Research Article

International Journal of Advanced Technology and Engineering Exploration, Vol 8(76)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2020.762185

Development of organization, social and individual cyber security awareness model (OSICSAM) for the elderly

Alya Geogiana Buja[1*], Siti Daleela Mohd Wahid[2], Teh Faradilla Abdul Rahman[3], Noor Afni Deraman[1], Mohd Nor Hajar Hasrol Jono[1] and Azlan Abdul Aziz[1]
Universiti Teknologi MARA Cawangan Melaka, Faculty of Computer & Mathematical Sciences, Malaysia[1]
Universiti Teknologi MARA Cawangan Melaka, Faculty of Business and Management, Malaysia[2]
Universiti Teknologi MARA Cawangan Selangor, Centre of Foundation Studies, Malaysia[3]

Received: 10-October-2020; Revised: 15-March-2021; Accepted: 17-March-2021

Abstract

This paper proposes a cyber security awareness model for the elderly. The massive use of internet has led towards cybercriminals like scamming, fraud, hacking and cyber bullying. It has been reported that the number of cyber security incidents is increasing and among the affected group is the elderly. In line with the government initiative for cyber security, therefore, this study aims to develop a cyber security awareness model for the elderly. Firstly, a feasibility study was conducted and several literatures related to cyber security awareness and the elderly's learning styles were reviewed thoroughly. Secondly, based on the literatures, the existing cyber security awareness models were analyzed by identifying the approaches used. Thirdly, the learning styles of the elderly were studied based on the elderly's impairments and concerns. Finally, the cyber security awareness models were mapped to the elderly's learning styles. Based on the mapping results, a cyber security awareness model has been developed for the elderly based on the Information Security Awareness Capability Model (ISACM), Information Security Awareness Program (ISAPM) General Model, Peer Education Model, and Security Awareness Model. The expected result of this study is a cyber security model consists of the involvement of organization, social and individual factors that are important in creating cyber security awareness for the elderly. Further works are recommended to analyse the effectiveness of the proposed model towards the elderly and experts' reviews are required.

Keywords

Adult, Cyber-attack, Cyber security, Peer education, Structural equation, Modelling.

1.Introduction

In Malaysia, the percentage of senior citizens had increased from 7.9% in 2010 to 9.5% in 2015 [1] and this is projected to continuously grow to 17.4% in 2035 and 19.8% in 2040. As the fertility rate and mortality rate are reducing while life expectancy rate is increasing, it was projected that 50.9% of female citizens' life expectancy to be 77.2 years whereas 49.1% of male citizens could live to 72.6 years. Senior citizens mostly have the same forms of physical limitations such as problems with vision, hearing, or mobility. Therefore, the Society 5.0 comes into place to develop strategies, tools, and recommendations to assist this group of people to have a healthy and independent life for as long as possible [2].

The solutions are to remotely provide medical care services, connect and share information between medical data as well as using the Artificial Intelligence (AI) and robots at nursing-care centres to support elderly's independence.

The advanced growth of communication technology today has greatly brought benefits in many ways but it is indirectly led to the exposure of data privacy and safety of end users to the outsiders. The elderly group, the most affected as Malaysians nowadays in the transition moving towards Society 5.0; a human-centered society that highly integrates cyberspace and physical space. There is zero trust in the cyberspace

*Author for correspondence

This work was supported by Universiti Teknologi MARA Cawangan Melaka under TEJA: Internal Grant (GDT2020-20).

which is unable to assure the safety of the users from becoming cybercrime victims such as fraud and scam. This can be seen from statistical data published by Malaysian Communications and Multimedia Commission (MCMC) that showed the pattern of cybercrime in this country is increasing from time to time. Government had launched several cyber education campaigns to provide continuous awareness among the society. However, the safety of the elderly in the cyberspace is now became a serious attention among the cyber security community. Therefore, this study would like to investigate further on cyber security education model that can suit the needs required by the elderly for IR4.0 readiness in Malaysia.

