Akademika 94(3), 2024: 90-107
https://doi.org/10.17576/akad-2024-9403-06

An Analysis of the Deployment of Synergistic Cyber Security Awareness Model for the Elderly (SCSAM-Elderly) in Malaysia

Analisis Penggunaan Model Sinergistik Kesedaran Keselamatan Siber untuk Warga Emas (SCSAM-Elderly) di Malaysia

NURUL ALIEYAH AZAM, ALYA GEOGIANA BUJA*, RABIAH AHMAD,
SHEKH FAISAL ABDUL LATIP & NOR MASRI SAHRI

ABSTRACT

This study explores the deployment analysis of the Synergistic Cyber Security Awareness Model for the Elderly (SCSAM-Elderly) in Malaysia. The incidence of cyber security events has been steadily increasing, particularly affecting the elderly demographic. The SCSAM-Elderly has been developed to address persistent challenges posed by cybercrimes, such as phishing, romance scams, and identity theft, with the primary objective of educating and heightening awareness among the elderly. Designed to be user-friendly and tailored for the elderly population, the SCSAM-Elderly aims to enhance their awareness. The study's objective is to analyze the pre-survey and post-survey data collected from elderly individuals in Malaysia using SPSS to confirm and validate the effectiveness of the SCSAM-Elderly model. Surveys were distributed to 50 elderly individuals in Melaka, and the data were analyzed using SPSS Version 27.0. This study employed a paired sample t-test, a statistical method used to determine if there is a significant difference between the average scores of two related groups. In this study, the two groups are the pre-survey and post-survey scores from the same participants. The results indicated that the SCSAM-Elderly model showed a significant increase in awareness after the implementation of cybersecurity training compared to before the training. The findings indicate that elderly individuals who underwent cyber security awareness training using this model demonstrated an improved ability to detect and counteract the impacts of cybercrimes. The novelty of this study lies in being the first cybersecurity awareness model focusing on the elderly with less technicality.

Keywords: awareness; cyber security; elderly; SCSAM-Elderly; SPSS

ABSTRAK

Kajian ini meneroka analisis pelaksanaan Model Sinergistik Kesedaran Keselamatan Siber untuk Warga Emas (SCSAM-Elderly) di Malaysia. Kejadian berkaitan keselamatan siber semakin meningkat, terutama sekali memberi kesan kepada golongan warga emas. SCSAM-Elderly dibangunkan untuk menangani cabaran berterusan yang ditimbulkan oleh jenayah siber seperti pancingan data, penipuan cinta, dan kecurian identiti, dengan matlamat utama untuk mendidik dan meningkatkan kesedaran dalam kalangan warga emas. Direka agar mesra pengguna dan disesuaikan untuk populasi warga emas, SCSAM-Elderly bertujuan untuk meningkatkan tahap kesedaran mereka. Objektif kajian ini adalah untuk menganalisis data pra-tinjauan dan pasca-tinjauan yang dikumpul daripada individu warga emas di Malaysia dengan menggunakan SPSS bagi mengesahkan dan mengesahkan keberkesanan model SCSAM-Elderly. Tinjauan telah diedarkan kepada 50 orang warga emas di Melaka, dan data dianalisis menggunakan SPSS Versi 27.0. Kajian ini menggunakan ujian sampel t-test berpasangan, kaedah statistik yang digunakan untuk menentukan sama ada terdapat perbezaan yang signifikan antara skor purata dua kumpulan yang berkaitan. Dalam kajian ini, dua kumpulan tersebut adalah skor pra-tinjauan dan pasca-tinjauan daripada peserta yang sama. Keputusan menunjukkan bahawa model SCSAM-Elderly menunjukkan peningkatan yang ketara dalam tahap kesedaran selepas pelaksanaan latihan keselamatan siber berbanding sebelum latihan. Penemuan ini menunjukkan bahawa individu warga emas yang mengikuti latihan kesedaran keselamatan siber menggunakan model ini menunjukkan peningkatan keupayaan untuk mengesan dan menangani kesan jenayah siber. Keunikan kajian ini terletak pada hakikat bahawa ia merupakan model kesedaran keselamatan siber pertama yang memberi tumpuan kepada warga emas dengan pendekatan yang kurang teknikal.

Kata kunci: kesedaran; keselamatan siber; warga emas; SCSAM-Elderly; SPSS

INTRODUCTION

The elderly represent one of the fastest-growing segments of Internet users; however, studies indicate that many enter the digital realm without the requisite knowledge to defend themselves against cyber-attacks, rendering them highly susceptible. Financial fraud targeting the elderly is prevalent in both urban and rural areas, and it is crucial to note that such cases are significantly under-reported in Malaysia, likely due to emotional stress hindering reporting efforts. The elderly often fall victim to fraudulent activities, given the perception of their substantial retirement savings. According to Jesrina Ann and Chong Wei (2023), since August 2022, numerous instances have been recorded wherein the elderly suffered substantial financial losses, ranging from RM100,000 to RM1.8 million, due to various scam methods.

Addressing this issue, governments and affiliated organizations have implemented various cyber security awareness models to reduce the vulnerability of older individuals to cybercriminals. However, most existing models are either overly complex or not well-suited for elderly individuals due to their limitations and disabilities. In response, the proposed model, the New Synergistic Cyber Security Awareness Model for the Elderly (SCSAM-Elderly), has been developed. This model consists of three phases: theory, practice, and analysis, designed for ease of implementation (Azam et al. 2022). Notably, the SCSAM-Elderly model is tailored for the elderly, with no technical steps involved. The model has launched a website as a platform to provide cyber security information to the elderly (Azam et al. 2022).

The objective is to analyze the pre-survey and post-survey data collected from elderly individuals in Malaysia using SPSS to confirm and validate the effectiveness of the SCSAM-Elderly model. Additionally, this research aims to unveil the efficacy of a novel, collaborative cybersecurity model, enhancing the elderly population's understanding of recurrent cyber-attack issues and fostering a cyber-secure environment to mitigate their vulnerability as potential victims.

LITERATURE REVIEW

CYBER SECURITY AND THE ELDERLY

Cybersecurity has become a global concern due to the rapid advancement of technology and widespread Internet usage (Muhammad et al. 2024). Protecting personal information is crucial, given the growing frequency of cybercrimes. Various organizations and governments have implemented preventive measures to address these issues (Mahajan & Kaur 2021). "Cybersecurity awareness" refers to an individual's understanding of online safety, including knowledge of current security threats and best practices, as well as the risks posed by unsafe behaviors like clicking on malicious links. Education is key, especially as users are consistently exposed to cyber threats regardless of time or place.

