

INNOVATION DEVELOPMENT FOR PREVENTING ONLINE FRAUD THROUGH CRIME PATTERN APPLICATION IN NONTHABURI PROVINCE

**¹Pol.Lt.Col.Jirut Sonkratai, ²Pol.Maj.Siwaluck Lailers,
³Assoc.Prof.Pol.Col.Dr.Kannika Kukudrua,
⁴Assoc.Prof.Pol.Col.Paphat Wasuthawat, ⁵Pol.Lt.Col.Neti Srisakul**

Abstract

The impact of online fraud has expanded widely, posing challenges for effective management and control despite continuous efforts by relevant agencies to develop mechanisms and preventive measures. This applied research aimed to develop an innovation for preventing online fraud, enhancing evidence management, and applying crime pattern theory within the context of Nonthaburi Province, Thailand. A research and development (R&D) design was employed with purposive sampling of 127 informants, including community leaders from Suan Yai, Talat Khwan, and Bang Khen subdistricts, police officers from Mueang Nonthaburi Police Station, officers from the Nonthaburi Provincial Administrative Organization and Nonthaburi Municipality, and local residents of Suan Yai. Two research instruments were utilized: a set of focus group discussion questions and an efficiency evaluation scale.

The development outcome was an enhancement of the SafetyVacc application, integrating a crime pattern menu and case classification guidelines within the "Fraud Awareness" feature. This innovation relied on crime pattern information contributed by communities and relevant officials, enabling experiential learning and awareness of current online fraud typologies. A strong emphasis was placed on evidence management to prevent data loss, thereby facilitating law enforcement in suspect apprehension. The application is compatible with both iOS and Android systems.

The efficiency evaluation results, both overall and by dimensions (content, design, and usability), were rated from high to very high. Post-implementation feedback suggested incorporating a real-time alert system for emerging online fraud threats and linking the application to online complaint channels or relevant authorities to support legal procedures. The findings highlight the utility of this innovation in strengthening public capacity for online fraud prevention and demonstrate its potential as a prototype for scaling up to other regions.

Keywords: Fraud Prevention Innovation, Online Fraud, Crime Pattern Theory

1. Introduction

According to the statistics presented at the fourth meeting of the Technology Crime Prevention and Suppression Committee on October 30, 2023, the number of online crime cases in Thailand averaged 562 cases per day between September and October 2023, with average daily financial damages of 85 million baht. The five most common cases were online fraud related to product and service sales, employment scams, loan scams, investment fraud, and call center scams (Royal Thai Government, 2023). Similarly, data from the National Online Complaint Management Center between March 1, 2022, and June 28, 2023, revealed that the leading types of online crime victimizing Thai citizens were fraudulent product or service sales, employment-related transfer scams, loan scams, investment fraud through computer systems, and call center threats (Siam Rath Online, 2023).

Despite ongoing efforts, the readiness of current legal measures remains limited. The Royal Decree on Measures for the Prevention and Suppression of Technology Crime (2023) authorizes investigators to accept complaints regarding technology-related crimes regardless of location within the Kingdom and requires financial institutions and businesses to temporarily suspend suspicious transactions involving deposit and e-wallet accounts. Furthermore, the Royal Thai Police issued Order 182/2023 (March 17, 2023), outlining procedures for complaint management, case administration, and assigning responsibilities to the Technology Crime Suppression Center (TCSD). The Royal Thai Police also developed an online complaint system (www.thaipoliceonline.com) to facilitate rapid reporting of technology-related crimes.

Although government agencies have attempted to harness technological advancements for awareness campaigns and fraud prevention—for example, through websites such as 24hicarecenter.com—these efforts remain fragmented, limited in accessibility, and insufficient for vulnerable populations, including the elderly, persons with disabilities, and those with limited digital literacy. Consequently, communication channels between state agencies and the public for online fraud prevention remain incomplete. Field interviews with educational personnel under the Nonthaburi Provincial Administrative Organization revealed knowledge gaps in legal procedures, evidence preservation, and victim support. Such misunderstandings often lead to critical evidence loss, hindering law enforcement. Moreover, there is currently no single, comprehensive, and accessible platform consolidating practical guidelines for citizens in managing online fraud cases, representing a significant pain point in state prevention measures.

