EMAGRAP
Economic Military and Geographically Business Review
EMAGRAP 3(2): 173–189
ISSN 3025-3160

Institute for Advanced Science, Social and Sustainable Future
MORALITY BEFORE KNOWLEDGE

Cybersecurity education for the elderly as a strategic tool to mitigate digital economic risks

Daffa Mahdy Brata[1,*], Bainul Dwi Tri Putra[1], Anindito[1]
[1] *Informatics, Faculty of Technique and Defense Technology, Indonesia Defense University, Bogor, West Java 16810, Indonesia.*
*Correspondence: daffa.brata@idu.ac.id

Received Date: November 23, 2025 Revised Date: December 29, 2025 Accepted Date: January 30, 2026

ABSTRACT
Background: The vulnerability of older people to online fraud has increased drastically, with national losses reaching IDR 2 trillion by April 2025. These frauds pose a significant threat not only to the elderly but also to the stability of Indonesia's financial sector and fintech industries, highlighting the need for systemic solutions that protect both individuals and businesses. This study aims to develop a cybersecurity education application for the elderly, which not only addresses common fraud patterns in Indonesia, such as fake lotteries, digital bank fraud, and WhatsApp social engineering, but also serves as part of a broader strategy to protect the digital economy, mitigate business risks, and strengthen financial sector security. **Methods:** The study uses the R&D method with the analysis, design, development, implementation, evaluation model. The application features an elderly-friendly interface with large fonts, simple navigation, and adaptive learning. User testing was conducted with elderly participants to assess usability and effectiveness, incorporating experiential learning principles to enhance engagement. **Findings:** Initial prototype evaluation with 15 elderly participants (aged 62-74) showed that 87% successfully completed basic navigation tasks independently, and 73% completed the full learning flow without assistance. The experiential learning approach integrated into the prototype design proved more effective than traditional lecture-based methods in preliminary testing. Common usability challenges identified included back navigation difficulties (40% of participants) and quiz submission confusion, informing iterative design improvements. **Conclusion:** This application offers a sustainable, cost-effective solution that not only reduces cybercrime-related losses among the elderly but also contributes to a broader strategy of economic digital security. **Novelty/Originality of this article:** This research introduces a unique approach that combines cybersecurity education for the elderly with strategies to mitigate economic risks in the digital economy. The application integrates an elderly-friendly interface and experiential learning techniques to enhance digital literacy, while simultaneously offering a scalable solution to reduce the broader impact of online fraud on the financial sector.

KEYWORDS: cybersecurity education; digital economy security; elderly digital literacy; online fraud risk; risk management.

1. Introduction

The vulnerability of older adults to online fraud has increased drastically amidst Indonesia's rapid digitalization, with national losses reaching IDR 2 trillion from 97,423 financial fraud cases by April 2025. These fraudulent activities pose a significant threat not only to individual victims but also to the financial stability of the country, especially affecting the banking and fintech sectors which face increasing costs for fraud prevention and mitigation (Apriyadi, 2025). Indonesia experienced over 11 million cyberattacks in the first quarter of 2022 (Tanuwidjaja, 2023). Despite this growing risk, older adults in

Cite This Article:
Brata, D. M., Putra, B. D. T., & Anindito. (2026). Cybersecurity education for the elderly as a strategic tool to mitigate digital economic risks. *Economic Military and Geographically Business Review, 3*(2), 173-189. https://doi.org/10.61511/emagrap.v3i2.2026.2631

Indonesia exhibit low levels of digital literacy and are particularly vulnerable to scams and online threats. In the United States alone, people aged 60 and over collectively lost $4.8 billion to internet fraud in 2024, with phishing scams topping the list of reported crimes (NCO, 2023). The impacts of financial cybercrime extend beyond financial losses to reduced trust and online activity, physical illness, emotional distress, and increased hospital admissions and mortality (Burton et al., 2022). This demonstrates that cybercrime victimization among the elderly represents not merely an economic problem but a comprehensive threat to their overall well-being and quality of life.

Older adults are susceptible to certain types of attacks such as romance scams and consumer fraud, and they struggle to differentiate between genuine and fake emails (Morrison et al., 2021). Research has linked poor digital literacy with cybersecurity vulnerability, with a lack of digital literacy creating avenues for cybercrime victimization through increased susceptibility to phishing and decreased ability to identify and verify threats such as fake websites and social media accounts (Morrison et al., 2023). The correlation between digital literacy deficits and cybersecurity risks underscores the urgent need for targeted educational interventions that address the specific learning needs and constraints of elderly populations. Age-related vulnerabilities include cognitive decline, diminished decision-making abilities, financial instability, and an increased tendency to trust others, significantly heightening susceptibility to cybercrime (Lazarus et al., 2025). A significant proportion of older adults lived in a period characterized by higher levels of trust in societal institutions and individuals, and this trust can expose them to potential exploitation by cybercriminals who portray themselves as reliable and trustworthy figures. Many older adults experience social isolation, which scammers exploit by posing as friendly, understanding voices over the phone or online, and this emotional manipulation can lead to quick compliance with requests (CSA, 2024). These psychological and social factors create a perfect storm of vulnerability that cybercriminals actively exploit through increasingly sophisticated social engineering techniques.

Older adults often lack formal exposure to cybersecurity training or appropriate support, have diverse levels of digital literacy, and may experience age-related cognitive and perceptual changes that impact their ability to recognize and respond to cyber threats (Fujs et al., 2025). Traditional approaches to cybersecurity education have proven inadequate for elderly learners. Traditional education methodologies are insignificant in cybersecurity awareness, and gamification-based platforms are more beneficial (Pramod, 2024). The knowledge retention rate for employees with traditional learning methods is only about 8-10%, but with experiential learning, retention can be as high as 75-90% (Bilodeau, 2022). This stark difference highlights the critical need for innovative approaches to cybersecurity education that move beyond conventional lecture-based methods. Traditional training methods have proven increasingly ineffective, unable to keep pace with the sophistication and frequency of cyberattacks, highlighting a pressing need for a transformative approach to cybersecurity education (Elm Learning, n.d.). Current countermeasures often overlook specific behavioral differences among different demographic groups, leading to generic solutions that fail to address the unique needs and limitations of elderly users (Burton et al., 2022).

