SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

A Light Review on Cyber Security Awareness Models for the Elderly

Nurul Alieyah Azam[1], Alya Geogiana Buja[1,*], Nor Masri Sahri[1], Rabiah Ahmad[2], Nur Fadly Habidin[3], Shekh Faisal Abdul Latip[4], Mohamad Yusof Darus[5], Mohd Shahril Hussin[6], Saharudin Saat[7]

[1] College of Computing, Informatics and Mathematics, Universiti Teknologi Mara Cawangan Melaka, Malaysia
[2] Faculty Engineering Technology, Universiti Tun Hussein Onn, Johor, Malaysia
[3] Faculty of Management and Economics, Universiti Pendidikan Sultan Idris, Perak, Malaysia
[4] Faculty of Information System and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia
[5] College of Computing, Informatics and Mathematics, Universiti Teknologi Mara, Shah Alam, Malaysia
[6] AVP, Cyber Forensics and Malware Analysis Lab, Kuala Lumpur, Malaysia
[7] Information Management, Ministry of Domestic Trade and Consumer Affairs, Malaysia

ARTICLE INFO

Article history:
Received 22 June 2023
Received in revised form 10 February 2024
Accepted 6 March 2024
Available online 25 April 2024

Keywords:
Awareness; Cybercrime; Cybersecurity; Elderly

ABSTRACT

Millions of people use the internet daily, including the elderly, who are among the most at-risk groups for cybercrime, such as fraud, hacking, and cyberbullying. However, there has been a lack of cybercrime studies focusing on them. Additionally, various cybersecurity models deployed by governments and organizations are found to be inconvenient and too technical for the elderly, especially those with impairments or conditions that require special attention. This subsequently leads to an increasing number of cybercrimes. Therefore, this paper presents a light review of existing cybersecurity models suitable for the elderly. Three methods were used to review existing cybersecurity awareness models. First, a feasibility study was conducted following several works of literature related to cybersecurity, types of cybercrimes involving the elderly, characteristics of the elderly commonly targeted by cybercriminals, cybersecurity awareness models, and the elderly's learning styles. Second, based on the literature review, the elderly's learning styles were analyzed. Finally, the cybersecurity awareness model suitable for the elderly was chosen and analyzed with respect to their phases, validity, and technicality. In conclusion, the SCSAM-Elderly was selected as the most suitable model for the elderly to learn and spread awareness of cybersecurity. This study could increase cybersecurity awareness and encourage educating the elderly to maximize their knowledge of cybersecurity. The findings from this study can guide organizations, agencies, governments, and educational institutions in their endeavours to educate the elderly about cybercrime and cyberattacks.

1. Introduction

1.1 Research Background

With the growth of information, communication, and technology (ICT), people all over the world can now connect with each other through an advanced information network. Even though the rapid

* *Corresponding author.*
E-mail address: geogiana@uitm.edu.my

https://doi.org/10.37934/araset.44.1.3145

advancement of ICT has helped people in a lot of different ways, it still cannot be guaranteed that users will not become victims of cybercrimes. With respect to this, cybersecurity has become an important concern for online users where securing information is deemed one of the most challenging problems. Generally, cybersecurity training is vital for all individuals, regardless of their age group, in order to protect themselves from the growing threats posed by cybercriminals. In a study conducted by Blackwood and Carlene [1], it is emphasized that cybersecurity awareness implies making Internet users mindful of cybersecurity issues and threats as well as assisting them in understanding cyber threats so they can entirely focus on utilizing the web securely [2]. Therefore, cybersecurity education is important since cybercrimes may occur to anyone, anywhere and at any time. Furthermore, Rahman *et al.,* [3] has highlighted that cyber security education and awareness are important to protect internet users from cybercrime and other cyber threats that are getting worse. All preventive measures contribute to making an individual knowledgeable, vigilant, and ready to cope with cybercrime issues are crucial in addressing cybercrime issues.

An elderly person is defined as an individual aged 60 and above [2]. As most elderly are known to be financially prepared for old age, they commonly become the main target of cybercriminals. In addressing this situation, there are several cyber security awareness models in place, but very few of them are designed with the needs of the elderly in mind mainly due to the sophistication of the technologies involved and the unique constraints that people with disabilities or impaired health face when interacting with [2]. Additionally, cybersecurity concerns among the elderly have been rarely talked about and most of the time, this issue has been put off [4]. According to the report released by CyberSecurity Malaysia, in 2022, there were a total of 7,292 cybercrime cases which there were 4,741 cases involving online fraudulence [5]. In the same year, Malaysia recorded an increase in the elderly population which is 2.4 million elderly residents compared to 2021 which is 2.3 million [6]. When the elderly retire and rely on their savings nest for financial support, they become prime targets for a certain type of cybercrime targets [7]. Most elderly victims have been commonly duped into withdrawing savings from safety deposit boxes after being convinced and duped by online criminals.

The existing cyber security awareness model that has been deployed in the initiatives was not suitable for the elderly group due to the advancement in information technology and attacks. Several of current cyber security awareness models can be too technical and do not focus on the elderly in Malaysia. The effectiveness of these models has not been validated through surveys or cyber security expert. The significance of this study can promote cyber secure to reduce risk of the elderly being victims and the industry can build more features for the development or application about cyber security awareness for the elderly. Therefore, this paper will light review existing cybersecurity awareness models that are suitable for the elderly. This is mostly due to the fact that improving the awareness and knowledge of elderly people regarding cyber security issues requires information regarding protection and prevention and privacy. Subsequently, the study's research background and literature review are covered in Section 1, followed by the methodology in Section 2, and the analysis of the cybersecurity models that are suitable for the elderly in Section 3. Finally, Section 4 presents the conclusion of this paper.