In response to these gaps, this research selected Nonthaburi Province as a pilot study area, leveraging prior research capacity and digital knowledge resources. Building on the project “Enhancing Capacity and Strengthening Security Immunity: Seamless 3S Preparedness for Aging Society among Educational Personnel under the Nonthaburi Provincial Administrative Organization”, the researchers previously developed the SafetyVacc application, a Line OA and web-based application providing health and online safety information (Kukudrua et al., 2023). In this study, the application was further developed to transform its original “Online Threats” module into a comprehensive online fraud management system across the entire chain (pre-incident, during incident, and post-incident). The upgraded system incorporates direct links to agencies such as the Technology Crime Suppression Division (TCSD), ensuring reliability, up-to-date information, and community-based accessibility. A distinctive feature of this innovation lies in integrating crime pattern theory into the application, allowing citizens not only to recognize emerging fraud patterns but also to validate information accuracy and relevance, thereby reinforcing resilience against online fraud.

2. Research Objective

The objective of this study is to develop an innovation for preventing online fraud, enhancing evidence management, and applying crime pattern theory within the context of Nonthaburi Province.

3. Research Methodology

This study employed a research and development (R&D) design consisting of four stages. Key informants for each stage and activity were purposively selected based on predetermined criteria, namely: (a) residence in the study area for at least one year, and (b) professional experience of no less than six months. In total, 127 informants participated: 54 in Stage 1, 43 in Stage 3, and 30 in Stage 4. The procedures were as follows:

Stage 1: Research Phase 1

- 1) Review of relevant theories, literature, research studies, regulations, and legal frameworks.
- 2) Conduct four focus group discussions with a total of 54 informants to collect data on practices before, during, and after online fraud incidents. Informants were divided into two groups:
 - *Group 1*: Community leaders from Suan Yai, Talat Khwan, and Bang Khen subdistricts, representing 46 communities (one leader per community).
 - *Group 2*: Eight officials, including police officers from Mueang Nonthaburi Police Station, officers from the Nonthaburi Provincial Administrative Organization (Departments of Education, Religion, and Culture, and Social Welfare), responsible for disseminating information to communities, senior citizen schools, and managing back-office systems of Facebook and the application, as well as officials from Nonthaburi Municipality (Departments of Social Welfare, Secretary's Office, and Strategy and Budget).

Stage 2: Development Phase 1

Based on findings from Stage 1, the researchers designed an online fraud prevention application by further developing the existing **SafetyVacc** platform. The enhancements included:

- Adding a "Fraud Awareness" module to the main menu.
- Integrating a "Crime Pattern" menu with practical guidelines categorized by fraud types, including call center scams, romance scams, loan scams, debt scams, sales fraud, prize transfer scams, employment scams, and other types.
- Providing contact details of relevant agencies for reporting online fraud. The prototype application was reviewed and evaluated by experts in cybercrime and information technology.

Stage 3: Research Phase 2

Verification and pilot testing of the innovation were conducted with 43 informants. Activities included:

- 1) Focus group discussions with 13 community leaders (4–5 per subdistrict across Suan Yai, Talat Khwan, and Bang Khen) to assess and evaluate the prototype.
- 2) Pilot testing of the prototype in Suan Yai subdistrict with 30 participants, followed by an evaluation using an efficiency assessment instrument.

Stage 4: Development Phase 2

The final stage involved testing the application's efficiency with 30 participants in Suan Yai subdistrict, using the efficiency assessment instrument for evaluation.