Lack of a shared framework found from different literature for cyber security as an educational discipline has brought to unfocused growth without any common body of knowledge or understanding of degrees and educational outcomes [3]. Moreover, the current literatures provide empirical guidelines on building educational cyber security model and implementation on existing cyber security awareness model; however, there have been little studies focusing on building educational model of cyber security and awareness for the elderly. Therefore, this study aims to develop a cyber security awareness model for the elderly.

Based on past studies that have been conducted thoroughly on the existing cyber security awareness and education models, it is found that the existing models are mostly designed for general groups of users such as Situation Awareness-Oriented Cyber Security Education [4] and The Hack-Space Integrated Model [5], which are too technical for senior citizens' cyber security education with high-end computer science vocabularies. In addition, Security Awareness Model [6], Information Security Awareness Capability Model (ISACM) [7], and Cyber Security Awareness Strategy [8] provide guidelines on how to develop awareness programs but the implementation of these models is not clearly defined especially in educating the senior citizens. The characteristics for a cyber security awareness and education model include the internal organization, setup, arrangement, target participants and relevance of security model which give some ideas to researchers on how to develop an education model for the elderly. Besides, Cyber Security Capability Maturity Model [9] suggests that any model development must match with the organizational and national cyber security goal; nonetheless, this model does not include the element of education for the elderly. Meanwhile, the Information Security Awareness Program (ISAPM) General Model [10] focuses on achieving a large number of audiences by delivering their modules on their website.

This study considers and proposes the combination of the Information Security Awareness Capability Model (ISACM), Information Security Awareness Program (ISAPM) General Model, Peer Education Model and Security Awareness Model in constructing a cyber security awareness model for the elderly. Therefore, the objectives of this study are i) to identify the constructs of the cyber security awareness model for the elderly and ii) to develop the cyber security awareness model for the elderly. Section 2 describes related literatures that have been reviewed for this study, including the existing cyber security awareness models and the elderly's learning styles. The research methodology for this study is presented in Section 3. The results of this study are presented in Section 4 and have been discussed in Section 5. Finally, this paper concludes and presents the future works of the study in Section 6.

2.Literature review

This section discusses the related literature on the existing cyber security awareness education models and the elderly's learning styles.

2.1Situation awareness-oriented cyber security education

A cyber security education curriculum has been developed for university students [4]. The approach was based on Situation knowledge Reference Model (SKRM) which captures the students' awareness on the cyber security situations. In the proposed curriculum, several hands-on lab activities that represent real-world cyber problems are introduced to bring the conceptual knowledge unit. There are four modules in the proposed curriculum: research module, lab module, situation awareness module and presentation module.

In the research module, it mainly entails students to discover the supporting materials online. This is to encourage students to examine cyber-attack incidents in the future by themselves. The supporting materials can be cyber-attack scenarios and business workflow. In its lab module, it emphasizes on hands-on lab activities such as exposing students to malware patterns, unauthorized access and possible countermeasure. This is the best practice to let students learn and experience by themselves on the real-world cyber-attack.

In the situation awareness module, students are required to generate graphs from the lab module. The graphs can be either in the form of a network topology graph or attack graph. From these graphs, students are able to visualize the different interconnections between them and find a solution. Finally, the presentation module is a phase where students display their communication skills in telling or writing the situational knowledge they have learned based on the identified cyber-attack incidents.

2.2Peer education model

Being competent in operating computer-based tasks is insufficient to justify that the individual is safe while carrying out online-related tasks or activities. In relation to this, little awareness and knowledge about cybercrime and security can lead elderly users to fall victim to fraud and other cybercrimes. In Australia, various initiatives have been implemented to help the elderly learn about using the Internet safely which are done by private and public libraries, senior clubs and church groups aiming to bring up their skills while surfing online. According to [5], firstly, it had been reported that elderly people prefer to learn on how to be safe online through their peers. Many senior groups carried out lessons to teach their same age group peers whereby those who were initially hesitant to learn about computer and Internet would see their peers able to do well after taking some lessons, and eventually gained confidence that they too can do it—consequently, they then signed up for the next class.