1.2 Literature Review

1.2.1 Cyber security

The term "cybersecurity awareness" refers to an individual's familiarity with topics related to online safety, such as the latest security threats, cybersecurity best practices, the risks associated with engaging in risky behaviours like clicking on malicious links or downloading infected

attachments, interacting with strangers online, disclosing personal information, and so on. Due to the rapid technological advancement and infrastructure of the Internet, cybersecurity has become a serious concern across the globe in the present times. Subsequently, effectively safeguarding personal information has also become a major concern among Internet users due to the increasing number of cybercrime cases daily. In relation to this, Mahajan *et al.,* [8] has discovered that there have been various preventive measures taken by various organizations and governments in addressing the issues related to cybercrimes. This includes cybersecurity education, especially in dealing with various emerging cybersecurity threats, which is thus vital since all Internet users are exposed to cyber threats anywhere and at any time. With regard to this, elderly citizens are the riskiest group of cybercrimes since they have reserved funds as their monetary retirement support, which points out that cybercriminals make them their main target [7]. According to the FBI's Internet Crime Report IC3 2021, there are four types of cybercrime among the elderly which are tech support scams, identity theft, investment scam, and confidence scam or romance [9], which is presented in the following sub-section.

1.2.2 Four types of cybercrimes faced by the elderly

The elderly often become cybercriminal's main targets due to their vulnerability and lower cyber literacy rate as compared to younger age groups. According to FBI's internet crime complaint center (IC3) [9], cybercrimes that are used on the elderly include tech support scams, identity theft, investment scam, and romance scam.

1.2.2.1 Tech support scam

Technical support scams would commonly act as customer service or tech support agents from well-known tech companies. Fraudsters might contact their target by email, calls, or text messages and offer to fix the problem, such as a compromised email or bank account, computer virus, and the renewal of a software license [10]. Victims are duped into thinking their financial accounts have been hacked and they need to transfer their funds, at which point the fraudster has full access to the victim's computer and steals their money. Tech support scam also requests their victims to download and install free remote desktop software so that they can spy, manipulate and act on the victim's computer without their knowledge or consent. This includes opening a currency account to facilitate liquidating the victim's real bank account. According to FBI's IC3 [9], they received 23,903 complaints from victims in 70 countries about technical support services fraud with a total amount of loss amounting to $347 million [9]. Most of those affected are above 60 years old and experience at least 68 percent of losses of nearly $238 million. Nevertheless, in 2021, IC3 noticed a complaint about fraudsters pretending to be customer support for businesses like banks, utilities, and even cryptocurrency exchanges.

1.2.2.2 Identity theft

Identity theft happens when an individual, group of people, or organization gets, transfers, owns, or uses others' personal information without permission to make money for themselves [11]. It includes using others' personal information to open a new account and use medical care. Identity theft targets seniors by stealing personal information or sensitive data. This information is then used to open fraudulent accounts or make purchases without the victim's permission. In many cases, the elderly are the victims of identity theft because criminals trust they have savings and are less likely

to monitor their credit reports and financial accounts. The elderly living in residential homes or under someone's care may be particularly vulnerable, as caregivers often have access to their personal records. The common sign that always happens to the elderly is they receive a call or mail from collection agencies that want to collect a debt made in the name of the elderly, receive a bill for medical treatment that the elderly never had, suddenly stop receiving bank statement and received unexpected mail like letter or statement regarding an account that elderly never open [10].

1.2.2.3 Investment scam

The illegal sale or claimed sale of financial products is known as investment fraud. They might say that you need to act quickly on an investment opportunity. According to FBI's IC3 [9], a total of 2,100 victims over 60 years old reported investment scams with losses of over $239 million. Online investment scams target the elderly by convincing them to invest in "guaranteed" high-return investments. The next characteristic of an investment scam is to offer low or no-risk investment, complex strategies, or unregistered securities. They seem to be smart, nice, and charming. In reality, fraudsters will pocket the victim's money without providing any promised return. Examples of investment scams include advance fee scams, market manipulation frauds, pyramid schemes, and Ponzi schemes. Pyramid schemes are where scammers tell victims that they can get big returns or profit on a small investment. However, the victims need to find other investors as well [12]. Other investors pay the money the victim gets as a profit. Ponzi schemes where the scammer, a portfolio manager, tells victims that they will invest victims' money and give back a lot of money. However, the victims' money is actually from other paid investors [12].

1.2.2.3 Romance scam

Romance scams are those that try to get the victim to open emotionally. In 2021, IC3 received the report from 7,658 victims who had lost more than $432 million to a romance scam [9]. The highest losses for these types of fraud are among the elderly over 60 years old. The common sign of romance scam is the scammer is resided in another country and being far away from the victim, using a good profile that seems too good to be true, always avoiding meeting in person, sweet talk, pretending to be careful, asking for money to proof of victim's love and seek victim's help by asking for money to help scammer tide through their so-called misery. The scammers build a trusting relationship with the elderly as one of their strategies. The criminal claim to be either a family member or the love interest of the victims. This terrible cybercrime typically targets elderly women who live alone, including those who have recently been widowed. This category also included grandparent scams, in which scammers pose as a panicked family member, typically a grandchild, nephew, or niece of an elderly. The loved one claims to be in distress and require emergency financial assistance. In 2021, FBI IC3 reported losing approximately $6.5 million due to grandparent scams [9]. This case study shows the types of cybercrimes aiming seniors in 2021 that have been reported by FBI IC3. The next section will review the characteristics of the elderly as the main target of cybercrime by cybercriminals.

