics and community empowerment in Islamic education. By integrating ethical principles into digital literacy training, the program aligns with the Muhammadiyah philosophy of holistic education, which connects faith (*iman*), knowledge (*ilmu*), and morality

(*akhlak*). This integration ensures that the use of technology remains purposeful, disciplined, and beneficial for the community. It also offers a replicable model for other Islamic educational institutions facing similar challenges in balancing modernization with moral responsibility.

Methodology

This community-service activity was implemented under the PRODAMAT organized by UAD. The program aimed to strengthen teachers' awareness and capability in ensuring digital safety through smartphone-security education. Rather than following a research-based experimental design, this activity emphasized community empowerment and participatory learning. It was designed to translate technological knowledge into practical skills and ethical awareness aligned with Muhammadiyah's educational and social mission of promoting beneficial knowledge and responsible digital behavior.

The community-service process followed a structured four-stage framework, consisting of Preparation, Implementation, Evaluation, and Follow-Up, as illustrated in Figure 2. These stages represented a continuous cycle of planning, action, reflection, and empowerment (Rakhmadi & Anshori, 2025). The diagram visualized the flow of the program, beginning with needs identification and coordination, followed by training implementation, evaluation of learning outcomes, and post-activity engagement. Each stage was interconnected to maintain systematic execution and sustainability in enhancing digital-safety literacy within the educational community.

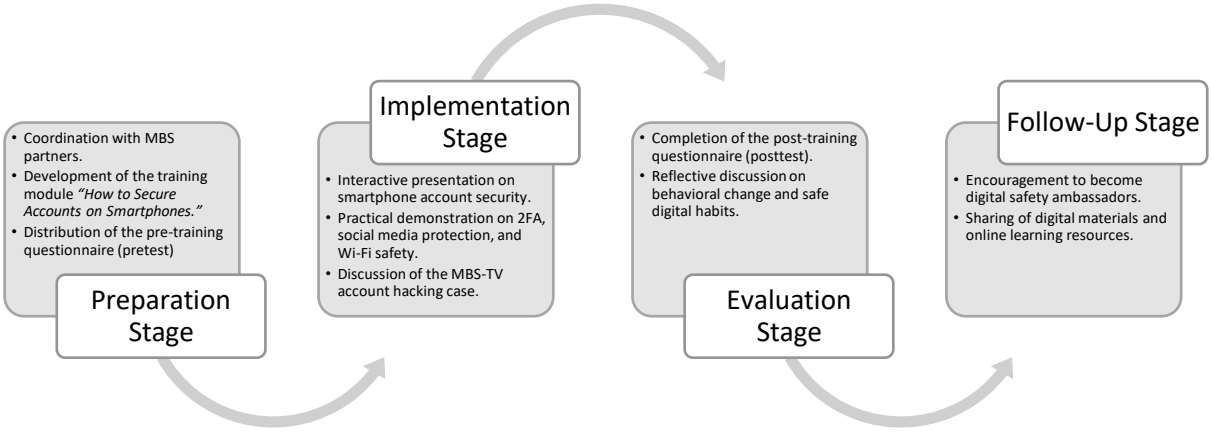

Figure 2. Framework and Stages of the PRODAMAT Community-Service Program

The methodological approach adopted a community-based empowerment model combining awareness building, skills training, and behavior reinforcement.

The activity positioned participants not as research subjects but as active collaborators contributing to the identification of problems and co-creation of solutions. The training highlighted the intersection of technology, ethics, and spirituality, emphasizing that responsible digital use is part of the Islamic value of *amanah* which represents the moral duty to safeguard trust and knowledge in the digital environment.

The partner institution for this community-service program was MBS Yogyakarta, an Islamic educational institution integrating religious and scientific learning. Fifteen participants, nine males and six females, took part in the activity. They consisted of ICT teachers, laboratory coordinators, and administrative staff who managed digital platforms for academic and institutional communication. Their varying backgrounds enabled the facilitators to tailor the content and ensure that all participants could engage meaningfully with the materials and discussions provided during the training. The activity was conducted within the facilities of MBS Yogyakarta, located in a suburban educational area known for its integration of religious and technological learning, as shown in Figure 3.

