DEVELOPING CAPACITY AND STRENGTHENING SECURITY IMMUNITY: 3S SEAMLESS AGING SOCIETY PREPARATION OF EDUCATION PERSONAL

a Kannika Kukudrua, b Jiraporn Poungin, c Sataporn Klangkan

ABSTRACT

Purpose: The aim of this study was to analyze the capacity and the needs of the security preparation before entering the aging society and to transfer the knowledge in the capacity development and to strengthen the security immunity in all ages.

Theoretical framework: This study integrates theories from sociology, psychology, education, and gerontology to understand the needs of older adults in online security. It uses social learning theory, age-stratification theory, technology acceptance model, community-based participatory research, ecological systems theory, and life course perspective to understand the capacity and needs for security preparation in an aging society and develop effective interventions.

Design/Methodology/approach: This study utilized the qualitative research by focus group and workshop method with the 60 educational personnel those who worked at the school in the Nonthaburi provincial administrative organization (Focus group method), and 95 key informants which were consisted of Chief Executive of the Nonthaburi provincial administrative organization, or the representative of the Nonthaburi provincial administrative organization in the department of the education, the religion and culture, the welfare, and the public health, the school administrators, the officer of the department of older persons, the officer of Department of Social Development and Welfare, the police officer of Technology crime suppression division, the lecturer of the Police nurse and the Royal police cadet academy, the lecturer of the Humanities from the Social faculty, the students of the Royal police cadet academy, the students of the Police nurse (Workshop method). All selected by the purposive sampling, and analyzed with the content analysis.

Findings: It found that the elderly were convinced by the scammers since the elderly were considered to have the financial capacity, some of them were lonely, and had the limitation knowledge in technology even with the education personnel.

Research, Practical & Social Implications: The study explores security vulnerabilities in aging societies, focusing on online scams and digital literacy among older adults. It provides qualitative research insights, offers theoretical advances, and suggests educational interventions to enhance security awareness. The findings also suggest policy recommendations for promoting online safety and digital inclusion among older adults.

a Royal Police Cadet Academy, Nakhon Pathom, Thailand. E-mail: kannika.kukudrua@hotmail.com
Orcid: https://orcid.org/0009-0008-4136-4544
b Royal Police Cadet Academy, Nakhon Pathom, Thailand. E-mail: poungin_j@hotmail.com
Orcid: https://orcid.org/0009-0007-6998-9100
c Police Nursing College, Bangkok, Thailand. E-mail: klangkan_s@hotmail.com
Orcid: https://orcid.org/0009-0000-6701-742X
Originality / value: The value of the study was to have the strength in aging society, the educational personnel needed to prepare for creating the capacity in order to strengthened the security immunity from the danger of the online society which can be concluded into 6 issues 1) Supporting the knowledge and creating the awareness 2) Creating the skill of using the online society 3) Developing the communication channel and the public relation 4) Participating of the community and the relevant organization 5) Creating the capacity of the family and community member, and 6) Developing the organization capacity.

Keywords: security immunity, aging society, educational personal.

Received: 25/12/2023
Accepted: 26/02/2024
DOI: https://doi.org/10.55908/sdgs.v12i3.3444

DESENVOLVER A CAPACIDADE E REFORÇAR A IMUNIDADE DE SEGURANÇA: 3S ENVELHECIMENTO SEM PROBLEMAS SOCIEDADE PREPARAÇÃO DA EDUCAÇÃO PESSOAL

RESUMO

Objetivo: O objetivo deste estudo foi analisar a capacidade e as necessidades da preparação de segurança antes de entrar na sociedade em envelhecimento e transferir o conhecimento no desenvolvimento da capacidade e fortalecer a imunidade de segurança em todas as idades.

Estrutura teórica: Este estudo integra teorias da sociologia, psicologia, educação e gerontologia para entender as necessidades dos idosos em segurança on-line. Ele usa a teoria da aprendizagem social, teoria da estratificação etária, modelo de aceitação tecnológica, pesquisa participativa baseada na comunidade, teoria de sistemas ecológicos e perspectiva de curso de vida para entender a capacidade e as necessidades de preparação para a segurança em uma sociedade envelhecida e desenvolver intervenções eficazes.