The elderly are particularly vulnerable to cybercrimes, especially due to their retirement savings, making them frequent targets (Casey Crane 2019). In Malaysia, the elderly population has risen to 3.8 million in 2023, which increases concerns about their vulnerability to cybercrimes, particularly since many lack cybersecurity awareness (Department of Statistics Malaysia 2023).

This study focuses on elderly individuals aged 60 and above who have embraced technology like smartphones and the Internet. The elderly's use of digital technology has increased due to pandemic restrictions (Fadzil et al., 2022). In Singapore, one-third of the elderly have

adopted digital technology (Perdana & Mokhtar 2022), and more than 70% of elderly Malaysians use it daily (Fadzil et al. 2023). Despite their growing digital literacy, elderly individuals still face substantial risks.

Research shows that while younger people (ages 16-24) have the highest risk of cyber victimization, elderly individuals aged 75 and above are more likely to suffer repeated victimization and financial loss (Havers et al. 2024). Additionally, wealthier elderly individuals are more susceptible to online scams and identity theft (Williams et al., 2018), which can lead to loneliness, depression, and other mental health challenges (Grigore & Maftei 2020). As the Internet becomes more integrated into daily life, the risk of cyber victimization among the elderly is likely to persist.

TYPES OF EXISTING CYBER SECURITY AWARENESS MODEL

Governments and organizations have implemented various cyber security awareness models aimed at reducing the vulnerability of older individuals to falling victim to fraudsters. However, the majority of current models are overly technical, making them unsuitable for elderly people with their disabilities and disabilities.

The first model, Situation Awareness-Oriented Cyber Security Education, proposed by Dai (2018), is a cybersecurity education framework based on the Situational Knowledge Reference Model (SKRM), designed to enhance university students' cybersecurity awareness.This model consists of four modules: research, lab, situation awareness, and presentation. In the research module, students are required to search for support materials online, which helps them independently investigate relevant cyber-attack scenarios. The lab module emphasizes hands-on activities, such as exposing students to malware patterns, unauthorized access, and potential countermeasures. This practical approach allows students to directly experience and learn about real-world cyber-attacks. In the situation awareness module, students create graphs such as network topologies or attack graphs based on the lab activities. These visualizations help them understand connections and develop potential solutions. Finally, in the presentation module, students demonstrate their ability to communicate effectively by describing or writing about the cyberattack incidents they have studied. However, the Situation Awareness-Oriented Cyber Security Education model, with its technical focus and hands-on labs, is more suitable for younger learners, such as university students (Dai 2018). The model primarily incorporates and delivers both theoretical and practical education components through the research and lab modules.

The second model, the Organization, Social, and Individual Cyber Security Awareness Model (OSICSAM), is designed by integrating selected existing cybersecurity models with elderly learning styles, incorporating organizational, societal, and individual elements (Buja et al. 2021). In this model, organizations play a key role in identifying security goals, designing awareness programs, and developing, implementing, maintaining, measuring, and reviewing cybersecurity awareness materials for the elderly. The societal and individual components reflect the peer education model, recognizing that elderly individuals often feel more comfortable learning and training alongside their peers. However, it is important to note that the OSICSAM model may not be suitable for senior citizens who are not affiliated with any organization. Additionally, the authors pointed out that a preliminary survey to obtain awareness ratings from the elderly was not conducted (Buja et al. 2021). A further limitation of this study is the lack of feedback from cybersecurity experts, which could have provided valuable insights. The education components provided in this model are practical and analytical in implementing and measuring layers.

The third model, the Cybersecurity Awareness Framework for the Elderly, was developed in 2021 (Zulkipli 2021). This framework uses the triangulation method and includes seven key steps for elderly users to protect their personal information online: updating software, patching devices, using strong passwords and keeping them secure, identifying current threats and attacks, improving internet skills, establishing support systems, and always signing out after use (Zulkipli 2021). First, elderly users should install and regularly update antivirus and antispyware software. Second, keeping devices such as computers, tablets, and mobile phones updated with the latest software patches is essential for protection against bugs and hackers. Third, using strong passwords and enabling two-factor authentication can help safeguard personal information. Fourth, staying informed about current threats, such as identity theft, which often targets the elderly, is critical. Fifth, enhancing internet skills, such as clearing browsing history after each session, can boost online safety. Sixth, it is vital to have a support system in place, so elderly users can seek help from trusted institutions when encountering suspicious emails, communications, or transactions. Finally, always logging out of apps and websites after use can reduce security and privacy risks. While this framework is deemed suitable for the elderly, it is acknowledged as being too technical, which may limit its accessibility to those without an IT background. Additionally, a significant limitation is the lack of participant surveys or interviews with cybersecurity experts to validate the framework's effectiveness. The model primarily provides practical guidance on how the elderly can protect their personal information online.

However, many existing cybersecurity awareness models are overly technical and do not clearly define how to educate the elderly effectively. The gaps addressed in this research stem from the evolving landscape of information technology and cyberattacks. The cybersecurity awareness models and approaches used in the past have proven unsuitable for the elderly population. Many of the existing models are too technical and do not cater specifically to the elderly demographic. To overcome these gaps, the proposed Synergistic Cyber Security Awareness Model for the Elderly (SCSAM-Elderly) was designed and developed, significantly contributing to the field by providing a tailored, less technical approach to cybersecurity education for the elderly. This model addresses their specific vulnerabilities and leverages accessible methods to enhance their awareness and understanding of cyber threats.

THE PROPOSED MODEL: A NEW SYNERGISTIC CYBER SECURITY AWARENESS MODEL FOR THE ELDERLY (SCSAM-ELDERLY) IN MALAYSIA

The proposed cybersecurity awareness and education model for the elderly, known as the Synergistic Cybersecurity Awareness Model for the Elderly (SCSAM-Elderly) (Azam et al. 2022), is specifically designed to educate and raise awareness among the elderly about current cyber-attacks. The model incorporates three key layers—theory, practical, and analysis—each validated by experts to effectively enhance cybersecurity awareness in this demographic (Alieyah et al. 2023).

The SCSAM-Elderly model is particularly suited for the elderly as it simplifies technical concepts, making them easier to engage with. A user-friendly website was developed as a platform, providing information on common cybercrimes targeting the elderly (Alieyah et al., 2023). The model focuses on three major types of cybercrimes: identity theft, phishing, and romance scams, which were carefully selected and validated by experts (Alieyah et al. 2023). This model consists of three integral layers: theory, practical, and analysis, as illustrated in Figure 1.