Figure 3. Location of Muhammadiyah Boarding School (MBS) Yogyakarta.

The program was facilitated by a team from the Informatics Doctoral Program of UAD, coordinated under the university's community-service committee. The team members were responsible for developing the learning materials, moderating sessions, demonstrating technical procedures, and guiding participants throughout the workshop. This structure allowed balanced delivery between conceptual

explanation, practical demonstration, and interactive engagement, consistent with the principles of collaborative community empowerment.

The preparation stage focused on establishing cooperation with the community partner and aligning objectives with institutional needs. Coordination meetings were held with MBS representatives to identify key issues related to digital-account security and to schedule the program activities. The facilitation team developed a concise training module entitled *"How to Secure Accounts on Smartphones."* Supporting materials, including presentation slides, digital posters, and pre-training questionnaires, were designed to assess baseline awareness and to provide a structured learning experience. Logistical preparation, venue arrangement, and participant communication were also completed during this stage.

The implementation stage comprised the main training activities. Conducted on Monday, 27 October 2025, from 09.00 to 11.50 a.m. at the MBS training hall, the workshop used a blended approach combining short lectures and interactive discussions. Participants learned step-by-step techniques for creating strong passwords, enabling two-factor authentication (2FA), managing secure social-media accounts, and recognizing unsafe Wi-Fi connections. A contextual case involving the unauthorized access of a school social-media account was discussed to connect the training content with real-life experience and institutional relevance (Cahyo Utomo & Rokhmah, 2022).

The workshop emphasized active participation and peer learning. Participants were encouraged to share personal experiences regarding account management and online security challenges. Facilitators provided individual guidance as participants practiced security configurations directly on their devices. The atmosphere was intentionally collaborative, allowing individuals with varying levels of digital literacy to support one another. This participatory approach reflected the principles of adult learning, where mutual interaction enhances comprehension and fosters empowerment.

The evaluation stage was conducted immediately after the training to gather participants' responses and reflections (Rakhmadi, Rochmadi, et al., 2025). A post-training questionnaire was distributed to assess participants' understanding of smartphone-security concepts and their awareness of safe digital practices. In addition to the questionnaire, participants joined a reflective dialogue facilitated by the academic team, during which they shared lessons learned and identified strategies to apply the material in their teaching and administrative contexts. The information

collected at this stage was used for internal documentation and improvement of future empowerment activities.

To measure the effectiveness of the training in enhancing awareness, skills, and behavior, several assessment methods were employed. Awareness was evaluated by asking participants to rate their understanding of key concepts such as the importance of secure passwords, the risks associated with phishing, and the benefits of two-factor authentication (2FA). This was assessed through a set of questions in the pretest and posttest questionnaires. Skills were measured by participants' ability to apply the concepts learned during the training, such as setting up 2FA and creating strong passwords on their own devices. Practical tasks during the session allowed facilitators to observe the participants' proficiency in implementing these security measures. Finally, behavior was assessed through a series of reflective questions in the posttest and group discussions, where participants expressed their intentions to adopt secure practices in their digital routines and share this knowledge with their colleagues. The combination of pretest-posttest comparisons and reflective dialogues provided a comprehensive understanding of the program's impact on participants' knowledge, practical abilities, and long-term commitment to digital safety.

Feedback from participants was systematically compiled and reviewed by the facilitation team. Comments regarding the clarity of instructions, relevance of materials, and learning atmosphere were documented. This feedback informed the continuous refinement of training modules used in subsequent programs under PRODAMAT. The reflection process also reinforced participants' sense of collaboration and ownership, as their input directly contributed to shaping the educational materials for broader community benefit.

The follow-up stage aimed to maintain engagement and encourage sustainable application of digital-safety practices beyond the training session. Participants were invited to act as digital-safety ambassadors within their school environment, sharing the knowledge gained with students and colleagues. Electronic materials and access to online learning resources were provided to support continued self-learning. Facilitators maintained post-activity communication through digital channels to monitor ongoing practices and to strengthen the partnership between the university and the community institution.