Experiential learning and gamification have emerged as promising alternatives for cybersecurity education. Through hands-on learning formats such as gamification, participants are more likely to remember skills and be able to put them to use, as gamification puts learners in real-world scenarios and makes them think under pressure. A focus on experiential learning, goal-driven outcomes, gamification, continuous assessment, and behavioral change proved to be a successful approach in preparing employees to combat evolving cyber threats. Gamification can boost engagement by 60% and make 90% of employees feel more productive and involved by weaving elements of game design into training programs. Serious games can transform security training into experiential learning, allowing participants to play roles and realistically experience attack processes, which can effectively improve learners' security awareness. This approach is particularly relevant for

elderly learners who may benefit from interactive, scenario-based learning that allows them to practice identifying threats in a safe, consequence-free environment.

The application of systematic instructional design models is crucial for developing effective educational interventions. The ADDIE model provides a systematic approach with five phases analyze, design, develop, implement, and evaluate representing a dynamic, flexible guideline for building effective training and performance support tools. The ADDIE model applies to meet different teaching requirements in all online educational environments and is considered a valuable source of additional information by providing good teaching practices. An instructional-design theory originating from formative research to design online learning communities for older adults in non-academic settings can provide appropriate guidance for adult learners. The ADDIE instructional design model provides a consistent and repeatable structure for designing education and training programs, and its flexibility allows instructors to adapt it to a variety of audiences and learning environments (Parikh, 2023). This makes ADDIE particularly suitable for developing cybersecurity education applications for elderly users, as it emphasizes thorough analysis of learner characteristics and needs before proceeding to design and development phases.

The main objective of this study is to design and test the effectiveness of a simulation-based educational application that not only enhances the elderly's ability to identify, understand, and independently avoid various forms of online fraud but also serves as a strategic tool for reducing broader economic risks associated with online fraud, particularly in the financial sector. Specifically, the study aims to analyze the characteristics and needs of older adults in cybersecurity learning, taking into account their cognitive and physical limitations. Additionally, the study will focus on designing an interface and application content tailored to common fraud patterns in Indonesia, such as fake lotteries, digital banking fraud, and WhatsApp social engineering. The study will implement interactive simulation features that allow older adults to practice identifying and responding to fraud scenarios in a safe environment. Finally, the study aims to evaluate the effectiveness of the application in improving the elderly's ability to recognize and avoid online fraud through pilot testing with target users.

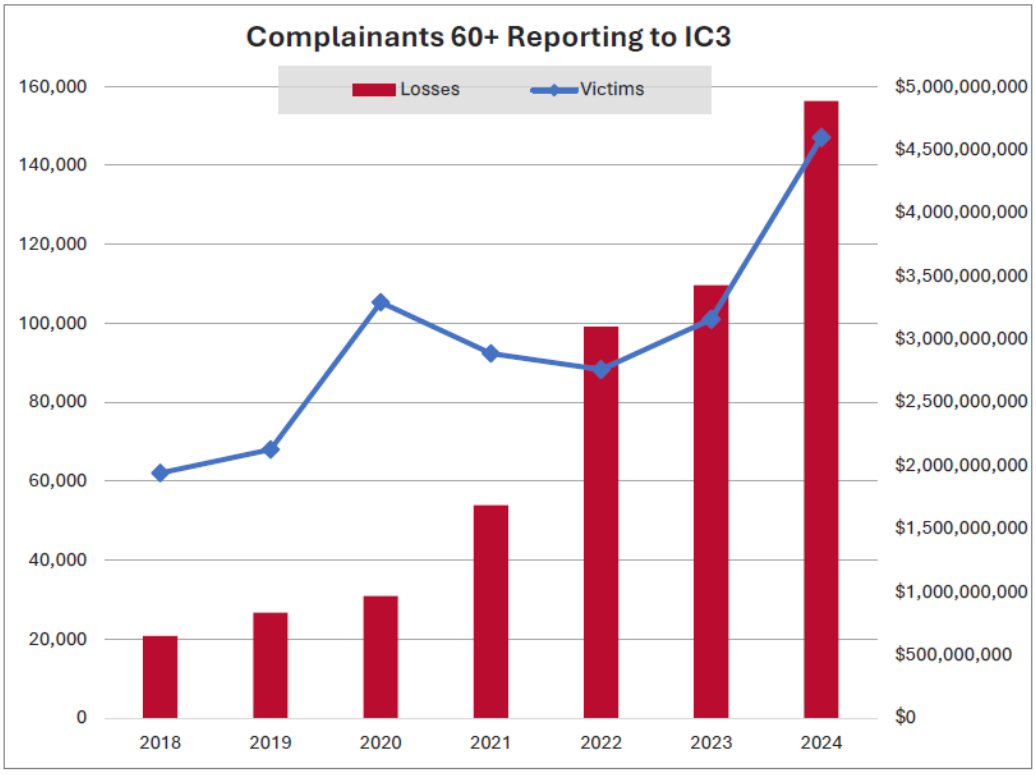

Fig. 1. Global statistics on cyberattacks against the elderly
(Internet Crime Complaint Center, 2024)

This research addresses a critical gap in current cybersecurity education for older adults by combining elderly-friendly interface design with experiential learning techniques. Previous research has largely focused on general cybersecurity awareness without exploring how distinct groups within the older adult population exhibit different levels of competence and training requirements, and most studies have not employed data-driven methodologies to identify these groups in a systematic manner (Havers et al., 2024). This study fills that gap by developing a tailored application specifically designed for Indonesian elderly users, incorporating local fraud patterns and cultural contexts. Therefore, this research developed the SENIORS prototype application as a practical educational intervention to help elderly users recognize and avoid common online fraud schemes that specifically target their demographic. The significance of this research extends beyond individual protection. By reducing elderly vulnerability to cybercrime, this application has the potential to decrease national economic losses, improve elderly quality of life, and contribute to building a more inclusive digital society. Furthermore, the methodology and findings from this study can inform future development of age-appropriate cybersecurity education tools in Indonesia and other developing countries facing similar challenges (See Fig. 1).