In the theory layer, the focus was on planning what needed to be achieved in cybersecurity for the elderly. Current issues of cyberattacks targeting the elderly were identified, with a

concentration on three commonly targeted cybercrimes: 1) phishing, 2) identity theft, and 3) romance scams. After planning and identifying the current cybercrime issues, the website application was designed and developed with its content based on these three cyberattack issues to spread security awareness among the elderly. The website included images or videos illustrating the three commonly targeted cyberattack issues. The goal was to ensure easy accessibility, comprehensibility, and the incorporation of multimedia elements suitable for the elderly. Importantly, the website application was designed to be accessible at any time, with no domain expiration. It was distributed to the elderly to enhance awareness and educate them about these three common cybercrime issues. The purpose was to help the elderly become more informed about these threats, build their confidence, and empower them to prevent becoming victims of cybercrime.

The practical layer built upon the theory phase. After the elderly learned about the three theories of cybercrime, they were tasked with answering questions to measure their understanding in the theory layer. For example, given that scamming text was identified as one of the tactics used in cyberattacks, the website included images or videos illustrating scamming text. Then, questions were presented, such as "*You receive a text message from the vendor who asks you to click on a link to claim your award. What should you do*?". The elderly users were expected to answer these questions and submit their responses. Furthermore, the practical layer delivered cybersecurity education with the objective of enhancing cybersecurity knowledge and awareness among the elderly population. Most importantly, this layer aimed to address the three common issues associated with cyberattacks targeting the elderly.

The analysis layer collected the findings after the respondents had submitted their answers within the practical layer. It identified the level of awareness among the elderly, indicating whether there had been an increase in awareness. To measure the level of awareness, the system monitored the answers submitted by the elderly. Each question was scored, and all correct answers were tallied to determine the overall level of awareness—whether low, moderate, or high. The elderly received their results via email. If the elderly's results are not satisfactory, they have to answer until they get full marks to ensure they understand, and their level of awareness increases.

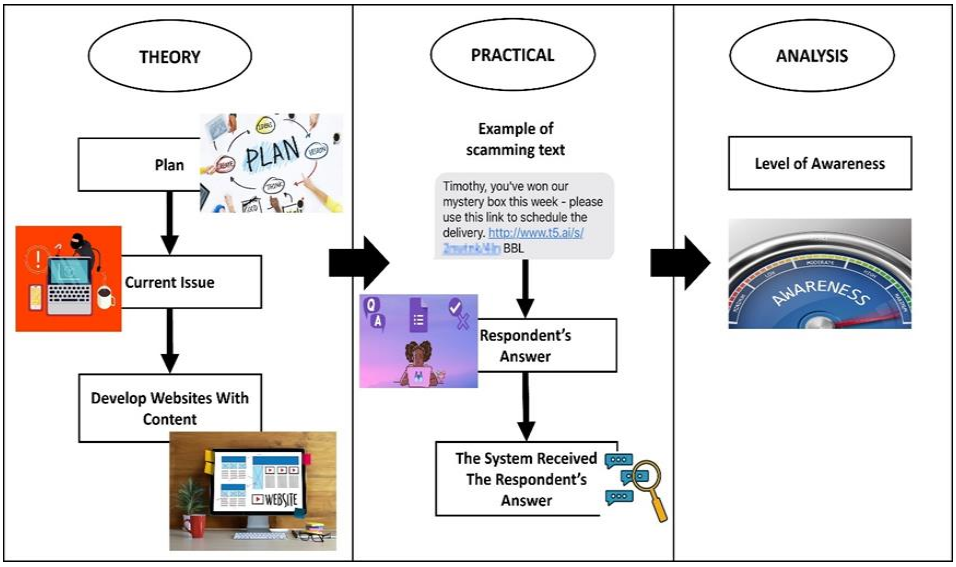

FIGURE 1. Synergistic Cyber Security Awareness for the Elderly (SCSAM-Elderly)
Source: Azam et al. (2022)

METHODOLOGY

The analysis of the survey for the proposed model, the New Synergistic Cyber Security Awareness Model for the Elderly (hereafter referred to as SCSAM-Elderly), involves five steps: 1) feasibility study, 2) survey development, 3) data collection, 4) analysis of the findings pre-survey and post-survey, and 5) documentation writing.

FEASIBILITY STUDY

The first step encompassed a feasibility study, a crucial phase that needed to be conducted systematically. This study employed a systematic literature review to gather data on cybersecurity, the elderly, existing cybersecurity awareness models, and the proposed model, SCSAM-Elderly, within the Malaysian context. The study focused on collecting updated data on cybersecurity awareness, particularly emphasizing existing models and approaches for measuring awareness among the elderly. The findings of the feasibility study and literature review are summarized and presented in the Literature Review section.

SURVEY DEVELOPMENT

The second step involves survey development. The survey questions were adapted from studies conducted by Blackwood-Brown (2018) and Garba et al. (2020). Additionally, the survey was translated into both English and Malay to accommodate respondents in Malaysia.

The survey consisted of eight sections. Section 1 focuses on demographic information, including gender, age, race, location, working sector, working categories, years of internet usage, and highest education level. In Section 2, there are questions related to cyber security knowledge, designed to assess the current level of awareness among the elderly group. In Section 3, questions related to privacy knowledge are included to gauge the elderly group's perception of privacy and their basic knowledge of privacy concepts. Section 4 consists of questions aimed at evaluating the elderly group's knowledge regarding trust when using the internet and online systems. Section 5 section focuses on password management, assessing the knowledge of the elderly group regarding effective password management practices. In Section 6, there are questions pertained to cyber security awareness, specifically focusing on how aware the elderly were of common cyber security threats they might encounter online. Section 7 measures computer self-efficacy, examining the elderly group's perception of their own computer usage abilities. The final section addresses the risk of identity theft, exploring the elderly group's beliefs regarding the possibility of their personally identifiable information (PII) being unlawfully used for someone else's gain.

Last but not least, is submitting the survey questions for approval from the Research Ethics Committee (REC). Finally, the survey was submitted for approval to the Research Ethics Committee (REC). Once approval was obtained, the third step involved data collection, where the survey was distributed to elderly participants in Melaka, Malaysia.

DATA COLLECTION

The third step is where the researcher used a set of survey in the second step for collecting the data. For this phase, this study conducted two guided surveys, namely, a pre-survey and post-survey. A guided survey session was carried out with a cohort of elderly individuals who are part of Society 5.0. For the purposes of this research, it was determined that a sample size of 50 elderly

participants from Society 5.0 would be selected for the study. The elderly group comprised 25 women and 25 men, with an equal number of individuals who were IT-literate or non-IT-literate, aged 60 years and above. Participants were selected from various locations in the state of Melaka, Malaysia.