All stages of the program were documented through attendance records, session notes, and photographs for administrative and reporting purposes. Participants were informed of the purpose of the activity, and their voluntary

participation was obtained prior to data collection. Responses from the questionnaires were anonymized and treated confidentially in accordance with the university's community-service ethics guidelines. The activity adhered to the ethical standards set by UAD and followed national publication ethics frameworks to ensure transparency and respect for all participants involved in the empowerment process.

Result and Discussion

The implementation of the *PRODAMAT* community-service program at MBS Yogyakarta took place on Monday, 27 October 2025, from 09:00 to 11:50 AM. The activity was attended by a total of 15 participants, consisting of 9 male and 6 female educators, all of whom held roles as teachers, laboratory coordinators, or administrative staff. These individuals were selected due to their significant involvement with the school's digital platforms and administrative systems, making them ideal candidates for the training on securing digital accounts. Table 1 presents the demographic profile of the participants, providing an overview of their gender, education level, and roles within the MBS.

Table 1. Demographic Profile of the Participants

Demographic Category	**Description**	**Count**
Gender	Male	9
	Female	6
Education Level	Diploma/Bachelor	11
	Senior High School	4
Role in Pesantren	Teacher	11
	Administrative Staff	4

The results from the pretest and posttest questionnaires, shown in Table 2, demonstrate a noticeable improvement in participants' knowledge and awareness of digital security after the training. The pretest mean scores reflect participants' understanding of key concepts such as the importance of strong passwords, the need for 2FA, and recognizing potential security risks like phishing. After the training, the posttest mean scores show an increase in knowledge and confidence regarding these topics.

The questionnaire used in this study was designed to assess participants' understanding, awareness, and behavior related to digital safety. It consisted of

several indicators grouped into three main dimensions: knowledge and understanding, attitude and digital awareness, and intention and safe digital behavior. Each statement was rated using a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). This scale allowed the researchers to measure both cognitive and behavioral changes before and after the training. The pretest and posttest results summarized in Table 2 reflect how participants' scores improved across all indicators, indicating not only increased knowledge but also stronger commitment to practicing secure digital habits.

To ensure the reliability and validity of the questionnaire used in this study, the instrument was reviewed and validated to ensure it accurately measured the participants' knowledge, attitudes, and behaviors related to digital security. Validity was ensured by ensuring that the questions in the questionnaire were directly aligned with the objectives of the training, which aimed at enhancing participants' understanding and skills in digital safety. The questionnaire was also reviewed by experts in the fields of technology and education to confirm the relevance of all questions. Reliability was assessed through a pilot test with a small group, which showed that the questionnaire provided consistent and reliable results when used with a larger group of participants.

The data presented in Section A—*Knowledge and Understanding*—demonstrate a clear improvement in participants' conceptual grasp of digital safety principles. The mean score increased from 4.63 in the pretest to 4.90 in the posttest, indicating that the training effectively strengthened the participants' comprehension of how and why digital protection is important. The largest gain occurred in understanding the importance of account security ($\Delta = +0.4$), showing that the session successfully clarified the risks associated with weak authentication and careless account management. Meanwhile, smaller gains were observed in recognizing suspicious links ($\Delta = +0.1$), suggesting that although awareness improved, ingrained habits such as verifying unfamiliar messages require continued reinforcement over time. Overall, the findings suggest that participants developed a stronger cognitive foundation in recognizing potential cyber-threats and understanding preventive actions such as regular system updates and the creation of complex passwords.

Table 2. Pretest–Posttest Results per Indicator (Knowledge & Attitude)

Category / Indicator	Pretest Mean	Posttest Mean	Change (Δ)
Section A – Knowledge and Understanding			
Understanding the importance of account security	4.6	5.0	+0.4
Need to regularly update systems and applications	4.5	4.8	+0.3
Being cautious about suspicious links or messages	4.8	4.9	+0.1
Average (A)	4.63	4.90	+0.27
Section B – Attitude and Digital Awareness			
Feeling safe using smartphones	3.8	4.2	+0.4
Belief that account security depends on user behavior	4.3	4.7	+0.4
Average (B)	4.05	4.45	+0.40
Section C – Intention and Safe Digital Behavior			
Intention to enable two-factor authentication (2FA)	4.4	4.8	+0.4
Intention to change passwords regularly	4.2	4.6	+0.4
Checking app permissions before installation	4.5	4.8	+0.3
Intention to teach others about account security	4.3	4.7	+0.4
Average (C)	4.35	4.73	+0.38