Design/Metodologia/Abordagem: Este estudo utilizou a pesquisa qualitativa por grupo de foco e método de workshop com os 60 funcionários educacionais que trabalharam na escola na organização administrativa provincial de Nonthaburi (método do grupo de foco), e 95 informantes-chave que foram constituídos pelo Chefe Executivo da organização administrativa provincial de Nonthaburi, ou o representante da organização administrativa provincial de Nonthaburi no departamento da educação, a religião e cultura, o bem-estar e a saúde pública, os administradores da escola, o oficial do departamento de pessoas mais velhas, o oficial do Departamento de Desenvolvimento Social e Bem-Estar, o oficial de polícia da divisão de supressão de crimes de tecnologia, o professor Professor da enfermeira de polícia e da Academia Real de cadetes de polícia, o professor da Faculdade de Ciências Humanas, os alunos da Academia Real de cadetes de polícia, os alunos da enfermeira de polícia (método Workshop). Todos selecionados pela amostragem intencional e analisados com a análise de conteúdo

Constatações: Constatou-se que os idosos eram convencidos pelos golpistas, pois os idosos eram considerados com capacidade financeira, alguns deles isolados e possuíam a limitação de conhecimento em tecnologia mesmo com o pessoal educacional.

Pesquisa, implicações práticas e sociais: o estudo explora vulnerabilidades de segurança em sociedades em envelhecimento, com foco em golpes on-line e alfabetização digital entre idosos. Ele fornece insights de pesquisa qualitativa, oferece avanços teóricos e sugere intervenções educacionais para aumentar a conscientização sobre segurança. Os resultados também sugerem recomendações políticas para promover a segurança on-line e a inclusão digital entre idosos.
Originalidade / valor: O valor do estudo foi ter a força na sociedade em envelhecimento, o pessoal educacional necessário para se preparar para a criação da capacidade, a fim de reforçar a imunidade de segurança do perigo da sociedade on-line, que pode ser concluída em 6 questões 1) Apoiar o conhecimento e criar a conscientização 2) Criar a habilidade de usar a sociedade on-line 3) Desenvolver o canal de comunicação e a relação pública 4) Participar da comunidade e da organização relevante 5) Criar a capacidade da família e do membro da comunidade, e 6) Desenvolver a capacidade de organização.

Palavras-chave: imunidade de segurança, envelhecimento da sociedade, educação pessoal.

DESARROLLO DE LA CAPACIDAD Y FORTALECIMIENTO DE LA INMUNIDAD DE SEGURIDAD: 3S SEAMLESS AGING SOCIETY PREPARACIÓN DE LA EDUCACIÓN PERSONAL

RESUMEN

Propósito: El objetivo de este estudio fue analizar la capacidad y las necesidades de la preparación de seguridad antes de ingresar a la sociedad de envejecimiento y transferir el conocimiento en el desarrollo de capacidades y fortalecer la inmunidad de seguridad en todas las edades.

Marco teórico: Este estudio integra teorías de la sociología, la psicología, la educación y la gerontología para comprender las necesidades de los adultos mayores en materia de seguridad en línea. Utiliza la teoría del aprendizaje social, la teoría de la estratificación por edades, el modelo de aceptación de la tecnología, la investigación participativa basada en la comunidad, la teoría de los sistemas ecológicos y la perspectiva del curso de vida para comprender la capacidad y las necesidades de preparación en materia de seguridad en una sociedad que envejece y desarrollar intervenciones eficaces.

Diseño/Metodología/enfoque: Este estudio utilizó la investigación cualitativa por grupo focal y método de taller con los 60 miembros del personal educativo que trabajaron en la escuela en la organización administrativa provincial de Nonthaburi (método de grupo focal), y 95 informantes clave que estaban formados por el Jefe Ejecutivo de la organización administrativa provincial de Nonthaburi, o el representante de la organización administrativa provincial de Nonthaburi en el departamento de educación, religión y cultura, bienestar y salud pública, los administradores de la escuela, el oficial del departamento de personas mayores, el oficial del Departamento de Desarrollo Social y Bienestar, el oficial de policía de la división de supresión de delitos de tecnología, el profesor de la enfermera de la Policía y la Real academia de cadetes de policía, el profesor de Humanidades de la facultad social, los estudiantes de la Real policía my, los estudiantes de la enfermera de la Policía (método Workshop). Todos seleccionados por el muestreo intencional, y analizados con el análisis de contenido.