Additionally, a guided pre-survey was conducted to assess the elderly participants' level of cybersecurity knowledge and awareness. The guided survey was conducted face-to-face, allowing the researcher to explain the questions to the respondents individually, ensuring each question was understood before the elderly respondents answered using a printed survey form. It took approximately twenty minutes per elderly individual to complete the pre-survey. The distribution and collection of the guided pre-survey spanned one month.

The newly developed SCSAM-Elderly model underwent validation through a post-survey administered to the same group that participated in the pre-survey. Before conducting the post-survey, the researcher went to the elderly and brought the laptop for them to access the SCSAM-Elderly website, which served as the platform for spreading awareness and educating them about cybercrime issues targeting them such as phishing, romance scam and identity theft. For example, the researcher explained the websites, and then the elderly accessed and learned from the websites. It took approximately 3 months for all the elderly to complete the cybersecurity awareness website training and post-survey. After the elderly completed learning from the websites, the post-survey was conducted. The post-survey reused the same questions from the guided pre-survey, allowing for a direct comparison of participants' knowledge before and after the training. They completed the survey on paper, and the researcher subsequently transferred the data from the paper to a Google Form. The collected data were analyzed using SPSS to assess whether the elderly participants' understanding of cybersecurity and awareness had improved in the post-survey compared to the pre-survey. The distribution and collection of survey spanned four months, from January 1, 2023, to April 30, 2023, covering both the pre-survey and post-survey steps.

The data collection process encountered several challenges. First, scheduling face-to-face sessions with elderly participants required careful planning, as many had mobility limitations. Additionally, varying levels of digital literacy posed a significant challenge during the post-survey phase. While IT-literate participants adapted quickly to the SCSAM-Elderly website, those unfamiliar with technology needed extra time and guidance, which slowed the process down. Furthermore, language barriers and difficulties in understanding certain concepts persisted. Despite translating the survey into both English and Malay, some elderly participants struggled with specific terms, requiring the researcher to provide repeated explanations. The extended data collection period of four months also introduced logistical challenges, as follow-up visits and consistent monitoring were necessary to ensure participants completed the training and post-survey on time.

ANALYZING THE FINDINGS OF PRE AND POST-SURVEY USING SPSS

The fourth step involves analyzing the data from both the pre-survey and post-survey using SPSS Version 27.0. This phase employs quantitative analysis, focusing on numerical data and statistical measures. This analysis includes examining numerical values, percentages, and statistical metrics to draw meaningful conclusions from the data.

For this study, a paired sample t-test was employed, a statistical technique used to determine if there is a significant difference between the average scores of two related groups (Tonggumnead 2021). Here, the related groups are the pre-survey and post-survey scores from the

same participants. According to Tonggumnead (2021), this method is instrumental in identifying whether there is a significant change in scores before and after the intervention.

In the context of evaluating a targeted cybersecurity education program for the elderly, the paired sample t-test is crucial for assessing the program's effectiveness. It helps determine if there is a statistically significant difference in the mean scores before and after the educational intervention (Dewantara et al. 2020). This choice of methodology not only strengthens the study's internal validity but also enhances the credibility and generalizability of the findings. The t-test allows the study's results to be more comparable and applicable to broader cybersecurity awareness research, improving its relevance and transferability to a wider audience.

According to Afifah et al. (2022), the formula for the paired sample t-test involves calculating the mean difference ($\bar{d}$) divided by the standard error of the mean difference ($s_{\bar{x}}$). The formula for the paired sample t-test is shown in the equation below:

$$t = \frac{\bar{d}}{s_{\bar{x}}}$$

The degrees of freedom (df) are used to determine the distribution from which the t-value is derived (Afifah et al. 2022). Where n represents the number of respondents who participated in the research. The df can be determined using the following formula:

$$df = n - 1.$$

In addition to the t-value, significance is assessed using the p-value from the output table. According to standard criteria, if the p-value is below 0.05, it indicates a statistically significant difference (Afifah et al. 2022). This method allows comparison of the means of two related groups, such as pre-test and post-test scores, to determine if there was a significant change following the intervention (Phetsut & Waemusa 2022).

For data preparation, the pre-survey and post-survey scores were entered into SPSS. Each row in the dataset represented an individual participant, with columns for pre-survey and post-survey scores. This arrangement allowed for accurate comparison of each participant's data before and after the intervention. Variables were clearly defined to differentiate between the pre-survey and post-survey scores, ensuring clarity and precision in the analysis.

Next, in order to conduct the paired sample t-test in SPSS Version 27.0, the following steps were taken: First, the dataset containing pre-survey and post-survey scores was loaded into SPSS. Next, the 'Analyse' menu was selected, 'Compare Means' was chosen, and 'Paired-Samples T Test' was selected. The pre-survey scores were assigned as the first variable and the post-survey scores as the second variable. By clicking 'OK,' SPSS generated an output that included the average scores (means) for both the pre-survey and post-survey, the difference between these means, the t-value, and the significance level (p-value). The SPSS output provided key statistics necessary for interpretation, including means, standard deviations, mean differences, t-value, degrees of freedom, and the p-value. A p-value less than 0.05 typically indicates a statistically significant difference between pre-test and post-test scores, suggesting that the intervention had a notable impact.

To ensure the reliability of the results, it is essential to use the same set of questions for both the pre-survey and post-survey. This consistency helps to ensure that any observed differences in responses are attributable to the intervention rather than variations in the questions.

By maintaining uniformity in the survey items, the study enhances the reliability of the findings and strengthens the validity of the conclusions drawn from the data.

DOCUMENTATION WRITING

The final phase in this research endeavor involves documentation, which includes the comprehensive recording of all pertinent data and analyses gathered throughout the research process.

RESULTS AND DISCUSSION

DEMOGRAPHIC PROFILE OF THE RESPONDENTS

Based on the distributed questionnaires, the initial sections aimed to gather general information from the respondents, including their gender, age, race, location, work history, working sector, working categories, years of internet usage, and highest education level. Refer to Table 1 for a detailed breakdown of this demographic data.