Section B—*Attitude and Digital Awareness*—reveals the most significant proportional increase among all categories, with the mean score rising from 4.05 to 4.45 (Δ = +0.40). This indicates a notable shift in participants' self-perception and awareness regarding their role in maintaining digital safety. The rise in confidence when using smartphones and in acknowledging that security depends on user behavior reflects an internalization of responsibility; participants moved from viewing security as a purely technical matter to understanding it as a behavioral commitment. This transformation aligns with the objective of digital empowerment programs, which emphasize awareness and self-discipline as key dimensions of sustainable literacy. The improved attitudes also suggest that experiential learning and peer interaction during the workshop were instrumental in helping participants connect their daily technology use with broader notions of safety, trust, and ethical accountability.

Section C—*Intention and Safe Digital Behavior*—shows consistently positive growth in participants' willingness to apply and share secure practices. The overall mean increased from 4.35 to 4.73, with particularly strong improvement in the intention to activate two-factor authentication and to change passwords regularly (both Δ = +0.4). These results indicate that the program succeeded not only in increasing knowledge but also in encouraging actionable behavior, a key indicator of sustainable learning outcomes. Participants also expressed greater readiness to check application permissions and to educate others about smartphone security, demonstrating the diffusion of empowerment beyond individual learning. This behavioral intention is essential for ensuring continuity of impact; once participants act as digital safety ambassadors within their institution, the culture of secure and ethical digital use can expand organically throughout the pesantren environment. Together, these results confirm that the *PRODAMAT* initiative effectively bridged the gap between understanding, awareness, and practice—transforming knowledge into responsible digital behavior.

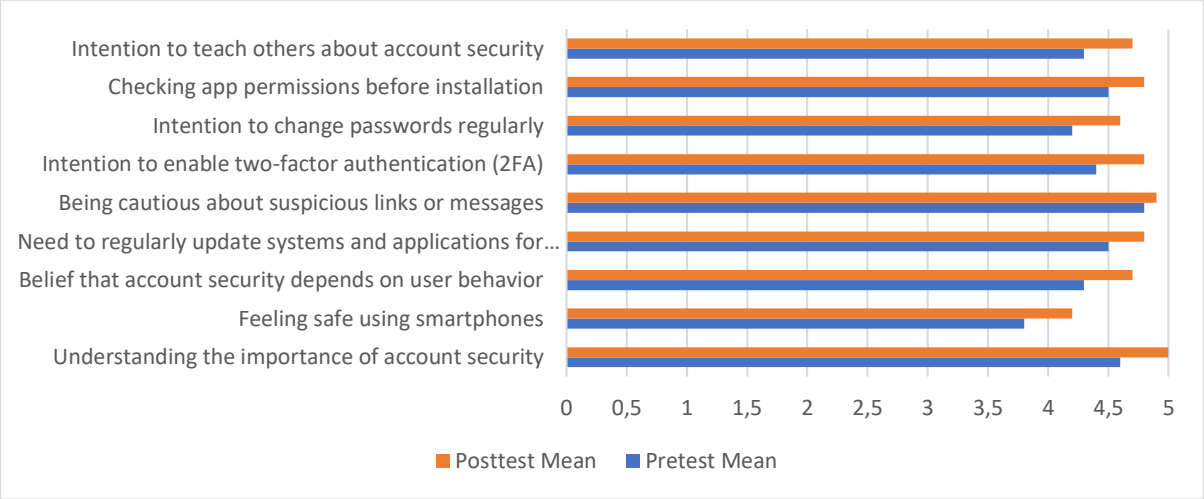

Figure 4. Comparison of Pretest and Posttest Scores per Indicator of Digital Safety Knowledge and Awareness

The results from the pretest and posttest clearly show a significant improvement in participants' knowledge and awareness regarding digital safety. The data indicates that the participants' understanding of security practices, such as creating strong passwords, enabling 2FA, and recognizing phishing attempts, increased after the training. This shift can be attributed to various factors, notably the interactive nature of the training session. During the workshop, facilitators provided a live presentation, allowing participants to actively engage with the material. For example, as shown in Figure 4, participants were guided through the process of setting up 2FA and checking app permissions on their own smartphones. This hands-on

approach enabled them to directly apply the concepts they learned, reinforcing their understanding of the importance of these security measures.