Research Instruments Two instruments were employed:

1. **Focus Group Discussion Guide:** consisting of five questions designed to assess and evaluate the application.
2. **Efficiency Assessment Scale:** adapted from the learning application efficiency scale developed by Kannika Kukudrua et al. (2023). This scale included two parts: (a) demographic information (8 items), and (b) evaluation of the fraud prevention application's efficiency (15 items) using a five-point Likert rating scale. The total consisted of 23 items.

Instrument Quality Assurance

The quality of instruments was validated through:

- **Content validity** assessed by three experts to ensure language clarity, content coverage, and alignment of items with conceptual definitions (Item Objective Congruence; IOC).
- **Reliability** verified through investigator triangulation to ensure data credibility across researchers and data collectors.

This research was approved by the Human Research Ethics Committee of the Royal Police Cadet Academy.

5. Research Findings

The results of this study can be summarized as follows:

The development of the online fraud prevention application was an extension of the SafetyVacc application, originally produced under the research project *“Enhancing Capacity and Strengthening Security Immunity: Seamless 3S Preparedness for Aging Society among Educational Personnel under the Nonthaburi Provincial Administrative Organization.”* The upgraded application incorporated the “Fraud Awareness” module, providing comprehensive information on online fraud across the entire chain—before, during, and after fraud incidents.

The application was designed to serve both citizens and state officials by enabling them to recognize fraudulent schemes, follow practical guidelines before and after victimization, and directly access contact channels for relevant agencies, including official online reporting systems, thereby preventing repeated

victimization. A distinctive feature of the innovation is the integration of crime pattern data, regularly updated to reflect current online fraud trends.

In addition, the system categorized online fraud into eight common typologies identified in the pilot study area:

1. Call center scams
2. Romance scams
3. Loan scams
4. Debt scams
5. Sales fraud
6. Prize transfer scams
7. Employment scams (work-from-home or part-time income fraud)
8. Other fraud types

These enhancements demonstrate the application's potential as a practical tool for raising awareness, guiding preventive actions, and strengthening collaboration between communities and law enforcement agencies in combating cyber-enabled fraud.

The development of the application is illustrated as shown in Figure 1.

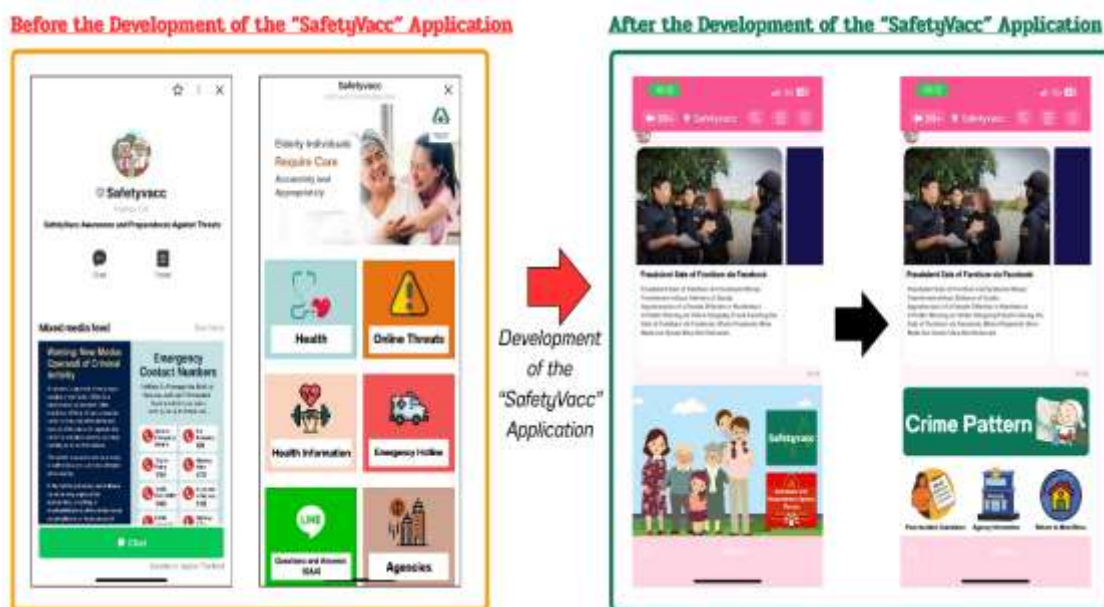


Figure 1 : Development of the "SafetyVacc" Application

The overall and dimensional evaluations of the online fraud prevention application were rated from high to very high. Among the three dimensions, usability received the highest mean score, whereas design received the lowest. Additional feedback from participants suggested specific improvements for each dimension.