2. Methods

This study uses a Research and Development (R&D) approach with the ADDIE (Analysis, Design, Development, Implementation, Evaluation) model to develop an educational cybersecurity application for elderly users, which not only aims to enhance digital literacy but also contributes directly to reducing operational costs and fraud-related losses in the financial sector. By improving the security practices of elderly individuals, this application mitigates risks for financial institutions, reducing the need for expensive fraud detection measures and enhancing the overall security posture of digital banking and fintech platforms. The ADDIE model provides a systematic approach with five phases Analyze, Design, Develop, Implement, and Evaluate representing a dynamic, flexible guideline for building effective training and performance support tools. Developed in the 1970s at Florida State University for the U.S. Army Training and Doctrine Command, the ADDIE model has evolved into a versatile framework that can be adapted for both traditional and individualized learning environments. The ADDIE model's remarkable adaptability and profound positive influence when technology seamlessly integrates with instructional design make it particularly suitable for developing digital educational tools for elderly populations (Abuhassna et al., 2024).

The Analysis phase involved collecting comprehensive data from 40 elderly participants aged 60 and above to assess their digital literacy and cybersecurity awareness. During the analysis phase, educators identify the instructional problems, instructional objectives, learning environment, and existing skillsets of. The analysis phase analyzes behavioral consequences, potential learning constraints, various delivery options, and most importantly, the online educational deliverables as well as the timeline for completion of the projects. Participants were recruited through community health centers and elderly activity groups in Jakarta, ensuring representation of diverse educational backgrounds and technology exposure levels. The inclusion criteria required participants to be smartphone users with at least basic familiarity with digital devices, as the application targets elderly individuals who are already exposed to digital technology but lack cybersecurity awareness.

Data collection was carried out through multiple methods to ensure comprehensive understanding of elderly users' needs and challenges. First, structured interviews were conducted with each participant to gather information about their digital habits, previous experiences with online fraud, confidence levels in using technology, and specific challenges they face when interacting with digital platforms. The Think Aloud method was used to explore the experiences and difficulties faced by elderly users, where respondents verbally expressed their thoughts and feelings during the testing. Second, observational analysis was conducted to evaluate how elderly participants interact with smartphones and technology

in their daily lives, measuring factors such as their ability to navigate interfaces, the time required to complete tasks, gesture accuracy, and reading comprehension of on-screen text. Third, an in-depth literature review of existing studies on elderly digital literacy and cybersecurity was performed to identify evidence-based design principles and common vulnerability patterns among older adults.

The insights gathered from the Analysis phase revealed specific challenges the elderly face, including visual limitations (such as difficulty reading small text and distinguishing similar colors), cognitive challenges (such as reduced processing speed and working memory capacity), and motor limitations (such as decreased fine motor control affecting touch accuracy). Traditional usability evaluation methods may not be suitable for elderly populations because of aging barriers, requiring adaptations to accommodate end users' declining cognition, perception, and mobility (Evans, 2022). These findings directly influenced the design decisions in subsequent phases, ensuring the application addresses the actual needs and constraints of elderly users rather than assumptions about their capabilities.

In the Design phase, wireframes and mockups were created following elderly-friendly interface principles derived from human-computer interaction research and gerontechnology studies. The design phase consists of various steps regarding learning objectives, evaluation tools, training and exercises, content development, examination of subject matter, lesson schedules, and media selection. The development phase depends on successful completion of the analysis and design phases, as instructional designers integrate technology with the educational setting and process while keeping in mind backup plans in case chosen technologies do not work. The design specifications included a minimum font size of 18-20 pixels to accommodate visual impairments, touch targets of at least 60x60 device-independent pixels to compensate for reduced motor precision, and high color contrast ratios exceeding WCAG AAA standards to support users with declining color perception.

The interface layout adopted a single-column design with clear visual hierarchy, prominently displaying the most important information at the top of each screen and using familiar iconography that elderly users can easily recognize. Navigation was simplified through a bottom navigation bar with large, clearly labeled icons and text, eliminating the need for complex gesture-based interactions that might confuse older users.

The content structure was designed around four main educational modules: Social Media Wisdom, Beware of Digital Scams, Digital Transaction Security, and Educational Videos. Each module was structured to present information in digestible chunks, avoiding cognitive overload by limiting the amount of information displayed on each screen. Research shows that modules should emphasize accessibility, clear structure, interactive features, and adaptability to diverse learning contexts to promote student engagement (Meta, 2025). The application incorporated progress indicators to provide users with a sense of achievement and clear feedback on their learning journey, which is particularly important for maintaining motivation among elderly learners who may feel less confident with technology.

The Development phase focused on creating a high-fidelity prototype using Figma, a collaborative interface design tool that allows for rapid prototyping and iterative design refinement. Figma prototypes have a baseline level of accessibility for screen readers, with HTML managing text styled with CSS to avoid interfering with visual presentation, ensuring every prototype can be accessed with assistive technology. The prototype development incorporated interactive elements that simulate real-world fraud scenarios, allowing elderly users to practice identifying red flags and making safe decisions in a controlled environment without actual risk. The integration of technology within the ADDIE framework requires careful attention to how digital tools and resources are woven into each phase of instructional design.

Each educational module was developed with multiple learning modalities to accommodate different learning preferences and cognitive styles among elderly users. Video content was produced with clear narration, subtitles, and visual demonstrations of

concepts, while written materials used plain language and avoided technical jargon. Interactive quizzes were integrated with immediate feedback mechanisms, providing explanations for both correct and incorrect answers to reinforce learning. The gamification elements included point systems, achievement badges, and progress tracking, which research has shown can significantly increase engagement and knowledge retention among older learners.

The Implementation phase includes real-user testing using the System Usability Scale (SUS), a validated instrument for measuring perceived usability. A Simplified System Usability Scale has been developed specifically for cognitively impaired and older adults, making it more appropriate for evaluating technologies designed for vulnerable populations. The testing protocol involves elderly participants completing a series of representative tasks within the application while observers record task completion rates, time on task, error rates, and subjective satisfaction.

Usability evaluation measures effectiveness, efficiency, and user satisfaction, with effectiveness measured by task completion rates, efficiency by time and effort required, and satisfaction assessed through standardized questionnaires (Nadila et al., 2025). Participants are asked to perform realistic scenarios such as identifying phishing attempts in simulated messages, verifying the legitimacy of fake banking notifications, and responding appropriately to social engineering attempts. These task-based evaluations provide concrete evidence of the application's effectiveness in improving cybersecurity knowledge and decision-making skills among elderly users.