1.2.3 Characteristics of the elderly being the main target of cybercrimes

The elderly may be more vulnerable due to impairment and disabilities, solitude, unfamiliarity with technology, and generational inclination to trust authorities and hesitate to report the crime [13]. However, abuse victims have different profiles and traits that make them more susceptible to

financial exploitation. The elderly who are managing their finances for the first time are more likely to trust the guidance from others. Since they trust authority more, the elderly are more likely to respond to communications from companies or official institutions. For example, scammers from impersonated organizations, including police, bank, and others. In addition, the elderly lack knowledge and awareness of cyber security due to a lack of exposure to technology, so they are less likely to identify themselves as potential victims and take fewer steps to protect themselves online [14]. Besides, memory loss might impair one's capacity to recognize criminal activity and retain relevant information about the incident and the perpetrator [15]. Con artists could try to fill up blank memory with data that facilitates fraud. Someone with memory loss or other cognitive disabilities is easier to take advantage of financially. The elderly's vulnerability to criminals may stem from their loneliness, prompting them to seek mates through online dating sites [16]. Criminals might use it to connect with their victims and build trust. Criminals may target the elderly because they typically have larger credit limits and are less likely to check their balances frequently [15]. They may have more diversified assets than their younger counterparts, including real estate, savings, and retirement funds. The next section will review the types of existing cybersecurity awareness models that may help to educate and spread awareness among the elderly.

1.2.4 Types of existing cyber security awareness models

1.2.4.1 The information security awareness capability model (ISACM)

According to Khando *et al.,* [17], Poepjes and Lane came up with the ISACM model in 2012. The ISACM model provides three features [18]. The first feature is the importance of awareness, which looks at how people's knowledge of cyber security control will affect their ability to stay safe and not fall for a scam. The second key feature is a person's ability to be aware of a problem. This refers to how well a person can deal with a problem. For instance, how the person can understand the different types, traits, and situations of scams. This knowledge can affect how well people stay away from scams. Last but not least, the awareness risk looked at the difference between how important awareness is and how important a person thinks it is. ISACM model has not been validated through surveys by experts and participants in the organization. The ISACM model provides step-by-step guidelines for creating an education and training initiative. Nevertheless, the specifics of how this model should be applied remain unclear, especially in teaching the elderly.

1.2.4.2 The information security awareness program (ISAPM) general model

In 2013, Maqousi *et al.,* [19] worked together to establish the ISAPM model by taking into account what was learned from the consumer education concept. Any organization that sets out to start a program to raise awareness about cybersecurity should know what its cybersecurity goals are. To start with, organizations need to confirm their preference for cybersecurity. Secondly, they must identify the program platform for the security awareness program such as workshops, training, flyers, digital media, online forums, and news sections. Meanwhile, the third step involves the development stage which centres around establishing a website utilizing a programming language, which relies upon the organization's decision. In relation to this, they can consider content management system (CMS) which gives an internet-based platform that permits users to contribute to improving the web framework and empower their jobs towards spreading cybersecurity awareness. The next step is implementation, where the organization chooses one of these three ways to run the program: on the organization's website, in the administrative tool menu, or on a separate website.

From that point onward, the program needs a maintenance protocol in ensuring the recency and credibility of the data. To accomplish this, talented workers that are able to control and keep up with the program ought to be delegated for the undertaking. Following that, the measuring stage highlights the procedures of evaluating and measuring the degree of security awareness among the users. This assessment should be carried out to produce a number of timely reports and make them available online, especially to authorized website users. In the last step, reviewing, the administrative and technical staff read periodic reports and look at the statistics from the measuring process. From the review, this team should decide whether to approve or come out with a new set of procedures to be included in the program. The decision and recommendations made by the reviewing team will be submitted to the development stage for further improvements. It is important to consider ISAPM when designing cybersecurity training programs for seniors. Because of its non-complex design, it may be utilized by various businesses. There is a requirement for a minor adjustment to the underlying platform for this method. The efficiency of cyber security training for the elderly depends on the quality of the material and the delivery method, so it is best to adapt the website to meet their needs.

1.2.4.3 The cyber security capability maturity model

In 2014, the Department of Energy came up with the cyber security capability maturity model which lets countries, organizations, and other groups figure out how good their cyber security is right at present [20]. The goal of this model is to figure out the different levels of capacity that can be found. If an organization implements something at the lowest level, it means that its capacity is either non-existent or very limited. On the other hand, an organization that implements something at the highest level has both a strategic method and the ability to optimize operational, threat, socio-technical, and political levels [20]. This model has five levels of scale. The lowest level, "start-up", shows that the organization has not done anything to raise cyber security awareness, or it could just be an initial discussion with little evidence. Meanwhile, the "formative" level shows that some elements have started to grow and be formed with clear evidence, but they may not be organized or well-defined. Besides, the "established" level also shows that the sub-parts factors are working. Still, the relative distribution of resources isn't thought about as much, and the strategic level shows that the company has decided which parts are most and least important for the organization. The level of dynamics shows that the company already has a clear plan for how to change its strategy based on key factors.

Therefore, in reading this model, a country or organization needs to conclude that its cyber security planning has used all the factors in this model. If the country does not meet the features in this model, then they have not reached maturity. For example, if a country intends to assess whether its cyber policy and strategy have reached maturity or not while it has not made any consultation on its cyber policy and strategy, then that country is considered to be in the initial level of maturity. However, if they have outlined their strategic plan and entered into the mediation process, the country is considered to be at the formative level of maturity. It is too difficult and technical to apply the suggestion made by this model, which states any model development program must align with the organization and national cyber security goals. Yet the component of education for the elderly is missing from this model.