Hallazgos: Se encontró que los ancianos fueron convencidos por los estafadores ya que se consideraba que los ancianos tenían la capacidad financiera, algunos de ellos estaban solos, y tenían la limitación de conocimientos en tecnología incluso con el personal educativo.

Investigación, implicaciones prácticas y sociales: El estudio explora las vulnerabilidades de seguridad en las sociedades que envejecen, centrándose en las estafas en línea y la alfabetización digital entre los adultos mayores. Proporciona conocimientos de investigación cualitativa, ofrece avances teóricos y sugiere intervenciones educativas para mejorar la conciencia de seguridad. Los resultados también sugieren recomendaciones de políticas para promover la seguridad en línea y la inclusión digital entre los adultos mayores.

Originalidad / valor: El valor del estudio fue tener la fuerza en la sociedad que envejece, el personal educativo necesario para prepararse para crear la capacidad con el fin de fortalecer la inmunidad de seguridad frente al peligro de la sociedad en línea que se puede concluir en 6 temas 1) Apoyar el conocimiento y crear la conciencia 2) Crear la habilidad de usar la sociedad en línea 3) Desarrollar el canal de comunicación y la relación pública 4) Participar de la
comunidad y la organización pertinente 5) Crear la capacidad de la familia y el miembro de la comunidad, y 6) Desarrollar la capacidad de organización.

Palabras clave: inmunidad de seguridad, envejecimiento de la sociedad, personal educativo.

1 INTRODUCTION

The scammer targeted to the elderly persons have become so common issue that we hear from the news daily. In 2020, the elderly lost nearly 4.1 billion dollars to the scammer, especially from the internet. Scammers typically target the elderly who are living alone, grieving a spouse, suffering from the disabilities, or the illness. The reason of the elderly being targeted was the elderly tend to be trusting, polite, and kind. They may owned their home and had savings, which made them especially appealing to the scammers. Sadly, many elderly didn’t report the scammer committed against them because they were either embarrassed or worried that family members would lose the confidence in their ability to manage their finances. The most common scams targeting to elderly by using the technology. As the technology changed rapidly, the elderly were at risk of being targeted now more than ever. The development of science and technology has had a real impact on human relations (Kartika et al., 2023). These were the example of the scam methods. 1) Romance Schemes, Online dating was the new norm, even with the elderly, which meant the scammers targeted to the lonely widows. These romance scammers would create the elaborate fake profiles on dating sites and social media, and used them to exploit the elderly. The scammer will often pretended to be a pity person, and stayed in the overseas, and needed the money for Visa or travel expenses. Sometimes, they requested the money for the emergency medical service with the promise to meet once they’re medically well enough. 2) Phishing Emails or Texts, phishing emails and texts look like they came from a trusted company, such as a bank or an online store. These emails may request the personal information, prompt you to follow a log-in link to verify your account, or asked you to update your payment information. Providing them with the above-mentioned allows them to steal your personal and financial information (Senior Services of America, 2023). Elder fraud was on the rise and had an alarming prevalence, and devastated the impact on victims and their families. The Federal Bureau of Investigation’s Internet Crime Complaint Center (IC3) released its annual report on elder fraud in 2022. The report provided the insights into the most common types of fraud
reported: Call Center Fraud, Investment Scams, Lottery/Sweepstakes/Inheritance Fraud, Non-Delivery Scams, Extortion, and Romance Scams: Confidence/Romance Scams: $419 million were lost in this category which includes romance and grandparent scams (Korzun, 2023). Over the past five years, Americans have reported losing $1.3 billion to online dating scams, according to the Federal Trade Commission. (Sathya, A. ., & Velmurugan, V. P. . 2022) The most recent FTC data showed such scams were up nearly 80 percent since 2020, with approximately $547 million lost to swindlers in 2021 alone. Known as “Romance scams,” these were the largest category of fraud now tracked by the FTC. And it wasn’t always a victim’s money. A clever scammer can not only leave their mark broke and broken-hearted, but also facing money laundering charges. Romance scams tend to target the elderly who were recently widowed and have resources (LEXISNEXIS, 2022). For example, an elderly woman from Indianapolis said that she lost $98,000 to a romance scammer. The victim was using a dating website after losing her husband a few years ago. She met someone on the site who claimed to be 20 years her junior. When asked if the age gap would be a problem, the scammer replied with, “Age was just a number.” The scammer then convinced the victim to move their conversations away from the dating site, and used the text messaging instead. The scammer claimed to own a construction company in Montreal, Canada, and asked for money to support his business (Collier, 2023).