- **Content:** Participants recommended incorporating case studies of recent online fraud incidents, adding a Frequently Asked Questions (FAQ) section addressing common concerns, and providing in-depth content on verifying online

information sources. Suggestions also included guidance on identifying trustworthy e-commerce platforms, methods for validating online sellers, and updating the application with newly emerging fraud schemes to maintain relevance.

- **Design:** Feedback emphasized the need to improve readability by adjusting background colors and font clarity. Participants suggested adding a help button or usage instructions on each page, as well as integrating a dark mode for enhanced user experience.
- **Usability:** Respondents proposed implementing a real-time alert system for emerging online threats, introducing step-by-step guidance for victims of online fraud, and linking the application to online complaint channels or relevant authorities to facilitate legal procedures.

Based on this feedback, the research team revised and enhanced the online fraud prevention application.

Post-Improvement Evaluation

Following the improvements, the application was re-evaluated. Results showed that participants' perceptions of its overall and dimensional efficiency remained at high to very high levels. Usability continued to receive the highest mean score, whereas content recorded the lowest. Importantly, comparative analysis revealed improvements across all dimensions as shown in Figure 2.:

- Content increased by **0.09**
- Design increased by **0.12**
- Usability increased by **0.01**

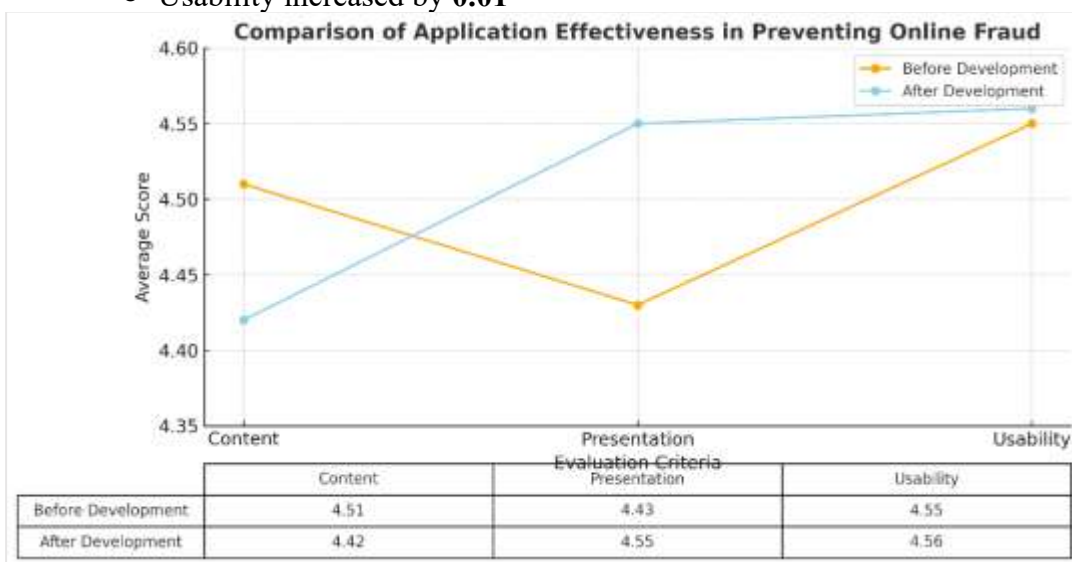


Figure 2 : Comparison of Application Effectiveness in Preventing Online Fraud

6. Discussion

The findings of this study highlight critical insights into addressing the growing challenges of online fraud, which has become increasingly severe and complex, generating widespread impacts on individuals and society. Beyond financial losses, online fraud undermines citizens' sense of safety, erodes trust in social and economic systems, and can exert macro-level consequences on national economic stability. Against this backdrop, the present research sought to establish a systematic framework for citizens to prevent and cope with cyber fraud by enhancing and extending the "SafetyVacc" application.