1.2.4.4 The security awareness model

In 2014, Kortjan and Von Solms [21] came up with the security awareness model. The security awareness model was suggested for South Africa to show how people there use cybercafés and how they think about cyber security. This framework has five layers and one resource module. The first layer is strategic that is in line with what the government wants people to know and learn about cyber security.

The second layer is a tactical layer that is made up of three parts. First, running campaigns in collaboration with businesses, universities, and government agencies with the aim to help make the Internet safer. Second, the framework is aimed at campaigns in schools, the community, and cyber security education for everyone and every week in the community. Campaign week is an annual event that tries to teach people about cyber security and the right way to use cyberspace. At the school level, this campaign involves primary and secondary schools as many students are unaware of cyber security. The campaign is hoped to become part of the school curriculum and be taught in a way that is appropriate to the student's age. The third part is to provide formal cyber security education to students and, finally, to employees.

Besides, the third layer of the security awareness model is the preparation layer. There are four components involved in this layer: subject, material, platform, and apparatus. Several topics related to cyber security and not just limited to cybercrime have been identified. For instance, if the campaign's target group is the students, perhaps the content is “how to report cyber-bully”, however, if the audience is the parents, the topic content could be “warning signs of children becoming victims of cyberbullying”. The topics chosen are then further explored to make a connection with the content appropriate to the platform and equipment. The communication platform could be paper-based or digital, whereas the equipment is in the form of video, posters, social media, and more.

The fourth layer of the security awareness model is the delivery layer which involves the responsibilities to themselves and to one another, namely the roles of learner and teacher. Students are then expected to take on the role of teacher when the topic has been learned. This is so that the student acquires the continuously imparted information.

The fifth layer of the security awareness model is the monitoring layer. In this layer, monitoring and analysis are needed to figure out how well the campaign is going. The results of this campaign are based on what people who took part and helped said. The analysis and reports should be sent to the tactical layer so that the national cyber security education and awareness campaigns can learn about the needs of the participants and how well their campaigns are working.

Last but not least, is the resources module. In ensuring that every component is addressed, a few sources should be recognized. Therefore, this system recognizes five types of resources that function to channel necessary inputs to all layers. To begin with, individuals who expected to take on a task. Second, the information that is used to run the task. Third, the computer application such as productivity software that is needed for the campaigns, Forth, the infrastructure including computer hardware, servers, and printers. Lastly, is the financial capital. The security awareness model is suitable for the elderly because it can be used as a guide to create programs that increase awareness, reduce the damage caused by cyber-attacks, and improve one's understanding of cyber security. Unfortunately, this approach collects surveys from the elite and not from the participants.

1.2.4.5 Situation awareness-oriented cyber security education

Based on a research by Dai [22], it is explained that every university student needs to have knowledge related to cyber security. The approach is based on the situational knowledge reference

model (SKRM), which captures students' awareness of cybersecurity situations. There are four modules in the proposed educational program: research, lab, situation awareness, and presentation. In the research module, students ought to look for support materials on the web in order to expose them to investigating relevant cyber-attack situations on their own. The lab module emphasized hands-on lab activities such as exposing students to malware patterns, unauthorized access, and possible countermeasure. This is the most effective method of allowing students to learn and experience real-world cyber-attack on their own.

In the situation, awareness module, students have to make graphs from the lab module. The graph may be a network topology or an attack graph. From this graph, students can see various connections between them and come up with solutions. Students need to demonstrate their ability to communicate effectively by describing or writing about the cyberattack incidents they have learned about during the presentation module. Hence, a simpler cyber security education model is required to teach the elderly how to identify cyber-attacks and avoid becoming victims. Therefore, there is no validation model through surveys among university students and cyber security experts. Situation awareness-oriented cyber security education model is too technical for seniors as it involves knowledge of advanced computer science vocabulary and technical steps.

1.2.4.6 The peer education model

According to the Joint Select Committee on Cyber-Safety in Australia, it has been reported that older people prefer to learn how to stay safe online through their peers [23]. Those who are hesitant to learn about computers and the Internet then see that their other friends can do well after taking a few lessons and gaining confidence then they can do it too and sign up for the next class. Second, the report explains the speed of teaching delivery. For example, when a young individual teaches an elderly user about cyber safety, the lesson is found to be too fast that they could not catch it. However, the speed is slower when their peers deliver the content in the same age group. Therefore, if the elderly are taught at their own pace, they will be more motivated to learn how to use a computer and the Internet, and they will have a better chance of succeeding. This is just the beginning for the elderly to learn how to use technology. As they become more confident in using the Internet, they will likely seek the help of their children or grandchildren if any issues arise. Both sessions were conducted in the peer education model. The first session is a briefing, and the second session is an evaluation session. The duration for both sessions is one hour, of which 50 minutes are for the discussion and the remaining 10 minutes are spent on the evaluation. The Peer Education Model is suitable for the elderly because it is not technical. However, it takes more time for seniors to learn about cybersecurity. Also, there is no validation model through surveys and experts to verify the effectiveness of this model.

1.2.4.7 The organization, social and individual cyber security awareness model (OSICSAM)

OSICSAM was developed in 2021 as reported by Buja *et al.,* [24]. The OSICSAM model was designed based on the combination of selected existing cyber security models and elderly learning styles that involved the organization, society, and individuals. Cyber security awareness model among the elderly can be synergized by the model through the integration among the organizational, societal, as well as individual elements. The organization is responsible for identity organization security goals, designing awareness programs, and developing, implementing, maintaining, measuring, and reviewing the materials for cyber security awareness for the elderly. Social and individual are related to the peer education model because the elderly are more comfortable learning

and training with their peer. However, the OSICSAM model is not suitable for senior citizens who are not involved with any organization. A limitation of this study was not gathering surveys from the elderly and comments from cybersecurity experts.