TABLE 1. Demographic Profile of Respondents

Variable	Descriptions	Frequencies	Percentage
Gender	Male	25	50
	Female	25	50
	Total	50	100
Age	60 - 69	36	72
	70 - 79	13	26
	80 – 89	1	2
	90 or over	0	0
	Total	50	100
Race	Malay	46	92
	Chinese	2	4
	Indian	2	4
	Total	50	100
Location	Rural	34	68
	Urban	16	32
	Total	50	100
Have you ever worked?	Yes	49	98
	No	1	2
	Total	50	100
Working sector	Self-employed	11	22
	Public	17	34
	Private	19	38
	Not working	1	2
	Retired	2	4
	Total	50	100
Working categories	IT company	25	50
	Non-IT Company	25	50
	Total	50	100
Number of years using the internet	Less than 5	14	28
	5 - 9	6	12
	10 - 14	12	24
	15 - 19	10	20

	20 - 25	3	6
	26 - 29	3	6
	30 - 34	2	4
	35 or over	0	0
	Total	50	100
Highest education level	Primary school	16	32
	Secondary school	16	32
	Foundation / Matriculation / STPM / STAM	4	8
	Diploma	6	12
	Bachelor Degree	7	14
	Master Degree	1	2
	PhD	0	0
	Total	50	100

Based on the data presented in Table 1, it is evident that there was an equal representation of male and female respondents, with 25 respondents each, indicating a balanced gender distribution in this research.

In terms of age distribution, 36 respondents fell in the age group between 60 and 69, 13 respondents were aged between 70 and 79, 1 respondent was aged between 80 and 89, while there were no respondents aged 90 and above. Regarding the racial composition of the respondents, 46 identified as Malay, 2 as Chinese, and 2 as Indian. Concerning location, 34 respondents were from rural areas, while 16 were from urban areas.

As for work history, 49 respondents had previous work experience, while 1 respondent was not currently working. In terms of the highest working category, 19 worked in the private sector, 17 in the public sector, 11 were self-employed, 2 were retired, and 1 was not working. In the working sector, 25 were employed in non-IT companies, while 25 worked in IT companies.

In terms of education level, 16 respondents had completed primary school, 16 had completed secondary school, 7 held Bachelor's degrees, 6 had Diplomas, 4 had completed foundation, matriculation, STPM, or STAM courses, and only 1 held a Master's degree.

ANALYSIS OF PRE-SURVEY AND POST-SURVEY

The survey was conducted with elderly respondents to evaluate their cybersecurity knowledge and awareness. The pre-survey and post-survey data were analysed using the Statistical Package for the Social Sciences (SPSS) Version 27.0. The paired sample t-test equation was applied as outlined in the methodology, providing a robust method for evaluating the impact of the intervention on participants' cybersecurity knowledge and awareness. The analysis revealed significant differences in responses for many questions. Table 2 presents the results of the paired samples t-test, covering 30 questions. For instance, question 1, which assessed knowledge about cybersecurity among the elderly, has a mean difference $\bar{d}$ of -0.780 and a standard error of the mean difference $s_{\bar{x}}$ of 0.059. The formula and calculations for the paired sample t-test are as follows:

$$t = \frac{\bar{d}}{s_{\bar{x}}} = \frac{-0.780}{0.059} = -13.220$$

As the results in equation above show, there is a highly significant difference between the pre-survey and post-survey measurements for question 1. The t-value of -13.220, associated with a very low p-value of 0.000 and 49 degrees of freedom, indicates improved awareness.

The survey is divided into seven sections designed to assess various aspects of cybersecurity awareness among elderly participants. It includes topics such as overall cybersecurity knowledge, privacy knowledge, trust in using online systems, password management skills, awareness of cybersecurity threats, self-efficacy in computer use, and perceived risk of identity theft. Each section focuses on specific areas to determine the participants' understanding and attitudes toward online safety and security practices.

The Cybersecurity Knowledgeable (CK) section assesses the current level of cybersecurity awareness among elderly participants through 11 targeted questions, ranging from Q1 to Q11. Each question is designed to reveal varying degrees of understanding, highlighting significant differences in how participants perceive and respond to cybersecurity issues. For example, a study by Morrison et al. (2021) stated that educational programs specifically tailored for the elderly are effective in increasing their understanding of cyber threats, thereby promoting a more proactive approach to online safety. Nevertheless, questions 4, 5, and 9 did not show a significant difference. Specifically, in Q4 ("*When you receive an email from an unfamiliar sender, do you open it?*") and Q5 ("*When you receive an email requesting your credential information such as name, date of birth, age, or credit card number, do you provide it?*"), the responses suggest that most elderly participants are already aware of the dangers associated with unfamiliar emails and sharing personal information. Similarly, for Q9 ("*Do you use debit or credit cards at an outdoor payment machine?*"), the lack of significant difference may be attributed to a general preference among elderly participants for using cash, possibly due to their limited familiarity with debit card payments. A study by Cruijsen et al. (2016) revealed that older adults often exhibit a preference for cash transactions over debit card payments, primarily because of their long-standing habits and the perceived complexity of using electronic payment methods.

The survey is structured into several sections, each evaluating different aspects of cybersecurity awareness among elderly participants. The Privacy Knowledge (PK) section, consisting of a single question (Q12), assesses participants' understanding of privacy concerns by asking whether they have ever rejected a mobile app's request to access personal data. The responses reveal significant differences in privacy awareness, highlighting varied attitudes towards data sharing among the elderly. For example, Jafari (2023) emphasizes that privacy concerns can lead to protective behaviors among social media users, suggesting that older adults may adopt similar strategies to safeguard their personal information. Additionally, Goyeneche (2023) indicates that older adults generally score higher on privacy concern dimensions compared to younger individuals, reflecting a growing apprehension about online information sharing with age.

The Trust Knowledge (TK) section (Q13) explores trust levels in using the internet and online systems, revealing significant differences in confidence regarding the security and reliability of digital platforms. The Password Management (PM) section (Q14-15) evaluates practices and knowledge about secure password strategies, showing significant differences in awareness and practices concerning password security. Studies have shown that many users, including the elderly, often resort to simplistic passwords like "123456" or "password" due to difficulties in remembering complex combinations (Ayyagari et al. 2019). This tendency is further compounded by cognitive decline associated with aging, which may hinder their ability to create and recall secure passwords (Dandachi et al., 2013).