In the Asia context, the 45 percent of people surveyed in the Philippines and Southeast Asia (SEA) lost their money to online love scams, according to a recent Kaspersky study. The oldest and loneliest group lost the most - over half a million pesos from the online romance fraud. Specifically, the two oldest generations - Baby Boomers (born 1946 to 1964), and the Silent Generation (born 1928 to 1945) - accounted for the bulk, or 33 percent, of those who fall prey to love scammers. Sadly, two in five in the most senior age group admitted to being defrauded by as much as P255,000 to P510,000 ($5,000-10,000) from love scams online. The rest, 22 percent of the victims, were fleeced for less than P5,100 ($100). (Ahmed , H. A., 2023) Romance scams surged when the pandemic hit. With limited physical movements, the internet, particularly social media platforms, provided a critical connection for people.

More than half (53 percent) of social media users around the world used the social networks more during the local and national lockdowns than before, according to
Kaspersky’s findings. Furthermore, 18 percent of the 1,007 adults surveyed to represent Southeast Asia (SEA) used social media mainly to find romance and the majority (76 percent) confirmed that the social media provided them with a vital connection during the global health emergency. Close to a quarter (24 percent) of the respondents from SEA said that they have formed the real-life in-person friendships with people met initially on social media while another 18 percent admitted they dated someone they’ve met on these platforms. Cybercriminals also moved quickly from dating sites or apps into the private channels. They asked many questions about their victims to manipulate them more easily but the scammers’ own stories are often inconsistent as they operated in teams, with different people hiding behind one identity. Also, scammers didn’t have a digital footprint. While some people didn’t use the social media, and try to minimize the amount of the personal information about them on the internet, it can be suspicious if you can’t find any trace of a person online. Scammers avoid using the video calls or face-to-face meetings as well. People who were scammed generally report that the other person made the constant excuses to avoid going on camera because they didn’t look like the person in their profile picture. They also wanted to avoid being identified to prevent being tracked down afterward. Cybercriminals requested for money based on the personal hardship, such as sick relatives or a failed business (Abadilla, 2022). In Japan, elderly woman suspected of falling for ‘Out of this world’ love scam. She believed he loved her. And that he was a Russian cosmonaut as he claimed. And that he actually needed money to return to Earth from the International Space Station. Now she lost ¥4.4 million. Police said Friday it suspected that a 65-year-old woman has fallen to the scammers after transferring that amount in a case it was investigated as an international romance scam, in which a fraudster swindles money from a person by establishing a deceitful relationship. According to the Higashi-Omi Police Station in Shiga Prefecture, the Higashi-Omi woman met the self-proclaimed Russian man via Instagram on June 28. He told her that he worked on the International Space Station. The alleged cosmonaut started sending her messages on the Line message app, telling her that he wanted to start a new life in Japan and professing his love for her. In one message, he said that saying it 1,000 times would not be enough, but he will continue to say he loves her. The person subsequently requested money needed for landing fees for a rocket’s return to Earth and other purposes. The woman believed the story and made five wire transfers totalling ¥4.4 million between Aug. 19 and Sept. 5. However, as the requests continued, she became
suspicious and reported the case to the police. “As he brought up the name of existing organizations like NASA [The U.S. National Aeronautics and Space Administration] and JAXA [The Japan Aerospace Exploration Agency], I believed him,” the woman was quoted as telling the police (The Yomiuri Shimbun, 2022).