1.2.4.8 Cybersecurity awareness framework for the elderly

Cybersecurity awareness framework for the elderly was developed in 2021 by Zulkipli [4]. The cybersecurity awareness framework for the elderly model uses the triangulation method and the awareness framework for the elderly. There are seven steps implemented in this model to reduce the risk among the elderly. The first step is to update the software that users need to install and use anti-virus and anti-spyware, which is important to protect personal information when the elderly are online. The second step is to patch devices by regularly updating computers, tablets, and mobile devices in order to protect users from bugs as well as providing software patches to protect against hackers. The third step is to use a strong password and keep it safe by enabling two-factor authentication to avoid attackers stealing personal information. The fourth step is to identify current threats and attacks, for example, identity theft which is a common method of information theft that targets the elderly. The fifth step is that the elderly need to update their internet skills, for example, by considering clearing their browsing history after each time they use the browser. The sixth step is the support system where the elderly can refer to a trusted institution if they need help, especially upon receiving any email, communication, or transaction that looks suspicious. The seventh step is to always remember to log out from any apps and websites after using them in minimizing the risk of vulnerable security and privacy risks. Therefore, this model is suitable for the elderly. However, this model is too technical and only those with an IT background can understand. Additionally, this model does not distribute surveys to participants or conduct interviews involving cybersecurity experts to verify its effectiveness.

1.2.4.9 The synergistic cyber security awareness model for the elderly (SCSAM-Elderly)

SCSAM-Elderly was developed in 2022 as reported by Azam *et al.,* [2]. Besides, the SCSAM-Elderly model implements components of education which are theory, practical, and analysis as shown in Figure 1 below. SCSAM-Elderly has three layers which are theory, practical, and analysis in order to educate and increase awareness among the elderly. In the theory layer, there is preparation for the goals that should be achieved in cyber security for the elderly. It is important to identify the current cyber-attack against the elderly. SCSAM-Elderly has educated the elderly by using the website by attaching all the current cybercrime theories that often happen to the elderly. The second layer is practical layer. In the practical layer, this model provides quizzes related to the current cybercrime for the elderly to answer. The third layer is the analysis layer, where the team will monitor all the quizzes' answers to determine whether elderly awareness is increased or not. Based on the level of awareness, the team can then determine how to better educate the elderly about cybercrimes. SCSAM-Elderly is not technical and suitable for the elderly in order to increase elderly's awareness. Last but not least, this model was validated by the questionnaire survey and cyber security expert.

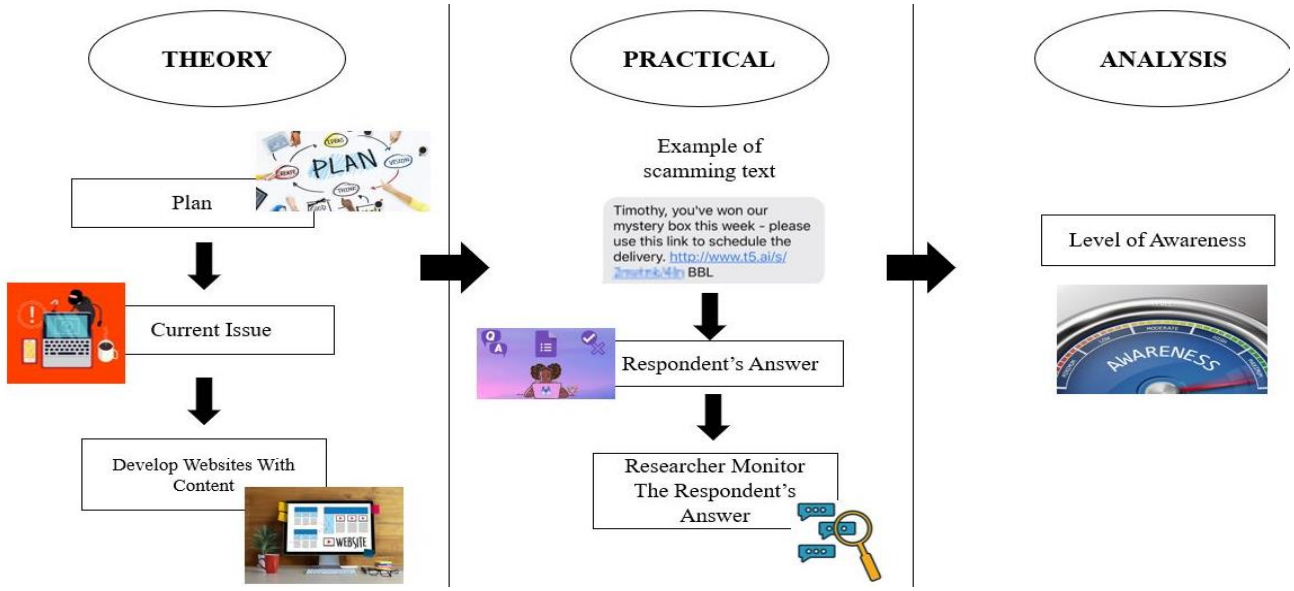

Fig. 1. The synergistic cyber security awareness model for the elderly (SCSAM-Elderly) [2]

1.2.5 The elderly's learning styles

Ramadhani *et al.,* [25] has highlighted that people's learning styles are defined by how they record, organize, and process information in their brains and minds. The elderly learn and process information in a very different way than younger people, so their way of learning is not the same. This may occur due to age-related concerns, a decline in cognitive ability, and physical limitations such as vision and hearing impairment [24]. Educational videos are provided based on visual and audio compatibility to increase knowledge and enjoyment of watching educational videos. Hence, there is no single learning method that an individual can fully adopt. Usually, a combination of one learning style with others will lead to intelligence and productivity. According to Mora *et al.,* [26], the elderly prefer images over sounds when learning and they also prefer to go step by step when solving problems. Besides, 55-to-65-year-old like to learn by doing, 66–74-year-old prefer watching and listening, while those 75 and above prefer to learn by watching and listening but also by thinking [27]. Visual learning style is a type of learning that makes greater use of vision and is well suited to the elderly who have hearing difficulties. However, when creating videos for the elderly, it is important to look at the changes and declines in sensory functions such as vision, hearing, and memory that occur as they age.