The Cybersecurity Awareness (CSA) section (Q16-21) measures participants' recognition of common threats such as phishing and malware, demonstrating significant differences in their awareness and responses to these threats. Sarno et al. (2019) found that older adults often exhibit a heightened sense of vulnerability to phishing attacks, attributed to both cognitive decline and past experiences with fraud. The Computer Self-Efficacy (CSE) section (Q22-24) assesses confidence in using computers, revealing significant differences in perceived digital competence. Many elderly individuals still struggle with digital literacy, which can impede their ability to fully comprehend the nuances of sophisticated phishing schemes (Ueno et al. 2021). The Risk of Identity Theft (PRIT) section (Q25-30) examines beliefs about the likelihood of personal information misuse, showing significant differences in perceived vulnerability to identity theft. The fear of identity theft can drive individuals to engage more actively in protective behaviors (Choi et al. 2021). For elderly individuals, learning about cybersecurity not only alleviates these fears but also fosters a sense of competence and autonomy. Douha et al. (2023) support this, emphasizing that cybersecurity awareness training can empower seniors to take proactive measures against cyber threats, thereby boosting their confidence in managing their online safety.

In conclusion, the survey uncovers substantial disparities in elderly participants' understanding and practices across key areas of cybersecurity. These findings emphasize the critical need for targeted interventions to address the gaps in cybersecurity knowledge and resilience within this demographic.

TABLE 2. Paired Samples T-Test

Question	**Paired Differences**		***t***	***df***	**p<0.05**	**Significance**
	Mean	**Std. Error Mean**				
1. Do you consider yourself knowledgeable about cybersecurity?	-0.780	0.059	-13.220	49	0.000	Highly significant
2. When using the computer system and the Internet, do you feel secure?	0.380	0.069	5.480	49	0.000	Significant
3. Do you know what Two-Factor Authentication (2FA) is and do you use it?	-0.400	0.076	-5.292	49	0.000	Significant
4. When you receive an email from an unfamiliar sender, do you open it?	-0.200	0.107	-1.871	49	0.067	Not significant
5. When you receive an email requiring your credential information such as name, date of birth, age, your credit card number? Do you send it?	0.020	0.045	0.444	49	0.659	Not significant
6. Do you ever reject app permission?	-0.080	0.039	-2.064	49	0.044	Significant
7. Do you know what is the difference between using HTTP and HTTPS?	-0.880	0.046	-18.956	49	0.000	Highly significant
8. Do you know what is the meaning of the concept phishing?	-0.900	0.043	-21.000	49	0.000	Highly significant
9. Do you use debit or credit cards at an outdoor payment machine?	-0.100	0.082	-1.219	49	0.229	Not significant
10. Do you shop/purchase items advertised on social networks or your private email?	-0.360	0.069	-5.250	49	0.000	Highly significant
11. Do you think that it is important to read the user agreements for free program/software before clicking accept?	-0.280	0.064	-4.365	49	0.000	Highly significant
12. Have you ever rejected a mobile app request for accessing your contacts, camera or location?	-0.080	0.039	-2.064	49	0.044	Significant

13. Do you have reason to believe that you are being observed online without your consent?	-0.360	0.069	-5.250	49	0.000	Highly significant
14. Do you use a harder-to-guess password to access your bank account than to access your social networking accounts?	-0.400	0.081	-4.950	49	0.000	Highly significant
15. Do you use the same passwords for both social networks such as Facebook, Twitter, iTunes, and your email accounts?	0.520	0.071	7.286	49	0.000	Highly significant
16. How aware are you of computer virus attacks?	-2.940	0.266	-11.070	49	0.000	Highly significant
17. How aware are you of identity theft resulting from phishing scams?	-4.260	0.310	-13.737	49	0.000	Highly significant
18. How aware are you of unauthorized people intercepting (i.e. capturing and stealing) your sensitive information online?	-3.920	0.313	-12.533	49	0.000	Highly significant
19. How aware are you of password security, e.g. setting strong passwords and keeping passwords safe?	-4.060	0.300	-13.524	49	0.000	Highly significant
20. How aware are you of social engineering attacks?	-2.980	0.267	-11.151	49	0.000	Highly significant
21. How aware are you of ransomware attacks?	-2.980	0.255	-11.698	49	0.000	Highly significant
22. I am comfortable working with computers	-2.100	0.208	-10.072	49	0.000	Highly significant
23. I can learn to use most computer programs, if I am given some training.	-1.780	0.250	-7.133	49	0.000	Highly significant
24. I can learn to use most computer programs just by reading the manuals and help documentations.	-2.780	0.251	-11.068	49	0.000	Highly significant
25. If my identity gets stolen while using the Internet, it would likely be because I was not careful and made mistakes while using it?	-2.040	0.337	-6.057	49	0.000	Highly significant
26. If my identity gets stolen while using the Internet, it would likely be because the Internet is not secure?	-2.180	0.339	-6.433	49	0.000	Highly significant
27. If my identity gets stolen while using the Internet, it is likely that others will know my personal details.	-2.080	0.339	-6.134	49	0.000	Highly significant
28. If my identity gets stolen while using the Internet, it is likely that I will lose money.	-1.800	0.345	-5.214	49	0.000	Highly significant
29. If my identity gets stolen while using the Internet, it is likely that others will misuse my data.	-1.840	0.358	-5.134	49	0.000	Highly significant
30. If my identity gets stolen while using the Internet, it is likely that I will feel anxious.	-2.240	0.370	-6.057	49	0.000	Highly significant

Source: Data Analysis SPSS

AWARENESS OF PRE-SURVEY AND POST-SURVEY

This section evaluates the elderly participants' cybersecurity awareness levels based on pre-survey and post-survey results to determine if their awareness increased. Figure 2 shows a significant impact of the cybersecurity awareness training on participants' knowledge and understanding. The pre-survey mean score of 40.60% saw a remarkable increase of 81.87% in the post-survey results, highlighting the initial lack of cybersecurity awareness among the elderly, which the training successfully addressed.

After the training, many participants expressed enjoyment in learning about cybersecurity (Kam et al. 2021), indicating a notable shift in their intrinsic motivation. These results strongly support the training's success in enhancing their understanding of cybercrime issues. Similarly, Blackwood-Brown et al. (2019) found that cybersecurity awareness training significantly improved senior citizens' ability to take proactive measures against cyber threats. Beyond the numbers, the program's impact is evident in fostering a proactive mindset and equipping participants with the knowledge necessary to navigate the dynamic cybersecurity landscape (Zulkipli 2021).

If other existing cybersecurity awareness models had been implemented, the results might not have been as successful as those achieved by the SCSAM-Elderly model. Many existing models lack a comprehensive theoretical framework and do not adapt well to the evolving cybersecurity landscape. As discussed in the literature review, these models tend to be overly technical, limiting their accessibility for individuals without an IT background and making them less suitable for elderly populations outside of organizational environments.