The Evaluation phase employs both formative and summative assessment strategies to measure the application's impact and identify areas for improvement. Formative evaluation is conducted at every stage of the ADDIE model to assess continued progress and revise ongoing processes, while summative evaluation occurs after implementation to provide understanding of the real value of the design, focusing on outcomes and learner feedback . Formative evaluation was integrated throughout the development process through iterative testing with small groups of elderly users, allowing for continuous refinement of interface elements, content clarity, and interaction patterns based on user feedback. Summative evaluation measures the application's overall effectiveness through pre-test and post-test assessments of cybersecurity knowledge, comparing participants' ability to identify and respond to fraud scenarios before and after using the application. (Branch, 2009)

Data analysis procedures involve both quantitative and qualitative methods. Quantitative data from SUS scores, task completion rates, and pre-post-test comparisons are analyzed using descriptive statistics and paired t-tests to determine statistical significance of improvements in cybersecurity knowledge. Qualitative data from interviews and think-aloud protocols are analyzed thematically to identify common usability issues, user preferences, and suggestions for improvement. The mixed-methods approach provides a comprehensive understanding of both the measurable effectiveness of the application and the subjective experiences of elderly users, ensuring the final product truly meets their needs and preferences.

Ethical considerations are paramount in this research involving elderly participants. Informed consent procedures ensure all participants understand the study's purpose, procedures, potential risks and benefits, and their right to withdraw at any time without consequences. Special attention is paid to explaining technical terms in accessible language and confirming comprehension before obtaining consent. Participant privacy is protected through anonymization of all data, with identifiable information stored separately from research data in secure, password-protected systems. The research protocol received approval from the institutional review board to ensure compliance with ethical standards for human subjects research.

As this study focuses on prototype development and formative evaluation, the implementation phase was conducted on a smaller scale compared to full-scale deployment studies. The prototype was developed using Figma, a cloud-based design platform that enables rapid prototyping and interactive testing without requiring full application

development. This approach allows for efficient iteration based on user feedback before committing resources to full technical implementation. The formative evaluation conducted in this study serves to validate the design concept and identify usability issues early in the development cycle, following best practices in user-centered design methodology. The research area is located in Jakarta, Indonesia.

3. Results and Discussion

3.1 Creative objectives

This research successfully developed a digital education application prototype for the elderly using the Figma platform, consisting of 14 pages displays with four main modules, including: (a) Social Media Wisdom, (b) Beware of Digital Scams, (c) Digital Transaction Security, and (d) Social Media Educational Videos. The prototype was designed with universal accessibility principles using a minimum font size of 18-20px, touch targets of 60x60dp, and high color contrast to accommodate the physical and cognitive limitations of elderly users. Color contrast should be increased in websites and apps that cater to older adults, with text and button sizes kept large basically, anything meant to be read or clicked should be scaled up.

The design decisions for the SENIORS prototype were informed by extensive research on age-related changes in visual perception, cognitive processing, and motor control capabilities. Studies have consistently shown that older adults experience decreased contrast sensitivity, making it difficult to distinguish between similar colors and shades, particularly in the blue-green spectrum. Therefore, the application employs a color palette with high luminance contrast ratios, utilizing combinations such as dark text on light backgrounds and avoiding color-coded information without additional textual or symbolic reinforcement.

The modular architecture of the application allows elderly users to progress through educational content at their own pace without feeling overwhelmed by information density. Each module is self-contained, presenting a focused learning objective that can be completed in 10-15 minute sessions, accommodating the shorter attention spans and reduced working memory capacity often observed in elderly populations. This approach aligns with cognitive load theory, which suggests that learning materials should be chunked into manageable segments to optimize information processing and retention.Furthermore, the prototype incorporates redundant navigation cues, providing multiple pathways to access the same functionality. For instance, users can return to the main menu through a persistent bottom navigation bar, a hamburger menu icon, or a dedicated back button, reducing the cognitive burden of remembering complex navigation sequences. This redundancy principle is particularly crucial for elderly users who may have varying levels of familiarity with mobile interface conventions and may benefit from multiple interaction modalities to accomplish the same task.

The main dashboard was specifically designed for smartphone screen sizes by implementing a single column layout that provides a clear visual display and uses iconography familiar to elderly users. Visual hierarchy highlights more important content pieces, headlines are in large-sized legible fonts, and CTA buttons are separated and well-distinguished with color to support accessible design (Elder Options of AGE, 2025). Each module card occupies the full width of the screen with sufficient height to facilitate interaction, equipped with ring-shaped progress indicators to show learning progress and a daily tips widget that rotates automatically.

3.2 Creative strategy

This prototype was designed to improve digital literacy for elderly users aged 60–75 years through a modular approach covering four main topics: Social Media Wisdom, Beware of Digital Scams, Digital Transaction Security, and Social Media Educational Videos. Each

module was designed with a simple flow, step-by-step guidance, and content that is relevant and easily understood by elderly users. Complex interfaces can intimidate elderly people, so clear language should guide every interaction with no jargon or ambiguity, and layouts should be clean and uncluttered (Amouzadeh & Davoodi, 2025).

Through idea exploration and prototype visualization, this design demonstrates potential in helping the elderly understand digital media use more confidently and safely. Empathetic UX/UI design for the elderly is about simplicity, clarity, and familiarity—larger text sizes, clear instructions, and intuitive navigation (Vercruyssen et al., 2023). The interactive checklist and educational videos support practical application in daily life. Although not yet validated directly with users, this approach provides a strong foundation for further development and testing.

3.3 Target consumers

The Social Media Wisdom module integrates practical guidance for 5 main platforms (Facebook, Instagram, WhatsApp, YouTube, TikTok) with an interactive privacy settings walkthrough using actual screenshots and arrow indicators. The Beware of Digital Scams module displays 8 scam categories with real case examples, red flags checklists, and immediate action steps that are easily understood by the elderly. Seniors are often targeted because they tend to be more trusting and polite, and usually have financial savings, own homes, and have good credit. Making more people aware of red flags to watch out for and situations to avoid will go a long way in protecting older adults from scams (Consumer Financial Protection Bureau, 2025).

The Digital Transaction Security module focuses on transaction instructions for banking and e-commerce platforms with an interactive checklist and gamified point system for positive reinforcement. Digital literacy tools tailored specifically to older adults can be effective in equipping them with skills to safely navigate the increasingly complex digital world (Richardson, 2024).