Furthermore, these changes affect the absorption of colours in the light entering the eye. Because aging eyes lose their ability to distinguish pale colours, yellows, and other pastels appear white. They also cannot distinguish between the colours blue, green, and purple, because these cooler colours appear as grey. Seniors who have colour vision problems can see bright colours at the warm end of the spectrum, such as reds and oranges [28]. Hence, the selection of the correct colour is essential. There are equipment and technology available to aid those who are colour-blind and find it difficult to complete routine chores such as wearing glasses and contact lenses. People who are colour-blind may be able to distinguish between colours with the use of special lenses and glasses. Second, visual aids. In order to cope with colour blindness, you can use various technological tools, such as visual aids, applications, and other technological advancements. By tapping on a specific area of a photo taken with a mobile device, people can learn what colour it was [29].

With hearing impairment, the elderly may have trouble communicating in different situations and may feel left out, which can make them feel lonely. At the same time, hearing loss may make it

harder for the person to notice and understand what is going on around them [30]. Concerning the sound, the audio utilized in the video ought to likewise be contemplated, since it takes more elderly individuals longer to listen and grasp voices. Memory merits a similar idea.

2. Methodology

There are three steps involved in reviewing on cyber security awareness model and the elderly's learning styles. First, feasibility study. Second, analysis of the elderly's learning styles. Third, analysis of cyber security awareness models.

2.1 Feasibility Study

Firstly, a feasibility study and literature review are carried out in gathering updated data on cyber security awareness and education, by particularly focusing on any existing models and approaches in measuring awareness among the elderly. Moreover, this study focused on cyber security, the types of cybercrimes involving the elderly, the characteristics of the elderly being the main target of cybercrimes, the cyber security awareness models, and the learning styles of the elderly. The findings are summarized in Section 2.

2.2 Analysis of the Elderly's Learning Styles

Table 1 represents the analysis of the learning style for the elderly based on the literature review covered in the first step. The elderly impairment or impediment is selected as the fundamental criteria that must be viewed in recognizing the learning styles [24]. This is significant particularly in the researcher's designing or developing stage of the materials planned for the elderly. The elderly's impairments are classified into six (6) which are vision for colour and sharpness, hearing, mobility or physical or movement, slow process of information, and speech. The learning styles that are viewed in this study did exclude the methodologies within written materials like books or flyers. However, the study did not include methods used in printed materials such as books or brochures.

Table 1
The analysis of the elderly's learning styles

Elderly's impairment/disability	Methods of learning styles
Vision (colour) [24]	Materials such as videos and website designed learning materials with the right colours
Vision (sharpness) [24]	Video with clear audio
Hearing [24]	Materials for learning styles designed with videos, images, and texts
Mobility/ physical/movement [24]	Using digital devices with designed learning materials
Slow process the information [24]	• Fun activities with friends • A simple poster, video and website with less sentences and appropriately designed learning materials
Speech	• Use melodic intonations when dealing with words that cannot be spoken or understood by the elderly • Speak louder than normal if the elderly have difficulties of hearing • Use body language to emphasize the point if the elderly have eyesight problems

2.3 Analysis of Cyber Security Awareness Model for the Elderly

The third step was the analysis of the existing cyber security awareness models that are suitable for the elderly. Section 4 presents the comparison of the existing cyber security awareness models for the elderly, together with the phases, validity, and technicality, which are depicted in Table 2.

3. Analysis

Table 2 shows the analysis of the cyber security awareness models, phases, validity, technicality, and components. Seven existing cyber security awareness models suitable for the elderly have been chosen. These phases are selected in order to identify the number of phases of the model that have been implemented. Besides, the validity was selected to identify whether a survey or expert had validated the model. In addition, technicality is also selected in the analysis to identify the level of technicality of the elderly. Meanwhile, the theory, practice, and analysis components are also analysed to determine whether these components are implemented in these models in order to educate and spread cyber security awareness among the elderly. Meanwhile, the theory is defined as providing a theory for each cybercrime topic or other related topics, while practical means preparing questions or practice to measure the elderly's understanding of the theoretical component. At the same time, an analysis is prepared to measure the level of awareness among the elderly, whether it has increased or not.

Table 2 shows that the ISACM is suitable for the elderly since this model provides theory and practice for the elderly to learn. The ISACM model implements three phases: awareness importance, awareness capability, and awareness risk. Additionally, questionnaire surveys and security expert has not validated the ISACM model. For technicality, this model is not technical for the elderly. However, this model is suitable for the elderly who work in an organization.

Meanwhile, ISAPM has six phases: identifying goals, designing, developing, implementing, measuring, and reviewing. The ISAPM model was verified by surveying the participants, and no technical steps have been implemented. However, this model is suitable for seniors working in organizations because the implementation of the website has been integrated with the organization's website. For the component, ISAPM only implements and provides theoretical and analytical components.

Besides, the security awareness model has six phases: strategic, tactical, preparation, delivery, monitoring, and resources. The security awareness model was validated by surveys, and no technical step was used. A survey by the elite validated this model but not by the participants. The components provided in this model are theory and analysis.