In contrast, the SCSAM-Elderly model uses a user-friendly website to educate the elderly on three specific types of cybercrime. It includes educational materials, interactive quizzes to assess comprehension, and an analysis system to evaluate the effectiveness of the training. Participants who do not achieve satisfactory results are required to review the websites and retake quizzes until they attain full marks, ensuring thorough understanding and significant improvement in cybersecurity awareness.

Moreover, the program not only increased awareness of potential threats but also instilled confidence in participants' ability to navigate and use digital technologies effectively. This confidence is particularly evident in their responses regarding comfort with computers and confidence in learning computer programs when provided with training (Miller 2024). The significant improvements in these areas suggest that the program successfully imparted both theoretical knowledge and practical skills that participants can apply in real-world situations. Overall, the findings indicate that the program effectively enhanced participants' cybersecurity awareness, knowledge, and skills, empowering them to better protect themselves and their digital assets in an increasingly complex cyber threat landscape.

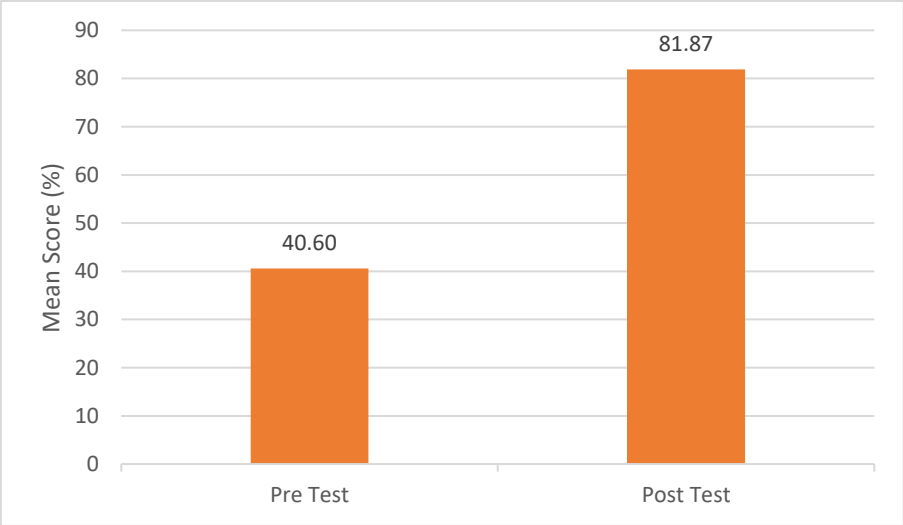

FIGURE 2. Bar Graph of Mean Score Awareness of Pre-Survey and Post-Survey
Source: Data Analysis SPSS

CONCLUSION AND FUTURE WORK

In conclusion, this study highlights the potential of deploying the proposed SCSAM-Elderly model to enrich the knowledge and awareness of cybersecurity among the elderly. The results from SPSS indicate that the SCSAM-Elderly model demonstrated an increase in awareness after the implementation of cybersecurity training compared to before the training. Cultivating and enhancing cybersecurity awareness is crucial, and encouraging the education of the elderly is essential to maximize their knowledge of cybersecurity. By using the SCSAM-Elderly model, elderly users can gain the knowledge and expertise needed to effectively protect themselves from potential threats on the Internet.

For future studies, it is recommended that further research explore the broader implementation of the SCSAM-Elderly model as a tool and guide for governments or organisations aiming to raise cybersecurity awareness among the elderly. This could involve integrating the model into public awareness campaigns, community programmes, and digital literacy initiatives targeted at the elderly population. Furthermore, there is a need to enhance the theoretical content to cover the latest types of cybercrime issues. It is crucial to continuously update and expand the theoretical content of the SCSAM-Elderly model to include the latest types of cybercrime issues. As cyber threats evolve, the model's educational material must remain current to effectively safeguard the elderly against new and emerging risks.

ACKNOWLEDGEMENT

Our sincere appreciation goes to Kementerian Pendidikan Tinggi Malaysia (KPT), Fundamental Research Grant Scheme (FRGS/1/2021/ICT07/UITM/02/1), RMC, and UiTM for the support given to this research endeavour. Thanks are also expressed to the Akademika for accepting this article for publication of the journal.

AUTHOR'S CONTRIBUTION

Introduction: Rabiah Ahmad; Literature Review: Nurul Alieyah Azam; Methodology: All authors; Result and Discussion: All authors; Conclusion: Nurul Alieyah Azam; Validation: Alya Geogiana Buja.

CONFLICT OF INTEREST

The authors declares that there is no conflict of interest.

REFERENCES

Afifah, S., Mudzakir, A., & Nandiyanto, A. B. D. 2022. How to Calculate Paired Sample t-Test using SPSS Software: From Step-by-Step Processing for Users to the Practical Examples in the Analysis of the Effect of Application Anti-Fire Bamboo Teaching Materials on Student Learning Outcomes. *Indonesian Journal of Teaching in Science* 2(1): 81–92.

Alieyah, N., Buja, A. G., Masri Sahri, N., Ahmad, R., Latip, S. F. A., Habidin, N. F., Darus, M. Y., Hussin, M. S., & Saat, S. 2023. Development of a New Synergistic Cyber Security Awareness Model for The Elderly in Malaysia (SCSAM-Elderly). *2023 IEEE 8th*

International Conference on Recent Advances and Innovations in Engineering (ICRAIE): 1-8.

Ayyagari, R., Lim, J., & Hoxha, O. 2019. Why do not we use password managers? a study on the intention to use password managers. *Contemporary Management Research* 15(4): 227-245.

Azam, N. A., Buja, A. G., Darus, M. Y., & Sahri, N. M. 2022. SCSAM-Elderly: A New Synergistic Cyber Security Model for the Elderly for IR4. 0 Readiness in Malaysia. *In 2022 IEEE 12th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*: 117-122.

Blackwood-Brown, C. G. 2018. An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills. Ph.D Thesis, College of Engineering and Computing, Nova Southeastern University, Florida, United States.

Buja, A. G., Wahid, S. D. M., Rahman, T. F. A., Deraman, N. A., Jono, M. N. H. H., & Aziz, A. A. (2021). Development of organization, social and individual cyber security awareness model (Osicsam) for the elderly. *International Journal of Advanced Technology and Engineering Exploration 8*(76): 511–519.

Casey Crane. 2019. 3 Cyber Fraud Tactics Targeting Seniors And Why They're So Effective. *Cybercrime Magazine*, 13 September. https://cybersecurityventures.com/3-cyber-fraud-tactics-targeting-seniors-and-why-theyre-so-effective/. Retrieved on: 15 September 2023.