The practical relevance of the content played a key role in the improvement of participants' awareness. The facilitators used real-world examples, such as the case of the MBS-TV account being hacked, to illustrate the real risks of inadequate digital security. By linking the content of the training to incidents participants could relate to, they were able to grasp the urgency and significance of the practices being taught. This connection to their own experiences made the training more impactful and actionable for them, as they saw firsthand the consequences of insecure digital behavior.

Participant engagement further contributed to the success of the training. The session was designed to be interactive, with participants encouraged to share their concerns and experiences related to digital security. This open environment fostered discussions where they could ask questions, express doubts, and offer suggestions. Such collaborative dialogue not only helped to address specific concerns but also allowed participants to learn from one another's experiences, further enhancing the value of the training.

Although the data indicated a small increase in the cautiousness about suspicious links (Δ +0.1), this suggests that while participants became more aware of the importance of being cautious with digital interactions, changing habits such as avoiding phishing links may take more time. Despite this, the overall trend showed an improvement across all indicators, suggesting that the training effectively influenced participants' understanding and attitudes towards securing their digital accounts. It is evident that the program succeeded in raising participants' awareness and provided them with the necessary tools to apply secure digital practices in their personal and professional lives.

The reflection on behavioral change and digital empowerment was a crucial aspect of the training, as it provided participants with an opportunity to evaluate how the training had impacted their personal digital security practices. During the final discussion, participants shared their experiences, discussing how their perceptions of digital security had evolved. Many reported feeling more confident in their ability to secure their online accounts, particularly with the introduction of 2FA. One teacher mentioned that they had already implemented 2FA on their email accounts and social media profiles after seeing how easy it was to activate during the workshop. This is a

clear example of how the training led to a concrete behavior change, where knowledge gained in the session was immediately applied to improve personal security.

Another participant expressed their intention to begin changing passwords regularly and using stronger password combinations, a practice they had not fully adopted prior to the training. The participants acknowledged that securing accounts and devices was not just about following technical steps but also about adopting new habits. This was reflected in their feedback, where they discussed not only the *what* of security practices but also the *why*, emphasizing their newfound awareness of digital threats. The conversation revealed that many participants now viewed digital security as a personal responsibility, aligning with the conceptual model of digital behavior change, which emphasizes the importance of awareness, education, reflection, and sustainability in the empowerment cycle (Fadlil et al., 2024).

As shown in Figure 5—the *Conceptual Model of Digital Behavior Change*, participants moved through the cycle from increased awareness of digital security risks to education on effective practices, followed by behavioral change, where they began applying these practices. The model suggests that for change to be sustained, participants must engage in reflection on the new behaviors, which was evident in their discussion and the plans they made to continue implementing the learned security measures. By the end of the session, many participants had internalized digital security not only as a technical skill but as part of their digital citizenship and daily routine.