In addition, the peer education model has two phases: briefing and evaluation. However, this model is not validated by surveys and experts. The peer education model is suitable for the elderly, and it is not technical as it is conducted by peers. The components provided in this model are theory and analysis.

Meanwhile, OSICSAM has six phases: identifying goals, organizing, designing, developing, implementing, maintaining, measuring, and reviewing the awareness program. OSICSAM model is not technical and thus is suitable for society, organizations, and individuals who are still working in organizations among the elderly. However, this model has not been validated by survey questions and experts. The components provided in this model are practical and analytic.

Table 2
The analysis of cyber security awareness models, phases, validity, and technicality

Cyber security awareness models	Phases	Validity (survey / expert)	Technicality	Components Theory	Theory	Theory
Information security awareness capability model (ISACM) [24, 8]	Three phases: 1. Awareness importance 2. Awareness capability 3. Awareness risk	×	Not technical	✓	✓	×
Information security awareness program (ISAPM) general model [24, 19]	Six phases: 1. Identifying goals 2. Designing 3. Developing 4. Implementing 5. Measuring 6. Reviewing	Survey	Not technical	✓	×	✓
Security awareness model [24, 21]	Six phases: 1. Strategic 2. Tactical 3. Preparation 4. Delivery 5. Monitoring 6. Resources	Survey	Not technical	✓	×	✓
Peer education model [24, 23]	Two phases: 1. Briefing 2. Evaluating	×	Not technical	✓	×	✓
Organization, social and individual cyber security awareness model (OSICSAM) [24]	Seven phases: 1. Identifying goals organization 2. Designing 3. Developing 4. Implementing 5. Maintaining 6. Measuring 7. Reviewing	×	Not technical	×	✓	✓
Cybersecurity awareness framework for the elderly [4]	Seven phases: 1. Updating software 2. Patching device 3. Using strong password 4. Identifying current threats 5. Updating internet skills 6. Support system 7. Always sign out	×	Technical	×	✓	×
Synergistic cyber security awareness model for the elderly (SCSAM-Elderly) [2]	Three phases: 1. Theory 2. Practical 3. Analysis	Survey Expert	Not technical	✓	✓	✓

Additionally, the cybersecurity awareness framework for the elderly. This framework has seven phases or steps: updating software, patching the device, using a strong password and keeping it safe, identifying current threats and attacks, updating internet skills, supporting system, and always signing out. The cybersecurity awareness framework for the elderly is suitable for the elderly with an IT background because it implements the technical steps of computer sciences. However, this model does not gather the survey from participants and experts to validate the effectiveness model. The component provided in this model is practical.

Last but not least, SCSAM-Elderly contains three phases: theory, practice, and analysis, which are easier to implement. The SCSAM-Elderly model is suitable for the elderly because no technical step is implemented. SCSAM-Elderly has launched a website as a platform to provide information related to current cyber security issues to the elderly. In addition, SCSAM-Elderly has been validated by surveys among the elderly and has been validated by the cyber security expert. The components provided in this model are theory, practical, and analysis.

Therefore, based on the analyses, three cyber security awareness models are not chosen due to their incompatibility for the elderly. First is situation awareness-oriented cyber security education as it implements technical steps with high-end computer science vocabulary items as well as involves hands-on lab activities. Second is the cybersecurity awareness framework for the elderly which implements technical steps with high-end computer science. Third is cyber security capability maturity model as it is too difficult and technical to apply the suggestion made by this model, which states any model development program must align with the organization and national cyber security goals.

4. Conclusion

In conclusion, this paper has discussed existing cybersecurity awareness models suitable for the elderly and methods that can prevent them from being cyber-attacked while improving their awareness. This study also reviewed the learning styles of the elderly based on their weaknesses or limitations. After reviewing existing cybersecurity awareness models, the synergistic cyber security awareness model for the elderly (SCSAM-Elderly) was found to be the most suitable model for educating the elderly. The SCSAM-Elderly model was chosen because it is not technical, validated by surveys and experts, has practical components such as theory and analysis, and is suitable for educating and spreading awareness on current cyber-attack issues related to the elderly. Since the COVID-19 pandemic, almost all seniors are using technology such as mobile phones, making it crucial to spread cybersecurity awareness, especially among seniors who may lack understanding of cybersecurity issues or the prevalence of cybercrimes. This study's findings can help organizations, agencies, governments, and universities identify the best models that suit their needs and goals to educate about cybersecurity awareness related to cybercrimes and cyber-attacks among the elderly.

Acknowledgement

Our sincere appreciation goes to Kementerian Pengajian 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.

References

[1] Blackwood-Brown, Carlene Gail. "An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills." PhD diss., Nova Southeastern University, 2018.

[2] Azam, Nurul Alieyah, Alya Geogiana Buja, Mohamad Yusof Darus, and Nor Masri Sahri. "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)*, pp. 117-122. IEEE, 2022. https://doi.org/10.1109/ISCAIE54458.2022.9794521

[3] Rahman, Nurul Amirah Abdul, Izzah Hanis Sairi, Nurul Akma M. Zizi, and Fariza Khalid. "The importance of cybersecurity education in school." *International Journal of Information and Education Technology* 10, no. 5 (2020): 378-382. https://doi.org/10.18178/ijiet.2020.10.5.1393