Choi, J., Kruis, N. E., & Choo, K. 2021. Explaining fear of identity theft victimization using a routine activity approach. *Journal of Contemporary Criminal Justice* 37(3): 406-426.

Cruijsen, C. V. D., Hernández, L., & Jonker, N. 2016. In love with the debit card but still married to cash. *Applied Economics* 49(30): 2989-3004.

Dai, J. (2018). Situation Awareness-Oriented Cybersecurity Education. *2018 IEEE Frontiers in Education Conference (FIE)*: 1–8.

Dandachi, G., Hassan, B. E., & Husseini, A. E. 2013. A novel identification/verification model using smartphone's sensors and user behavior. *The 2nd International Conference on Advances in Biomedical Engineering*: 235-238.

Department of Statistics Malaysia. 2023. *Current Population Estimates, Malaysia, 2023*. Putrajaya: Department of Statistics Malaysia.

Dewantara, D., Wati, M., Mısbah, M., Mahtari, S., & Haryandi, S. 2020. Blended learning to improve learning outcomes in digital electronics courses. *Proceedings of the 1st South Borneo International Conference on Sport Science and Education (SBICSSE 2019)* 407: 118–190.

Douha, N. Y., Renaud, K., Taenaka, Y., & Kadobayashi, Y. 2023. Smart home cybersecurity awareness and behavioral incentives. *Information & Computer Security* 31(5): 545-575.

Fadzil, N. M. H., Shahar, S., Rajikan, R., Singh, D. K., Ludin, A. F. M., Subramaniam, P., Ibrahim, N., Vanoh, D., & Ali, N. M. 2022. A scoping review for usage of telerehabilitation among older adults with mild cognitive impairment or cognitive frailty. *International Journal of Environmental Research and Public Health 19*(7): 1–14.

Fadzil, N. M. H., Shahar, S., Singh, D. K., Rajikan, R., Vanoh, D., Ali, N. M., & Noah, S. M. A. 2023. Digital technology usage among older adults with cognitive frailty: A survey during COVID-19 pandemic. *Digital Health* 9: 1–14.

Garba, A., Musa, M. A., & Othman, S. H. 2020. A Study on Cybersecurity Awareness Among Students in Yobe : A Quantitative. *International Journal on Emerging Technologies* 11(5): 41–49.

Goyeneche, D., Singaraju, S., & Arango, L. 2023. Linked by age: a study on social media privacy concerns among younger and older adults. *Industrial Management & Data Systems* 124(2): 640-665.

Grigore, A. and Maftei, A. 2020. Exploring the mediating roles of state and trait anxiety on the relationship between middle adolescents' cyberbullying and depression. *Children* 7(11): 240.

Havers, B., Tripathi, K., Burton, A., Martin, W., & Cooper, C. 2024. A qualitative study exploring factors preventing older adults from reporting cybercrime and seeking help. *CrimRxiv*: 1-22.

Jafari, M. and Shaghaghi, Z. 2023. Navigating privacy concerns: social media users' perspectives on data sharing. *AI and Tech in Behavioral and Social Sciences* 1(1): 20-26.

Jesrina Ann Xavier & Chong Wei Ying. 2023. Combating Financial Fraud Amongst Senior Citizens Through Design Thinking. *BERNAMA Thoughts*, 21 August. https://bernama.com/en/thoughts/news.php?id=2216684. Retrieved on: 20 September 2023.

Kam, H., Ormond, D., Menard, P., & Crossler, R. E. 2021. That's interesting: an examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal* 32(4): 888-926.

Mahajan, R. & Kaur, M. 2021. A Review on Cyber Security and Its Threats. *EasyChair*, 28 November. https://easychair.org/publications/preprint/cW4z. Retrieved on: 20 January 2024

Miller, L. M. S., Callegari, R. A., Abah, T., & Fann, H. 2024. Digital literacy training for low-income older adults through undergraduate community-engaged learning: single-group pretest-posttest study. *JMIR Aging* 7: e51675.

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.

Muhammad, F., Awang, S. A., Shaarani, A. Z. M., Hussin, M. Y. M., & Mahjom, N. 2024. Pengaruh Pengetahuan Tip Pencegahan Terhadap Keyakinan Remaja di Pantai Timur bagi Melindungi Diri daripada Jenayah Scam. *Akademika* 94(2): 179–196.

Perdana, A., & Mokhtar, I. A. 2022. Seniors' adoption of digital devices and virtual event platforms in Singapore during covid-19. *Technology in Society* 68: 101817.

Phetsut, P., & Waemusa, Z. 2022. Effectiveness of Mobile Assisted Language Learning (mall)-based intervention on developing Thai EFL Learners' oral accuracy. *International Journal of Technology in Education* 5(4): 571–585.

Tonggumnead, U. 2021. A comparative study on the efficiency of test statistics in testing the differences between two dependent datasets. *International Journal of Applied Mathematics* 34(1): 43–74.

Ueno, D., Daiku, Y., Eguchi, Y., Iwata, M., Amano, S., Ayani, N., Nakamura, K., Kato, Y., Matsuoka, T., & Narumoto, J. 2021. Mild Cognitive Decline Is a Risk Factor for Scam Vulnerability in Older Adults. *Frontiers in Psychiatry* 12: 685451

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. 2018. Under the corporate radar: examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior* 40(9): 1119-1131.

Zulkipli, N. H. N., Rashid, N. A. M., Zolkeplay, A. F., & Buja, A. G. 2021. Synthesizing Cybersecurity Issues And Challenges For The Elderly. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12(5): 1775–1781.

Nurul Alieyah Azam
College of Computing, Informatics and Mathematics
Universiti Teknologi Mara Cawangan Melaka, Malaysia
Email: nurulalieyah20@gmail.com

Alya Geogiana Buja (Corresponding author)
College of Computing, Informatics and Mathematics
Universiti Teknologi Mara Cawangan Melaka, Malaysia
Email: geogiana@uitm.edu.my

Rabiah Ahmad
Faculty Engineering Technology
Universiti Tun Hussein Onn, Malaysia
Email: rabiah@uthm.edu.my

Shekh Faisal Abdul Latip
Faculty of Information System and Communication Technology
Universiti Teknikal Malaysia Melaka, Malaysia
Email: shekhfaisal@utem.edu.my

Nor Masri Sahri
College of Computing, Informatics and Mathematics
Universiti Teknologi Mara Cawangan Melaka, Malaysia
Email: normasri@uitm.edu.my