In Thailand, Thai police said there were over 400 reports of the romance scams in each month. Royal Thai Police (RTP) said that 403 cases that were reported in January 2023 related to the love frauds, resulting in substantial financial loss for over 190 million baht. RTP was trying to promote the public to be aware of the issue of romance scams which mainly targeting women in their 40s. According to RTP spokesperson Noppawan Panya, said that most of the victims being deceived into transferring money to scammers, and being lured into a fraudulent investment. The strategies that the scammers used included: Creating fake hope or sympathy, luring victims into a fake investment, tricking victims into clicking a link or downloading an app that gave the scammer remote access to the victim’s smartphone, including the Blackmailing. The police warned the public to be cautious when encountering the strangers on the social media, advising them to never click links, download apps, or send photos to strangers as they may be scammers. Usually, the fraudsters create a fake account with an attractive profile picture, and use excuses such as medical bills, travel expenses, or gift-sending fees to trick their victims. In response to this alarming issue, Prime Minister has ordered the Thai Royal Police to crack down on cybercrime, including romance scams, under the campaign “Stop Walk Talk.” If one feels or is uncertain that they are being scammed, they are urged to call the 1441 hotline or 08-1866-300 immediately. The public can also report such incidents online via the Thai Police Online website, The Pattaya News reported. Most victims of romance scams in Thailand are reported to be women in their 40s. Middle-aged women are the main targets of criminal gangs who prey on those who have taken the questionable step of seeking true love online (Abhasakun, 2023). Thai women over 40 are the key target for online African scam gangs posing as wealthy western lovers and offering promises of a better life. In the last decade, the numbers of middle class and well-off Thai women in this age group has also shot up as Thai women, following an Asian and indeed worldwide trend, in pursuing careers are not yet content to marry Thai men with less income or status. Then there is the unique Thai susceptibility to gambling which makes the Thai lotteries the national past time and it is easy to see why many unfortunate women are snared by the African criminal gangs. The problem may be easing somewhat today in Thailand as
the word gets out and the Thai police force targeting online crime, continues to publicize and provide comprehensive information on each series of arrests including the background and organisation structures of the actors and the gangs involved, to the public (Boonkong & O’Connor, 2019).

Although anyone can be targeted by scammers, there were several factors that put older women at high risk. In general, women live six to eight years longer than men, according to the World Health Organization. That means as more women lived to old age, more women than men were in the target demographic for elder fraud. As women outlive men, they often live alone and have no companion with whom to discuss a fraudster's request for money. Living alone can also lead to loneliness, and fraudsters prey on that isolation and emotion. Ambrose describes how one client was targeted by an IRS scam:

Every morning for months, she got a phone call from the scammer, checking on her and making sure she took her pills, Ambrose said. When the scam came to light, the client said she considered the caller to be like a son to her. Additionally, women were more likely to serve as caregivers, a role that can often be impacted by scams. “Sometimes the stress and isolation of caregiving can make them more Association (RBC Wealth Management, 2023).