This application functions as an online platform aggregating verified, up-to-date knowledge about online scams, while also providing citizens with step-by-step guidelines for actions to be taken before, during, and after victimization. Importantly, it incorporates verified contact channels with relevant authorities such as the Anti-Online Scam Operation Center (AOC), financial institutions, and local police stations, ensuring that users avoid repeated victimization through fraudulent or unofficial sources. Moreover, the system promotes integration among state agencies, community networks, and evidence management stakeholders, thereby reinforcing collaborative responses to cyber-enabled crimes.

The extension of SafetyVacc represents a significant innovation in crime prevention. Originally developed as a Line Official Account and web-based application offering basic information on health and online risks, the enhanced version incorporates new modules, namely the Crime Pattern, Post-Incident Guidelines, and Agency Information. These additions reflect the application of criminological knowledge—particularly crime pattern analysis—to transform offender behavior and modus operandi into community learning tools. The design allows users to prepare systematically across all stages of victimization and has further potential for capacity-building and community-based crime prevention training.

In comparison with other platforms such as "Cyber Check," developed by the Cyber Crime Investigation Bureau (CCIB), and "Whoscall," which focuses on caller identification and blocking, the enhanced SafetyVacc demonstrates an advantage as a one-stop service platform. Unlike these single-function tools, SafetyVacc integrates fraud awareness, reporting, victim response protocols, and official contact points in a unified interface. Its design emphasizes accessibility, with simple navigation and continuous updates, making it suitable even for populations with limited technological literacy, such as the elderly.

Evaluation results further emphasize the application's practicality: despite minor variations across content, design, and usability scores, participants confirmed that the tool provides comprehensive, reliable, and user-centered information. This reflects a key design principle of crime prevention technology: tools must "understand the user's context" to be effective, particularly for ordinary citizens who face cyber threats in everyday life but may lack advanced digital literacy. Incorporating crime patterns ("modus operandi") into the platform further

strengthens users' ability to anticipate emerging threats, reducing susceptibility to repeat victimization.

These findings align with prior studies. Ounphatthanasilp et al. (2024) revealed that risky behaviors in online financial transactions among elderly populations are directly related to risk perception and digital literacy, reinforcing the importance of systematic fraud-prevention education. Similarly, Lertsatitpirote and Kanyajit (2023) found that victims of online scams were often characterized by inexperience, excessive optimism, and greed, with common fraud typologies including online sales scams, account hacking for financial gain, romance scams, and financial investment fraud. The present study's integration of these typologies within the Crime Pattern module further validates the necessity of equipping users with scenario-specific preventive guidelines.

7. Recommendations

Policy Recommendations

1. Royal Thai Police (RTP).

The Royal Thai Police should strengthen concrete collaboration and coordination channels with local administrative organizations (LAOs), given their proximity to communities and direct responsibility for citizen safety and quality of life. This collaboration should include the establishment of two-way communication systems through the online fraud prevention application, enabling citizens to easily, conveniently, and rapidly access reliable information. Such a system would foster resilience and build strong community networks against evolving methods, forms, and stages of cyber fraud. In this process, the RTP acts as the key provider of information, while LAOs serve as intermediaries for disseminating knowledge to the public, thereby ensuring that technology is fully leveraged in crime prevention.

2. Local Administrative Organization Executives.

LAO executives should prioritize their role as mediators in disseminating knowledge, preventive practices, and procedural guidelines related to online fraud across the entire fraud lifecycle through the application. Budgetary resources should be allocated to continuously enhance public technological literacy and cyber risk awareness. This would mitigate community leaders' limitations in digital knowledge, address technological disparities, and reduce inequalities in access to digital resources and devices.