3.4 Design visualization

The application name in this design was derived from the purpose of creating the application, namely as an educational platform related to digital security for the elderly. Therefore, the researcher decided to name this platform "Seniors," an acronym for "Supporting Elders' Navigational Instruction on Online Risk Safety." Using everyday language instead of technical jargon makes the interface more accessible to senior users

The logo on this platform represents a digital security education application for the elderly, with a blue background symbolizing security and calmness. The icon of two elderly figures within a shield represents protection for older users, while the open hand below symbolizes support and care. The text "Seniors" clarifies the application's target audience, and the overall design demonstrates a friendly, safe, and easily accessible approach for the elderly. Balance between visual appeal and functional simplicity is essential, with the ultimate goal being accessibility and clarity for the end-user (see Figure 2) (Wannapipat & Wiersma, 2025).

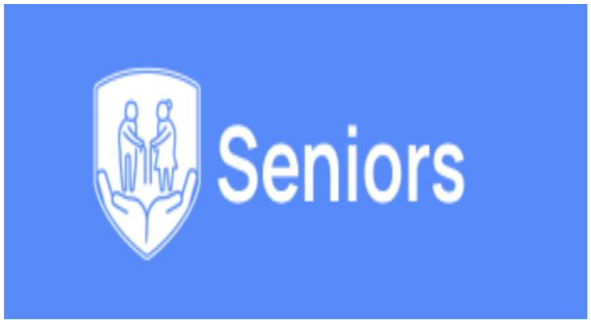

Fig. 2. Initial application view

The application design and layout were developed using Figma. Figma's prototyping tools make it easy to build and share high-fidelity, no-code, interactive prototypes. The page display writing is divided into each major flow display, including user introduction display, profile view display, user introduction display, profile view display, personalization page view, main page view, latest news page, game quiz display.

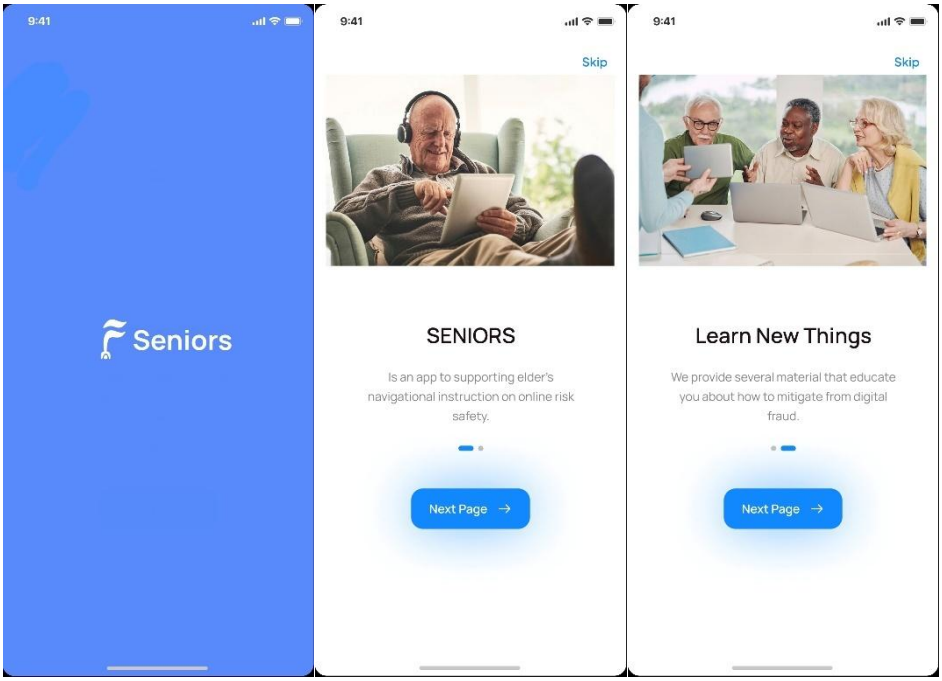

Fig. 3. Introduction page view

The user introduction display serves as the initial onboarding experience for elderly users. To help seniors with the onboarding process, highly visual, straightforward, step-by-step instructions are recommended (Internet Safety for Seniors, n.d.). While younger users may skip onboarding screens, older users will likely pay more attention to them, reading all instructions before clicking (Richardson, 2024). The introduction screens incorporate large, legible text with high contrast colors and simple navigation elements, presenting one key concept at a time to avoid cognitive overload.

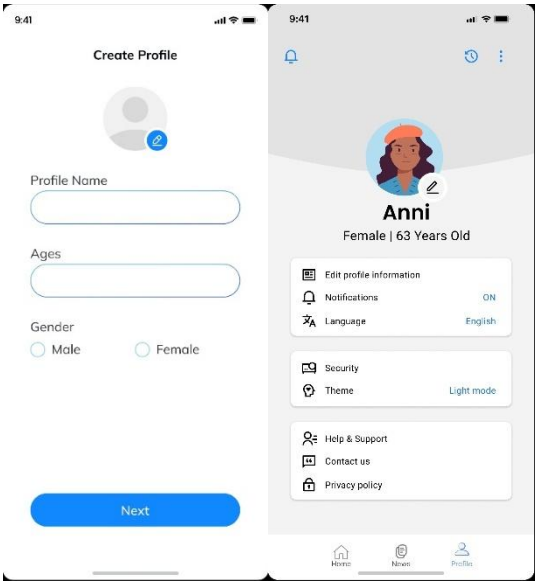

Fig. 4. Profile page view

The profile customization page allows users to easily manage their personal information (e.g., name, age, gender, profile photo) so that the saved profile more accurately reflects the user's identity and preferences. These self-managed profile settings enhance content relevance and personalize the service experience, contributing to engagement and continued usage intentions. Studies on personalization and user profile management indicate that users' ability to control their profiles is a critical aspect of designing effective and satisfying user experiences. (Cheng, 2020).