Most of the previous papers focused on many areas in this issue, for example, the first one, Coluccia et al. studies in the title of “Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review”. This paper presents a scoping review of the quantitative and qualitative evidence on this issue, focusing on epidemiological aspects, relational dynamics, and the psychological characteristics of victims and scammers. Results showed that sixty-three percent of social media users and 3% of the general population report having been a victim at least once. Some psychological variables appear to be associated with the risk of being scammed, such as female gender, middle-age, higher levels of neuroticism, tendencies to the romantic idealization of affective relations, sensation seeking, impulsiveness and susceptibility to addiction (Coluccia et al. 2020). The second one, Cross and Layt studies in the title of “I Suspect That the Pictures Are Stolen”: Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities”. This article examines how individuals responded to suspicions of inauthentic identities to a person they were communicating with online. The article explores the implications for this victim-based detection strategy. In doing this, it argues that while effective for
romance fraud victims, responses can further exacerbate the ongoing harms experienced by those whose identities have been compromised by romance fraud offenders (Cross& Layt, 2022). The third one, Buil-Gil and Zeng studies in the title of “Meeting you was a fake: Investigating the increase in romance fraud during COVID-19”. This paper analyses changes in romance fraud, loneliness, and internet use during the pandemic. The analysis shows that cyber-enabled romance fraud experienced a large increase after April 2020 which is greatly above any expected crime variation considering known pre-COVID trends (Buil-Gil & Zeng, 2022). The last one, DeLiema studies in the title of “Elder Fraud and Financial Exploitation: Application of Routine Activity Theory”. This study analyzes differences between fraud and financial exploitation victims and tests routine activity theory as a contextual model for victimization. Routine activity theory predicts that criminal opportunities arise when a motivated offender and suitable target meet in the absence of capable guardians. Results showed that fraud and financial exploitation victims performed poorly on tests of cognitive functioning and financial decision making administered by a forensic neuropsychologist following the allegations. Based on retrospective record review, there were few significant differences in physical health and cognitive functioning at the time victims’ assets were taken, although their social contexts were different. Significantly more fraud victims were childless compared with financial exploitation victims. Fraud perpetrators took advantage of elders when they had no trustworthy friends or relatives to (DeLiema, 2018).

The current study attempts to fill this gap in the literature by focusing on firstly, the capacity and the needs of the security preparation before entering the aging society, and secondly, the knowledge in the capacity development and to strengthen the security immunity in all ages

1. To analyze the capacity and the needs of the security preparation before entering the aging society
2. To transfer the knowledge in the capacity development and to strengthen the security immunity in all ages

2 LITERATURE REVIEW

The literature review for this study would explore existing research and scholarly works related to several key areas:
Online Security and Aging Population: This section would examine studies that highlight the vulnerabilities of older adults to online scams and cybercrimes. It would explore factors contributing to their susceptibility, such as limited digital literacy, cognitive decline, and social isolation. Additionally, it would review interventions and strategies aimed at enhancing online security awareness and skills among older adults.

Role of Educational Personnel in Security Preparedness: This section would focus on the role of educational personnel, including teachers, administrators, and support staff, in promoting online safety within educational settings and the wider community. It would investigate their attitudes, knowledge, and practices related to cybersecurity education and their effectiveness in imparting digital literacy skills to both students and older adults.

Community-Based Approaches to Security Immunity: Here, the review would explore community-based initiatives and partnerships aimed at strengthening security resilience across different age groups. It would examine successful models of collaboration between educational institutions, government agencies, non-profit organizations, and community groups in addressing online security challenges and promoting digital inclusion among older adults.

Theoretical Frameworks and Conceptual Models: This section would discuss theoretical frameworks and conceptual models relevant to understanding the intersection of aging, technology adoption, and security resilience. It would explore theories such as social learning theory, technology acceptance model, and ecological systems theory, as well as their applicability to designing interventions and strategies for enhancing security immunity in an aging society.

Policy and Practice Implications: Finally, the literature review would discuss policy initiatives, guidelines, and best practices aimed at safeguarding older adults against online threats and promoting their digital well-being. It would examine existing policies related to cybersecurity education, consumer protection, age-friendly technology design, and elder abuse prevention, highlighting areas for improvement and future directions in policy development and implementation.

Overall, the literature review would provide a comprehensive overview of the current state of knowledge on security preparedness in an aging society, identify gaps in the literature, and set the stage for the empirical investigation conducted in the study.
3 METHODS

Research Method. This study utilized the qualitative research by focus group and workshop method for analyzing the capacity and the needs of the security preparation before entering the aging society, and for transferring the knowledge in the capacity development and to strengthen the security immunity in all ages respectively.

Participants. 155 key informants were used in this research. In the initial step, the 60 educational personnel those who worked at the school in the Nonthaburi provincial administrative organization (Focus group method), and 95 key informants which were consisted of Chief Executive of the Nonthaburi provincial administrative organization, or the representative of the Nonthaburi provincial administrative organization in the department of the education, the religion and culture, the welfare, and the public health, the school administrators, the officer of the department of older persons, the officer of Department of Social Development and Welfare, the police officer of Technology crime suppression division, the lecturer of the Police nurse and the Royal police cadet academy, the lecturer of the Humanities from the Social faculty, the students of the Royal police cadet academy, the students of the Police nurse (Workshop method). All selected by the purposive sampling, and this research also was approved the ethics by the office of the committee for research ethics Royal Police Cadet Academy

Instrument. The researchers developed the research questions based on the previous literature. The focus group method had 9 indexes which were relevant to the capacity and the needs of the security preparation before entering the aging society, and another workshop method had two issues which were relevant to transfer the knowledge in the capacity development and to strengthen the security immunity in all ages.