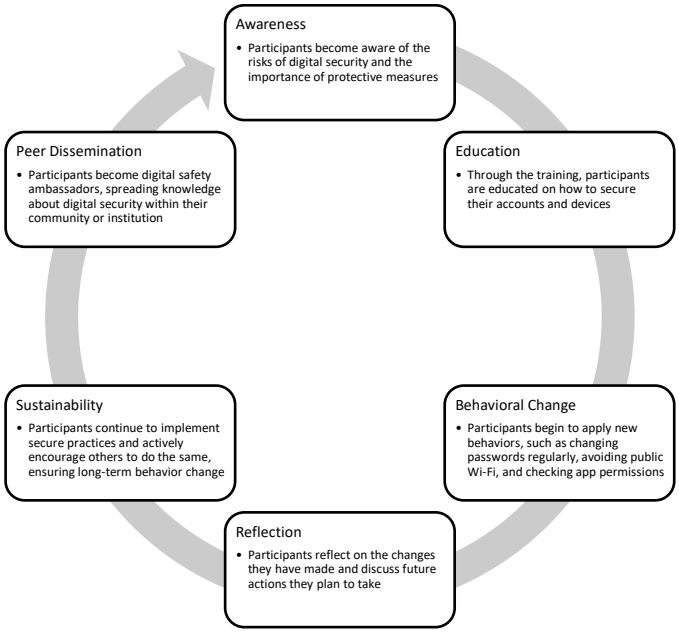

Figure 5. Digital Behavior Change Cycle: From Awareness to Empowerment

Despite the overall success of the program, there were several challenges encountered during the implementation of the training. One notable challenge was time constraints. The limited time available meant that not all participants could engage with every aspect of the training in as much depth as desired. For example, some participants requested more time to practice advanced security settings, such as password managers and additional features of 2FA. To address this, the facilitators ensured that additional resources were provided, such as detailed step-by-step guides and video tutorials, allowing participants to review the material at their own pace after the session.

Through these challenges, several valuable lessons were learned. Practical, hands-on learning was crucial to the success of the training, as it allowed participants to gain confidence in applying the security measures. Additionally, the training highlighted the importance of flexibility in addressing the varying levels of digital access and skills among participants. Future sessions could benefit from offering additional follow-up support, such as one-on-one consultations or extended online resources, to ensure that participants continue to feel empowered in their digital safety practices long after the training has ended. By adapting the training to meet the diverse needs of participants, the program can become even more impactful in fostering long-term behavioral change.

The *PRODAMAT* community-service program has made a significant contribution to the empowerment of the participants, particularly in terms of enhancing their digital literacy and security awareness. By focusing on securing online accounts and understanding digital safety measures, the training directly addressed a gap in the participants' knowledge and practices. Most of the participants, who are educators and administrative staff, manage important digital platforms in their daily professional tasks. Therefore, the capacity-building aspect of the program was crucial, as it equipped them with practical skills to safeguard not only their personal information but also the data and digital resources of the institution they serve. This newly acquired knowledge can be immediately applied in their roles, enhancing the overall digital security culture within the MBS.

The empowerment aspect of the program aligns closely with the goals of PRODAMAT, which emphasizes the importance of community development through education and skill-building. The training was not just about transferring technical knowledge, but also about fostering a sense of responsibility towards digital security, in line with the broader educational mission of Muhammadiyah. By integrating

dakwah digital (digital preaching) into the program, the initiative highlights the significance of ethical and responsible use of technology, a core value in Muhammadiyah's approach to education. This connection between religious values and modern technology is essential, as it helps bridge the gap between traditional teachings and the digital challenges faced by today's society.

At the conclusion of the program, a group photo was taken featuring the facilitators, participants, and school administrators of MBS Yogyakarta. The photo symbolizes collaboration, unity, and shared commitment among all stakeholders involved in strengthening digital literacy and security awareness within the educational community.

Figure 6. Group photo of facilitators and participants at MBS Yogyakarta after the completion of the PRODAMAT community-service program.

The program's impact extends beyond immediate knowledge transfer to creating a sustainable empowerment process. The participants were not only educated on secure digital practices but were also encouraged to become digital safety ambassadors within their community. This approach ensures that the knowledge gained in the training will continue to be disseminated through the teachers and staff, who will now play an active role in promoting safe digital behavior to their students and colleagues. The long-term impact of this initiative will depend on the participants' ability to transfer what they have learned to others, creating a ripple effect that can strengthen the entire pesantren's capacity to navigate the challenges of the digital world.

The sustainability of this empowerment is further reinforced by the follow-up strategies embedded in the program, such as providing additional learning resources and keeping the lines of communication open for ongoing support. This ensures that

the lessons learned are not forgotten after the training session, but instead become ingrained in the daily practices of the participants. The digital safety ambassadors will continue to influence their peers, fostering a culture of continuous learning and shared responsibility for digital security within the MBS. Through this process, the program contributes not only to immediate skill-building but also to the creation of a self-sustaining ecosystem where knowledge and responsibility for digital safety are passed on through the community.