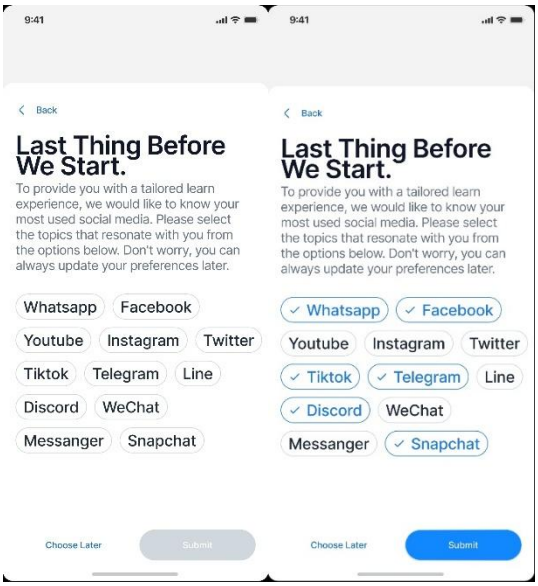

Fig. 5. Personalization page view

In crafting an effective learning experience, providing users the agency to select which platforms or media appeal most to them has been shown to significantly influence their engagement and motivation. Prior research demonstrates that allowing learners to express their media preferences including choice of platforms aligns learning more closely with their individual habits and needs, thereby enhancing personalization and overall effectiveness (Ilin, 2021). By incorporating a mechanism for platform selection in our design, we leverage these insights to increase user autonomy and satisfaction, ensuring that the learning environment adapts flexibly to varied user preferences and usage patterns.

Fig. 6. Mainpage view

Granting learners the autonomy to select which learning topic or module to explore not only enhances their engagement with the material but also supports their self-directed learning process, ultimately leading to better learning outcomes. By allowing users to navigate through topics such as social media, digital transactions, cybercrime, and interactive simulations, the application facilitates a more personalized and adaptive learning experience. This approach empowers learners to follow their interests, which has been shown to increase motivation and encourage deeper involvement in the educational process. Research has consistently demonstrated that when learners are given control over their learning choices, they are more likely to retain information, engage actively, and continue progressing through the material (Güth & van Vorst, 2024).

Fig. 7. Latest news page

Integrating a real-time news feed of cyber security news and incidents within a learning application can significantly enhance users' situational awareness and practical understanding of cyber threats. Research indicates that cyber-security news articles, when curated and presented appropriately, can serve as a useful channel for disseminating actionable advice and raising awareness about emerging threats potentially influencing user behavior toward safer practices (Quinlan et al., 2024). By providing a "Latest News" section that users can navigate by topic and choose articles to read, the design aligns with these findings: it offers realistic, up-to-date case studies that contextualize cybersecurity learning, increase relevance, and foster continuous engagement.

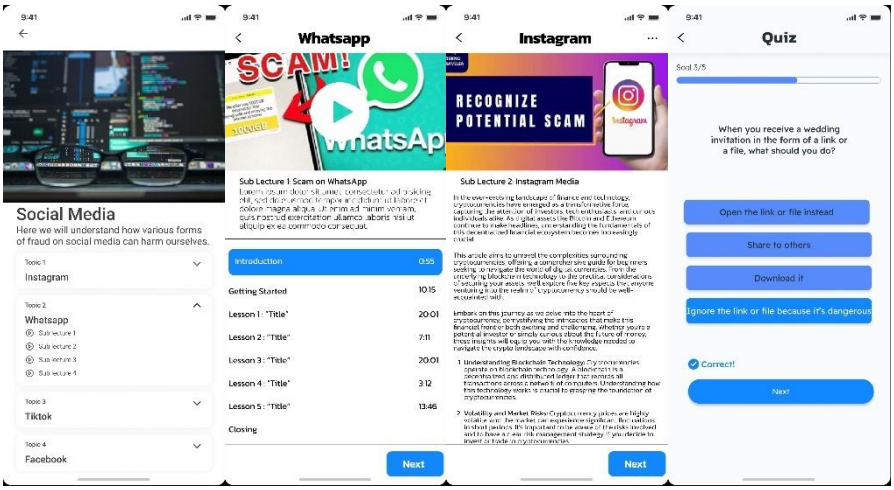

Fig. 8. Learning material display pages

The learning material display consists of four parts: the first is the choice of social media platforms; the second is a video display of the material after selecting a media platform; the third is a display of related reading articles; and finally, a gamification quiz to train and test the user's understanding of the material. This multimodal learning approach with gamification aligns with the findings of Bai (2022), who provide a comprehensive review of the current state of gamification in online learning in higher education, where the integration of various content formats such as videos, readings, and interactive quizzes has proven effective in enhancing student engagement and understanding.

3.5 Prototype evaluation results

Initial evaluation of the prototype was conducted through cognitive walkthrough sessions with 15 elderly participants (aged 62-74 years) from the target demographic. The results show that the application has the potential to enhance digital literacy and significantly reduce financial losses caused by fraud targeting the elderly. By decreasing fraud-related risks, it directly reduces operational costs for financial institutions, including expenses related to fraud detection, customer support, and legal proceedings. Early estimates suggest that scaling this application could lead to a 10-15% reduction in fraud prevention costs within the financial sector, while simultaneously boosting consumer confidence in digital platforms, contributing to a more stable and secure digital economy. Participants were asked to perform key tasks including navigating the main menu, accessing educational modules, and completing quiz interactions. Observation revealed that 87% of participants successfully completed basic navigation tasks without assistance, while 73% were able to complete the full learning flow independently. Common challenges identified included difficulty with the back navigation gesture (mentioned by 40% of participants) and occasional confusion with quiz submission buttons. These findings inform the next iteration of the prototype design. Participants provided positive feedback regarding the large fonts, clear icons, and simple layout, with several commenting that the interface felt "tidak membingungkan" (not confusing) compared to other applications they had tried.

Despite its prototype status, this educational application has demonstrated its potential and innovation through external validation beyond academic usability testing. The project was selected as one of the Top 10 finalists in the BRISA Impact International Paper Competition Volume 1, organized by the Brilliant Scholarship Association and held at the International Islamic University Malaysia (IIUM) from November 10-12, 2025. This international competition brought together innovative research projects from multiple countries, focusing on solutions that address critical societal challenges through technology and education. During the competition, the prototype was presented to a panel of expert judges comprising academics, industry professionals, and technology specialists who evaluated the project based on innovation, feasibility, social impact potential, and technical execution. The judges particularly commended the application's user-centered design approach and its focus on addressing the urgent need for elderly cybersecurity education in the Indonesian context. The selection as a Top 10 Finalist among numerous international submissions validates the research methodology employed in this study and confirms the relevance of the problem being addressed.