Analysis. The content analysis was used in this research

4 RESULT AND DISCUSSION

It can be concluded into two parts which were as follows;

Part 1. The result of analyzing the capacity and the needs in the security preparation before entering the aging society in the aspect of the online society and the health
The result found the three issues which were consisted of the problem condition or the danger that might affected to the elderly, the capacity, and the needs of the security preparation.

First issue: The problem condition or the danger that might affected to the elderly

1. The online society aspect was more dangerous towards the elderly than the other days in the past. Most of the elderly were convinced by the scammers since the elderly were considered to have the financial capacity, but they had the limitation knowledge in technology which related to one of the key informants that said that “The more advance in technology, the more criminal in technology. Especially, the elderly was easy to convince.” It is in line of Haase. Analysis revealed that 55.9% of respondents reported that they adopted the new technology since the beginning of the pandemic. Older adults reported the following key barriers to using technology: 1) a lack of access (including finance-, knowledge-, and age-related issues) and 2) a lack of interest (including a preference for telephones and a general lack of interest in computers) (Haase et al., 2021).

2. The health aspect can be concluded into 4 issues which were as follows 1) Chronic disease such as Diabetes, High blood pressure, Heart disease and stroke, and so on. 2) The deterioration of the various body systems, for example Dementia, Confusion, Alzheimer's disease, and the vision problem, and so on. 3) Office Syndrome, and 4) The mental problem which related to one of the key informants that said that “Most of the elderly always stay at home, and have lot of free times to sit in front of the television.” It is in line of Shao et al. The results revealed that factors shown to influence fraud victimization among older adults include cognitive decline, emotional regulation and motivational changes, their overly trusting nature, psychological vulnerability, social isolation, risk-taking, and a lack of knowledge and information regarding fraud prevention. Based on a review of the literature, future research can benefit from constructing a comprehensive fraud victimization theory, improving research methods, extending existing research, exploring physiological mechanisms of elderly fraud, and strengthening prevention and intervention efforts (Shao et al., 2019).

Second issue: The capacity in the security aspect preparation
1. The online society aspect found that most of the education personnel had the experiences of falling to the crime victim from using the online society both direct and indirect ways which related to one of the key informants that said that “For those elderly who had the typing skill, and loved to communicate to their friends used to be convinced by the online advertising, and believed. Therefore, the education personnel had the capacity in taking care of oneself and their family in using the online society which related to one of the key informants that said that “We have the experience and the knowledge if how we not going to be the victim of the crimes by deleting the link, or the suspected application, monitoring the reliability of the product page including with separating the saving account from the payment account”.

2. The health aspect found that the education personnel was the person who teach the knowledge, so they always need to study which related to one of the key informants that said that “Even we have the health knowledge, but according to our task that we need to prepare the teaching staffs, sometime we faced to the health problems.” Another key informants said that “In the present days, there was a wide variety and differences in health education media which presented. Sometimes there was the exaggeration in advertising causing the confusion about the information. Therefore, it was one reason why educational personnel needed to prepare for the health safety”.