Conclusion

The *PRODAMAT* community-service program on smartphone security education at MBS Yogyakarta successfully addressed the need to improve digital literacy and account safety awareness among teachers and administrative staff. The pretest–posttest comparison demonstrated measurable progress in three main domains. First, in the knowledge and understanding dimension, participants' mean score increased from 4.63 to 4.90, showing that the training effectively strengthened their conceptual understanding of key security practices such as creating strong passwords and recognizing digital threats. Second, in the attitude and digital awareness domain, the average score rose from 4.05 to 4.45, reflecting a clear shift in perception where participants began to view digital safety as a personal and moral responsibility rather than merely a technical task. Third, in the intention and safe digital behavior domain, the mean score increased from 4.35 to 4.73, indicating that participants were not only more knowledgeable but also more willing to apply and share secure practices such as enabling 2FA and educating others about account protection. These three aspects collectively confirm that the program fostered both cognitive and behavioral transformation toward safer digital engagement.

The program also demonstrated the importance of integrating digital literacy with ethical and religious values, as promoted through Muhammadiyah's vision of *dakwah digital*. By emphasizing that technology use should be guided by responsibility, honesty, and integrity, the program not only improved participants' technical competence but also reinforced their moral and spiritual awareness in navigating the digital world. This holistic approach to empowerment positioned digital safety as an extension of ethical practice—an inseparable part of educators' professional and social responsibility in fostering a digitally conscious community.

Future implementations of similar programs are encouraged to extend the duration of training or incorporate structured follow-up sessions to reinforce and

expand participants' secure digital habits. Sustaining the empowerment process through continuous mentoring, online learning materials, and peer collaboration will ensure long-term impact. Moreover, integrating smartphone security and digital ethics into the school curriculum would help cultivate a culture of digital responsibility among students, ensuring that the spirit of the PRODAMAT program continues to thrive as a sustainable model of community empowerment within the digital era. Going forward, it is essential that the institution itself plays an active role in maintaining this momentum by providing ongoing support, developing policies to secure digital practices, and ensuring that digital literacy remains a priority in the educational framework. Reflecting on the success of this initiative, it becomes evident that true digital empowerment lies not only in individual efforts but in the collective commitment of both educators and institutions to uphold safe and ethical digital practices.

Acknowledgment

The authors would like to express their sincere gratitude to Ustadz Rahmat Susanto, S.Pd., M.Pd., Vice Principal for Education at Muhammadiyah Boarding School (MBS) Yogyakarta, for his valuable support and cooperation during the implementation of the *PRODAMAT* community-service program. Appreciation is also extended to Prof. Dr. Muchlas, M.T., Rector of Universitas Ahmad Dahlan (UAD), for his continuous guidance, motivation, and institutional support that enabled this program to be successfully implemented as part of UAD's commitment to community empowerment and the integration of technology, education, and ethical values.

References

Bellini, P., Nesi, P., & Pantaleo, G. (2022). IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies. *Applied Sciences*, *12*(3). https://doi.org/10.3390/app12031607

Cahyo Utomo, I., & Rokhmah, S. (2022). Konfigurasi SSL Untuk Meningkatkan Keamanan Web server Pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta. *JURTI*, *6*(2).

Fadlil, A., Riadi, I., & Mu'Min, M. A. (2024). Mitigation from SQL Injection Attacks on Web Server using Open Web Application Security Project Framework. *International Journal of Engineering, Transactions A: Basics*, *37*(4), 635–645. https://doi.org/10.5829/ije.2024.37.04a.06

Firdonsyah, A., Purwanto, Imam Riadi, Mahrus Ali, & Ammar Fauzan. (2025). A Supervisory Approach to Building Ethical Digital Forensic Frameworks through Participatory Action Research. *Data and Metadata*, *4*, 1179. https://doi.org/10.56294/dm20251179

Gunawan, D., Nugroho, Y. S., Irsyadi, F. Y. Al, Utomo, I. C., Andreansyah, I., & Islam, S. (2022). A Privacy Preserving Data Anonymization Method for Customer Transaction Data Publishing. *2022*

International Conference on Information Technology Systems and Innovation (ICITSI), 171–176. https://doi.org/10.1109/ICITSI56531.2022.9970910

Irsyadi, F. Y., Utomo, I. C., Rahman, A. A., Kojyro, H. D., Mursetyani, D., Putri, S. Q. A., & Sadi'udin, M. W. (2024). Optimalisasi Sistem Jaringan Informasi pada MIM Taraman Sragen. *Jurnal Pengabdian Masyarakat Abdi Teknoyasa*, *5*(1).