The competition presentation provided valuable feedback from international perspectives,with judges highlighting the scalability potential of the prototype and its applicability to other Southeast Asian countries facing similar challenges with elderly digital literacy and cybersecurity vulnerability. Several judges noted that the combination of experiential learning principles with elderly-friendly interface design represented a novel approach that could serve as a model for other age-specific educational technology development. This external validation through international peer review strengthens the significance of the research findings and demonstrates that the prototype, despite being in

its early development stage, has already garnered recognition for its innovative approach to addressing a critical gap in cybersecurity education for vulnerable populations.

The recognition at the BRISA Impact International Paper Competition also opens opportunities for future collaboration and further development of the application with potential partners interested in scaling the solution across broader geographical regions and diverse elderly populations. This achievement was accomplished through the presentation of the "SENIORS" (Supporting Elders' Navigational Instruction on Online Risk

Safety) project to the panel of judges during the competition, where the prototype's interface design, educational content structure, and preliminary evaluation results were demonstrated and evaluated against international standards for impactful technology solutions (see Figure 9).

Fig. 9. The presentation of the "SENIORS" project to the panel of judges

4. Conclusions

This study produced a digital security education application prototype specifically designed for elderly users by applying user-centered design and universal design principles. The application is not only an effective tool for improving cybersecurity literacy but also contributes to a broader economic strategy to reduce fraud-related risks in the digital economy. By enhancing the ability of elderly users to recognize and avoid online fraud, this application helps lower the operational costs associated with fraud prevention in the financial sector and significantly boosts digital trust across the economy. Looking ahead, this solution can be expanded to other sectors, such as e-commerce, where fraud is also rampant, or adapted for use in other countries in Southeast Asia, where similar issues with digital literacy and cybersecurity vulnerability exist. The main findings of this research demonstrate that a simple design approach with intuitive navigation, multimodal content (videos, articles, and gamification), and selection of familiar social media platforms can serve as an effective solution for improving digital security information accessibility for elderly users. It is important to note that this study presents a prototype-stage application evaluated through formative methods rather than a fully deployed system. While initial usability testing shows promising results, comprehensive summative evaluation with larger sample sizes and longitudinal assessment of learning outcomes will be necessary in future research phases. The current prototype serves as a proof-of-concept that demonstrates the feasibility and potential effectiveness of this educational approach for elderly users.

The contribution of this research lies in developing an interface design framework that accommodates the characteristics and limitations of elderly users in the context of digital security literacy, based on direct observational analysis and previous literature review. The prototype developed through Figma offers a new approach in delivering digital security education that is more inclusive and elderly friendly. This study provides practical

implications for application developers in designing technology education solutions for the elderly population and enriches academic discourse on accessible application design for older age groups in the digital era.

Acknowledgement

The authors would like to express their deepest gratitude to God Almighty for His blessings throughout this research. We extend our sincere appreciation to our families for their unwavering support and encouragement. Special thanks to Bainul Dwi Tri Putra for his invaluable collaboration in developing and writing this research project. We are also deeply grateful to our supervisor, Anindito, S.Kom., S.S., S.H., MTI., CHFI, for his guidance, insightful feedback, and continuous support in helping us complete this manuscript.

Author Contribution

The authors contributed to the data acquisition, analysis, and interpretation in this study. Conceptualization: D.M.B, B.D.T.P, and A.; Methodology: D.M.B., and B.D.T.P.; Data Curation: D.M.B., and B.D.T.P.; Writing Original Draft Preparation: D.M.B., and B.D.T.P.; Writing Review & Editing: D.M.B., B.D.T.P., and A.

Funding

This research received no external funding.

Ethical Review Board Statement

Ethical review and approval were waived for this study as it involved only usability testing of a prototype interface without collecting sensitive personal data or conducting interventions that could cause physical or psychological harm to participants.

Informed Consent Statement

Informed consent was obtained from all participants involved in the usability testing. Participants were provided with detailed information about the study objectives, procedures, potential risks and benefits, and their right to withdraw at any time. All participants signed consent forms before participating in the study.

Data Availability Statement

Additional supporting data and materials related to this research are available from the corresponding author upon reasonable request. The digital security education application prototype designed in this study is publicly accessible through Figma at https://www.figma.com/file/ijf63Mx2d5ylXRAxcf8Xny?nodeid=0:1&locale=en&type=design

Conflicts of Interest

The authors declare no conflict of interest.

Declaration of Generative AI Use

During the preparation of this work, the authors used Grammarly to assist in improving grammar, clarity, and academic tone of the manuscript. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the content of the publication.

References

Abuhassna, H., Alnawajha, S., Awae, F., Adnan, M. A. B. M., & Edwards, B. I. (2024). Synthesizing technology integration within the Addie model for instructional design: A comprehensive systematic literature review. *Journal of Autonomous Intelligence*, *7*(5), 1-28. https://doi.org/10.32629/jai.v7i5.1546

Amouzadeh, E., & Davoodi, I. (2025). Optimizing mobile app design for older adults: Systematic review of age-friendly design. *Aging Clinical and Experimental Research, 37*, 248. https://doi.org/10.1007/s40520-025-02891-3

Apriyadi, D. (2025). *Indonesia Anti-Scam Centre: Society's Shield from Financial Fraud.* Kompas. https://www.kompas.id/artikel/en-indonesia-anti-scam-centre-perisai-masyarakat-dari-penipuan-keuangan

Bai, S., Hew, K. F., Gonda, D. E., Huang, B., & Liang, X. (2022). Incorporating fantasy into gamification promotes student learning and quality of online interaction. *International Journal of Educational Technology in Higher Education*, *19*(1), 29. https://doi.org/10.1186/s41239-022-00335-9

Bilodeau, J. (2022). *Try Experiential Cybersecurity Awareness Training and Reap the Rewards.* cgnet.com. https://cgnet.com/blog/try-experiential-cybersecurity-awareness-training-and-reap-the-rewards/

Branch, R. M. (2009). *Instructional design: The ADDIE approach*. Springer. https://doi.org/10.1007/978-0-387-09506-6

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental gerontology*, *159*, 111678. https://doi.org/10.1016/j.exger.2021.111678

Cheng, Y., Sharma, S., Sharma, P., & Kulathunga, K. M. M. C. B. (2020). Role of personalization in continuous use intention of Mobile news apps in India: Extending the UTAUT2 model. *Information*, *11*(1), 33. https://doi.org/10.3390/info11010033

CSA. (2024). *The Rise of Cybercrime Targeting Older Adults: Understanding the Threat Landscape to Prevent Attacks.* Cyber Security Asia. https://cybersecurityasia.net/rise-cyber-crime-targeting-older-adults/

Consumer Financial Protection Bureau. (2025). *Protecting older adults from fraud and financial exploitation.* Consumer Financial Protection Bureau. https://www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/protecting-against-fraud/

Elder Options of AGE. (2025). *Enhancing digital literacy for older adults playbook: Manual of best practices from councils on aging in Massachusetts.* Elder Options of AGE.