**Third issue: The needs of the security preparation**

1. The online society aspect found that the educational personnel needed to prepare for creating the capacity in order to strengthened the immunity from the danger of the online society which can be concluded into 6 issues 1) Supporting the knowledge and creating the awareness 2) Creating the skill of using the online society 3) Developing the communication channel and the public relation 4) Participating of the community and the relevant organization 5) Creating the capacity of the family and community member, and 6) Developing the organization capacity which related to one of the key informants that said that “Creating the community leader to be an influencer will be the great impact for the community.” It is in line of Islam et al. The results showed that the traditional leadership qualities had a significant correlation with the development of social cohesion (Islam et al., 2020).
2. The health aspect found that the needs of the education personnel in preparing to the aging society were comprised of the 8 issues: 1) The annual health check-ups 2) Approach the correct and update data 3) Creating the health literacy 4) Creating the good attitude in the health behaviour promotion 5) Having the community channel for collaboration 6) Launching the organization’s concrete promotion policy 7) Collaborating with all partners both the public and the private section, and 8) Using the application for the health screening including with the call center and the emergency hot line which related to one of the key informants that said that “In the stage of the preparation, creating the health literacy for the elderly was very important because they were in the risky group of facing the health problem. It is in line of Ghorbanian Zolbin et al. The purpose of this paper is to assess the relationship between elderly people's health literacy skills and those people's decision to make use of digital health service platforms. The results show that health intervention programmes help to enhance health literacy skills of elderly people. The finding help them to understand that with digital health platforms, elderly people have quicker access to health services, improving the quality of care provided to them (Ghorbanian Zolbin et al., 2022).

Part 2: The result of the knowledge transfer in the capacity development and to strengthened the security immunity in all ages

The result found the two issues which were consisted of the security knowledge series in the aspect of the online society and the health aspect and knowledge transfer in the capacity development and to strengthened the security immunity in all ages

1. The security knowledge series in the aspect of the online society and the health aspect

1.1 The security knowledge series were consisted of the danger from the online society, the risky behavior of falling the online society victim, the prevention of the danger from the online society, the skill of using the online society, the awareness of the online society, the crime warning website, and the emergency hotline which related to one of the key informants that said that “The public Wi-Fi was very dangerous, and you have got to be extra carefully before you doing the financial business through online.” It is in line of Maimon et al. It was found that accessing public Wi-Fi networks can be as dangerous as it is convenient. People who access a public Wi-Fi network should engage in self-protective
behaviours to keep their data safe from malicious actors on the same network as well as persons looking over their shoulder (Maimon et al., 2020).

1.2 The health knowledge series which was consisted of 1) Chronic disease such as Diabetes, High blood pressure, Heart disease and stroke, and so on. 2) The deterioration of the various body systems, for example Dementia, Confusion, Alzheimer's disease, and the vision problem, and so on. 3) Office Syndrome, and 4) The depression including with the manual of the guideline of promoting the health / the elderly care / the elderly assessment / the hospital information which related to one of the key informants that said that “Elders should have the knowledge of Chronic disease. That’s why they should avoid having the alcohol or junk foods.” It is in line of Song et al. The older people's chronic diseases knowledge should be improved and health education programs should target males, older people with lower educational level, having no health insurance, having no family history of chronic diseases, participating in no societies, and less frequently gathering with friends/relatives. Also, lower level medical facilities should improve their skills of health education (Song et al., 2013).

2. The knowledge transfer in the capacity development and to strengthened the security immunity in all age

It can be concluded into two issues which were as follows;

1) In the classroom of the Royal police cadet academy and the police nurse students.
2) In the workshop for the officers, the school administrators of the Provincial administrative organization, the officer of the department of older persons, the police officer at Technology crime suppression division, the lecturer of the Police nurse and the Royal police cadet academy.

The policy recommendation

1. The relevant organizations in the government should have the operational plan for focusing and driving the personnel potential in the issue of the online social, and the health in order to promote the personnel and the local people quality of life in the area.

2. The relevant organizations in the government should create the public relation plan for approaching the target group for creating the awareness of the importance including with learning how to use the safety application.
3. The relevant organizations in the government should allocate the budget for supporting and linking the organization data bases between the internal and external organizations for strengthening the networking.

4. The relevant organizations in the government should give the priority to the expanding to the application development model in every elderly categories.

5. The relevant organizations in the government should sign the MOU in elaborating the application development guideline for developing the content and proposing the data for the most benefit of the elderly.

5 CONCLUSION

Using the public relation and setting the security training for the public health volunteer, or any people who are interested in taking the elders for getting ready to enter the aging society, and also updating the online society and the health data in the channel of Facebook, Line Official would be the most benefit for the aging users.

REFERENCES