Jalil, A., Tohara, T., Shuhidan, S. M., Diana, F., Bahry, S., & Norazmi Bin Nordin, M. (2021). Exploring Digital Literacy Strategies for Students with Special Educational Needs in the Digital Age. In *Turkish Journal of Computer and Mathematics Education* (Vol. 12, Issue 9).

Karayel, T., & Saygılı, M. (2025). Understanding smartphone security behavior through the core constructs of protection motivation theory: A comparative study of iOS and android users. In *Computers and Security* (Vol. 158). Elsevier Ltd. https://doi.org/10.1016/j.cose.2025.104652

Khatib Sulaiman, J., Cahyo Utomo, I., Kholisotul, N., Muhammad Izudin Rojak, K., & Artikel Abstrak, I. (2024). Evaluasi Kerentanan Keamanan Pada Perangkat IoT: Studi Kasus Pada Smart Home. *Indonesian Journal of Computer Science*, *13*(3).

Maimun, M. H., Kussudyarsana, Maulana, H. K., Rahman, A. A., & Utomo, I. C. (2022). Pemanfaatan Digital Marketing pada Pondok Pesantren Tahfidz Al-Qur'an Ath-Thohiriyah Muhammadiyah. *Abdi Psikonomi*, *3*, 63-69].

Rakhmadi, A., & Anshori, A. (2025). Leveraging the SAW Method in a Decision Support System to Improve Elderly Nutrition at Laweyan Home for the Elderly. *Jurnal Bakti Nusa*, *6*(2), 42–50. https://doi.org/10.29303/baktinusa.v6i2.144

Rakhmadi, A., Firdaus, M. I., & Nugroho, S. (2025). COmputing and INformation Systems Journal A Systematic Implementation of the Waterfall Model in E-Commerce System Development for Small Businesses. *COmputing and INformation Systems Journal*, *1*(1). www.coins-indocompt.org

Rakhmadi, A., Fravy Qanza, A., Utomo, I. C., & Jember, U. M. (2025). Enhancing Business Operations through Technology: A Community-Driven Inventory System for Dymas Kulit Home-Based Leather Craft Business. *J-ABDIMASTEK*, *4*(1), 32–43. https://doi.org/https://doi.org/10.32528/abdimastek.v4i1.3560

Rakhmadi, A., Rochmadi, T., Azis, A., Ayuningtyas, A., Sarmini, & Wahyusari, R. (2025). A Conceptual Framework for Integrating SUS into ITIL: Enhancing IT Service Management Through Usability Evaluation. *The Indonesian Journal of Computer Science*, *14*(5). https://doi.org/10.33022/ijcs.v14i5.4842

Riadi, I., Yudhana, A., & Inngam Fanani, G. P. (2023). Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation. *International Journal of Safety and Security Engineering*, *13*(1), 11–19. https://doi.org/10.18280/ijsse.130102

Shuwandy, M. L., Jouda, A. S., Ahmed, M. A., Salih, M. M., Al-qaysi, Z. T., Alamoodi, A. H., Garfan, S., Albahri, O. S., Zaidan, B. B., & Albahri, A. S. (2025). Sensor-based authentication in smartphone: A systematic review. In *Journal of Engineering Research (Kuwait)* (Vol. 13, Issue 2, pp. 741–750). Elsevier B.V. https://doi.org/10.1016/j.jer.2024.02.003

Wintolo, H., Kusumaningrum, A., Alriavindra Funny, R., Mulyani, S., & Triono Nuryatno, E. (2025). Peningkatan Reputasi Sekolah Melalui Pelatihan Penulisan Artikel Ilmiah Bagi MGBK Madrasah Aliyah. *Abdi: Jurnal Pengabdian Dan Pemberdayaan Masyarakat*, *7*(1), 164–170. https://doi.org/10.24036/abdi.v7i1.1077