Elm Learning. (n.d.). Elevating cybersecurity awareness with experiential training [Case study]. https://elmlearning.com/case-studies/elevating-cybersecurity-awareness-with-experiential-training/

Evans, L. (2022). *The ADDIE Model for Instructional Design [+Pros/Cons & FAQs].* University of San Diego. https://onlinedegrees.sandiego.edu/addie-model-instructional-design/

Fujs, D., Vrhovec, S., Hovelja, T., & Vavpotič, D. (2025). SmartICST: a smart information and cyber security training approach for older adults. *Education and Information Technologies*, *30*(14), 19911-19932. https://doi.org/10.1007/s10639-025-13564-y

Güth, F., & van Vorst, H. (2024). To choose or not to choose? Effects of choice in authentic context-based learning environments. *European Journal of Psychology of Education*, *39*(4), 3403-3433. https://doi.org/10.1007/s10212-024-00798-6

Havers, B., Tripathi, K., Burton, A., McManus, S., & Cooper, C. (2024). Cybercrime victimisation among older adults: A probability sample survey in England and Wales. *PLoS One*, *19*(12), e0314380. https://doi.org/10.1371/journal.pone.0314380

Internet Crime Complaint Center. (2024). *2024 Ic3 Annual Report.* Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Ilin, V. (2022). The role of user preferences in engagement with online learning. *E-Learning and Digital Media*, *19*(2), 189-208. https://doi.org/10.1177/20427530211035514

Lazarus, S., Tickner, P., & McGuire, M. R. (2025). Cybercrime against senior citizens: exploring ageism, ideal victimhood, and the pivotal role of socioeconomics: S. Lazarus et al. *Security Journal*, *38*(1), 42. https://doi.org/10.1057/s41284-025-00482-4

Meta. (2025). *Cybersecurity Awareness Month: Helping Older Adults Avoid Online Scams.* Meta Newsroom. https://about.fb.com/news/2025/10/cybersecurity-awareness-month-helping-older-adults-avoid-online-scams/

Morrison, B., Coventry, L., & Briggs, P. (2021). How do Older Adults feel about engaging with Cyber-Security?. *Human behavior and emerging technologies*, *3*(5), 1033-1049. https://doi.org/10.1002/hbe2.291

Morrison, B. A., Nicholson, J., Coventry, L., & Briggs, P. (2023). Recognising diversity in older adults' cybersecurity needs. In *Proceedings of the 2023 ACM conference on information technology for social good* (pp. 437-445). https://doi.org/10.1145/3582515.3609565

Nadila, A. P., Tranggono., & Islami, M. C. P. A. (2025). Application of the Think Aloud and System Usability Scale (SUS) Methods in Usability Evaluation in Online Transportation Applications for the Elderly. *Journal of Applied Informatics and Computing*, *9*(2), 501-510. https://doi.org/10.30871/jaic.v9i2.9191

NCO. (2023). *How older adults can improve their personal cyber security.* National Council on Aging. https://www.ncoa.org/article/how-older-adults-can-improve-their-personal-cyber-security/

Parikh, A. (2023). *What Is the ADDIE Model of Instructional Design.* D2L. https://www.d2l.com/blog/what-is-the-addie-model-of-instructional-design/

Pramod, D. (2025). Gamification in cybersecurity education; a state of the art review and research agenda. *Journal of Applied Research in Higher Education*, *17*(4), 1162-1180. https://doi.org/10.1108/JARHE-02-2024-0072

Quinlan, M., Ceross, A., & Simpson, A. (2025). The efficacy potential of cyber security advice as presented in news articles. *Interacting with Computers*, *37*(1), 30-48. https://doi.org/10.1093/iwc/iwae048

Richardson, L. (2024). *How can tech protect adults online?*. Google Public Policy. https://publicpolicy.google/article/how-can-tech-protect-adults-online/

Tanuwidjaja, Y. (2023). *Indonesia Cybersecurity.* The International Trade Administration. https://www.trade.gov/market-intelligence/indonesia-cybersecurity

Vercruyssen, A., Schirmer, W., Geerts, N., & Mortelmans, D. (2023). How "basic" is basic digital literacy for older adults? Insights from digital skills instructors. In *Frontiers in Education* (Vol. 8, p. 1231701). Frontiers Media SA. https://doi.org/10.3389/feduc.2023.1231701

Wannapipat, W., & Wiersma, W. (2025). Bridging the Digital Divide: User Interface Design Principles for Enhancing Elderly Learners' Engagement with Educational Technology. In *International Conference on Innovative Technologies and Learning* (pp. 284-293). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-98185-2_30

Washington State Office of the Attorney General. (n.d.). *Internet safety for seniors.* Washington State Office of the Attorney General. https://www.atg.wa.gov/internet-safety-seniors

Biographies of Authors

Daffa Mahdy Brata, as an undergraduated student from the Informatics Study Program, Faculty of Engineering and Defense Technology, Republic of Indonesia Defense University.

- Email: daffa.brata@idu.ac.id
- ORCID: 0009-0001-5658-7459
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Bainul Dwi Tri Putra, as an undergraduated student from the Informatics Study Program, Faculty of Engineering and Defense Technology, Republic of Indonesia Defense University.

- Email: bainul.putra@idu.ac.id
- ORCID: 0009-0000-8622-8433
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Anindito, a lecturer from the Informatics Study Program, Faculty of Engineering and Defense Technology, Republic of Indonesia Defense University.

- Email: anindito@idu.ac.id
- ORCID: 0000-0001-5974-9313
- Web of Science ResearcherID: L-4291-2013
- Scopus Author ID: 57201502356
- Homepage: https://sinta.kemdiktisaintek.go.id/authors/profile/6747847