3. Capacity Building at the Community Level.

LAO executives should assign responsibility to relevant local departments for directly developing and conducting training programs on the online fraud prevention application. This will empower local leaders and community networks to act as effective intermediaries between government agencies and citizens. Well-trained community networks can serve as the frontline for disseminating accurate information and raising alerts, supported by adequate budget allocations to modernize the application and extend its usability across broader geographical areas.

Practical Recommendations

1. Technology-Mediated Coordination.

Both the Royal Thai Police and LAOs should establish intermediary systems or employ technological tools to enhance coordination for maximum public benefit. Given that the fraud prevention application is compatible with both iOS and Android systems, it can serve as an effective communication tool for delivering verified information, coordinating responses during online fraud incidents, and facilitating user-friendly channels for reporting and information sharing within communities.

2. Integration with Community Policing.

The online fraud prevention application should be integrated into community policing initiatives, thereby strengthening local resilience against cyber fraud. Furthermore, the application can provide actionable leads to patrol units and operational task forces, while also facilitating coordination with relevant agencies. This model can be extended to provincial, regional, and national levels, allowing a holistic and scalable approach to online fraud prevention.

3. Monitoring and Evaluation.

LAO executives should establish clear accountability structures and assign roles for monitoring and evaluating the effectiveness of the fraud prevention application. Such evaluation ensures that citizens derive maximum benefit, reduces risks of victimization, and communicates the application's significance. Public communication should leverage existing LAO channels—such as monthly meetings with community leaders, digital media platforms, and local outreach networks—to expand awareness from the community level to broader administrative scales.

8. References

- Clarke, R. V. (1997). *Situational crime prevention: Successful case studies*. Harrow and Heston.
- Kao, Y., Abraham, A., & Snášel, V. (2012). Fast failure recovery for distributed applications using fine-grained checkpointing. In *Proceedings of the 2012 International Conference on Computational Science (ICCS 2012), Procedia Computer Science*, 9, 1210–1219. <https://doi.org/10.1016/j.procs.2012.04.129>
- Kukkudrua, K., Phuangin, J., Klangkarn, S., Inthomya, S., Iamcharat, M., & Phokchaivisith, T. (2023). *Capacity development and seamless safety immunity enhancement: The 3S model for preparing educational personnel of Nonthaburi Provincial Administrative Organization for an aging society*. Royal Thai Police Cadet Academy.
- Royal Thai Government. (2023). *Government of Thailand*. <https://www.thaigov.go.th/news/contents/details/73958>
- Royal Thai Government Gazette. (2023, March 16). *Royal Decree on Measures for the Prevention and Suppression of Technology Crimes, B.E. 2566 (2023)*. Vol. 140, Part 18 K, p. 4.

- Siamsrat Online. (2023, July 16). *Technology Crime Suppression Division assesses cybercrime statistics in the second half of 2023 and recommends six preventive measures*. <https://siamrath.co.th/n/462388>
- Lertsatitpirote, K., & Kanyajit, S. (2023). Causes and types of online fraud victimization in Thailand. *International Journal of Criminal Justice Sciences*, 18(2), 387–400. <https://doi.org/10.5281/zenodo.4756325>
- The Standard. (2024, June 20). *Cyber police recommend the Cyber Check application for screening scam phone numbers*. THE STANDARD. <https://thestandard.co/thai-police-online-cyber-check/>
- Thairath Online. (2022, June 24). *Whoscall: A popular application that saves Thai people from call center scam gangs*. <https://www.thairath.co.th/lifestyle/tech/2424781>
- Ounphatthanasilp, U., Piboonkitkul, S., & Wonghan, P. (2024). Guidelines for preventing risky online financial transaction behaviors among the elderly in Suphan Buri Province. *Journal of Humanities and Social Sciences Dhonburi Rajabhat University*, 8(1), 124–140. https://so02.tci-thaijo.org/index.php/human_dru/article/view/267286