[4] Zulkipli, Nurul Huda Nik. "Synthesizing cybersecurity issues and challenges for the elderly." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12, no. 5 (2021): 1775-1781. https://doi.org/10.17762/turcomat.v12i5.2180
[5] CyberSecurity Malaysia, "MyCERT : Incident Statistics - Reported Incidents based on General Incident Classification Statistics 2022." In *Malaysia Computer Emergency Response Team (MyCERT).*
[6] Department of Statistics Malaysia, "Demographic Statistics Fourth Quarter 2022, Malaysia." In *Department of Statistics Malaysia Official Portal* (2023).
[7] Crane, Casey. "3 Cyber Fraud Tactics Targeting Seniors and Why They're So Effective." In *Cybecrime Magazine* (2019).
[8] Mahajan, Rishab, and Mansirat Kaur. "A Review on Cyber Security and Its Threats." (2021).
[9] FBI's Internet Crime Complaint Center (IC3), "Elder Fraud Report 2021." In *Federal Bureau of Investigation* (2021).
[10] Kristen Setera, "FBI Warns Public to Beware of Tech Support Scammers Targeting Financial Accounts Using Remote Desktop Software." *Federal Bureau of Investigation* (2022).
[11] Li, Yuan, Adel Yazdanmehr, Jingguo Wang, and H. Raghav Rao. "Responding to identity theft: A victimization perspective." *Decision Support Systems* 121 (2019): 13-24. https://doi.org/10.1016/j.dss.2019.04.002
[12] Jonathan Skrmetti, "What You Need to Know about Investment Scams." In *Tennessee Attorney General*.
[13] DeLiema, Marguerite. "Elder fraud and financial exploitation: Application of routine activity theory." *The Gerontologist* 58, no. 4 (2018): 706-718. https://doi.org/10.1093/geront/gnw258
[14] Gloag, Andrew, and Polly Mackenzie. "Protected by Design." (2019).
[15] Burton, Alexandra, Claudia Cooper, Ayesha Dar, Lucy Mathews, and Kartikeya Tripathi. "Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review." *Experimental gerontology* 159 (2022): 111678. https://doi.org/10.1016/j.exger.2021.111678
[16] Bolimos, Ioannis A., and Kim-Kwang Raymond Choo. "Online fraud offending within an Australian jurisdiction." *Journal of Financial Crime* 24, no. 2 (2017): 277-308. https://doi.org/10.1108/JFC-05-2016-0029
[17] Khando, Khando, Shang Gao, Sirajul M. Islam, and Ali Salman. "Enhancing employees information security awareness in private and public organisations: A systematic literature review." *Computers & security* 106 (2021): 102267. https://doi.org/10.1016/j.cose.2021.102267
[18] Poepjes, Robert, and Michael Lane. "The Development of An Information Security Awareness Capability Model (ISACM)." In *SECAU 2012 Congress*. 2012.
[19] Maqousi, Ali, Tatiana Balikhina, and Michael Mackay. "An effective method for information security awareness raising initiatives." *International Journal of Computer Science & Information Technology* 5, no. 2 (2013): 63. https://doi.org/10.5121/ijcsit.2013.5206
[20] The Department of Energy. "DOE Cybersecurity Strategy 2018-2020." ENERGY.GOV, Jun. 2018.
[21] Kortjan, Noluxolo, and Rossouw Von Solms. "A conceptual framework for cyber-security awareness and education in SA." *South African Computer Journal* 52, no. 1 (2014): 29-41. https://doi.org/10.18489/sacj.v52i0.201
[22] Dai, Jun. "Situation awareness-oriented cybersecurity education." In *2018 IEEE Frontiers in Education Conference (FIE)*, pp. 1-8. IEEE, 2018. https://doi.org/10.1109/FIE.2018.8658929
[23] Baldassarre, Maria Teresa, Vita Santa Barletta, Danilo Caivano, Domenico Raguseo, and Michele Scalera. "Teaching Cyber Security: The HACK-SPACE Integrated Model." In *ITASEC*. 2019.
[24] Buja, Alya Geogiana, Siti Daleela Mohd Wahid, Teh Faradilla Abdul Rahman, Noor Afni Deraman, Mohd Nor Hajar Hasrol Jono, and Azlan Abdul Aziz. "Development of organization, social and individual cyber security awareness model (OSICSAM) for the elderly." *International Journal of Advanced Technology and Engineering Exploration* 8, no. 76 (2021): 511. https://doi.org/10.19101/IJATEE.2020.762185
[25] Ramadhani, Aulia, Taufan Bramantoro, Fridaniyanti Khusnul Khotimah, Lintang Maudina Santosa, Nancy Cynthia Sudiartha, I. Ketut Brahma Pande Cakti Mudara, Widya Rizky Romadhona et al. "SEIMUT PERSIA: promoting dental and oral health care and physical performance in elderly." *Indonesian Journal of Dental Medicine* 3, no. 1 (2020): 10-12. https://doi.org/10.20473/ijdm.v3i1.2020.10-12
[26] Mora, Juan F., Isabel R. Quito, and Luis S. Sarmiento. "A case study of learning styles of older adults attending an English course." *Maskana* 8, no. 2 (2017): 1-15. https://doi.org/10.18537/mskn.08.02.01
[27] E. Truluck, Bradley C. Courtenay, Janet. "Learning style preferences among older adults." *Educational gerontology* 25, no. 3 (1999): 221-236. https://doi.org/10.1080/036012799267846
[28] B. Moore. "How color and design affect environments for the aging – AIA." In *The American Institute of Architects*. 2018.
[29] National Eye Institute. "Color Blindness." In *National Eye Institute*. 2019.
[30] Bulğurcu, Suphi, Irmak Uçak, Ayşegül Yönem, Evren Erkul, and Engin Çekin. "Hearing aid problems in elderly populations." *Ear, Nose & Throat Journal* 99, no. 5 (2020): 323-326. https://doi.org/10.1177/0145561319883526