Secondly, the report explained on the teaching delivery speed. For example, when an elderly user was taught by a younger instructor about cyber safety, the lesson was found to be delivered too fast that they could not keep up. However, when the content was delivered by their peers from the same age group, the speed was much slower and they felt motivated to use the computer and internet as they were taught at their own pace whereby they have a higher chance to succeed. This is just the starting point for them to familiarize with the technology. Once they are confident to use the Internet, they would likely to ask their children or grandchildren when any problem persists.

COTA New South Wales [9, 10], Australia has been implementing peer education model in their program for elderly people to learn about information technology. Each session using Peer Education model conducted by COTA is about a one-hour information session including 50 minutes of discussion and 10 minutes of evaluation. The lesson is presented by a skilled COTA volunteer peer personnel and suitable for a group of 10- 25 participants at a time. At the end of the session, both peer educator and the participants are required to evaluate every information session. Researchers who want to gain community understanding in cyber security were recommended to have few steps in their guideline [11].

2.3Security awareness model

A cyber security awareness framework and education was proposed for South Africa to portray cyber-safe practices among South Africans and Internet users [12]. The framework consists of five layers and one module which are strategic layer, tactical layer, preparation layer, delivery layer, monitoring layer and resources. Each layer is defined as the following:

- Strategic Layer

This layer follows the vision of the government on cyber security awareness and education. The vision can be found in the South Africa cyber security policy that includes the cyber security culture. The first step in this layer is to identify the objectives of cyber security in the National Cyber Security Policy. Secondly, to form the responsible unit to spread the awareness education through new administrations and collaborations with several government departments and some private organizations. After the responsible unit has decided on the new administrations and collaborations, a strategic plan should be drafted that explains the approaches of cyber security awareness and how to educate people in South Africa about their online safety.

- Tactical Layer

The tactical layer is a continuation from the previous level. It consists of four components. Firstly, conducting campaigns in collaboration with private sector, academia and government bodies. The collaboration is aimed at helping to increase cyber security levels. Secondly, the framework targets campaigns run at school level, community, cyber security education for all, and through weekly campaigns.

- Preparation Layer

This level outlines the cyber security awareness and educational resources for the campaigns mentioned in the previous level. There are 4 components to the topic, content, platform, and equipment. Some related topics are identified, but are not limited, to fraud, cyber-bullying, identity theft, phishing, securing personal data and importance of sharing private information online.

- Delivery Layer

This layer considers the ways of identifying target audience to which the campaign will spread the awareness and education. Nonetheless, this level also outlines the responsibilities of each audience to themselves and to each other, namely learners' role and educators' role. After the lesson has come to the fore, students need to teach others and take on the role of educators. This is to ensure that the benefits of knowledge can be conveyed continuously.

- Monitoring Layer

In the monitoring layer, in order to evaluate whether the campaign is successful, monitoring and analysis are necessary. The findings of this campaign are from the participants' and volunteers' feedback. The framework proposes that an evaluation should be based on a set of standards, indicators of excellence and a timely report should be produced.

2.4An information security awareness capability model (ISACM)

A model of information security awareness capability is developed based on several theories combining the aspect of information security's best practices and security's awareness theory [13]. The design of ISACM comprises of three key features in which all these features are according to the controls listed within the ISO/IEC 27002. The first feature is the awareness importance, in which people's awareness about cyber security control will influence the process of successfully avoiding themselves from being a scam victim. The second key feature is awareness capability, which refers to how capable a person when dealing with a problem. For example, how a person is capable to understand the types, characteristics and situations of a scam activity. This understanding could influence the rate of successful scam avoiding. Last but not least, the awareness risk which looks into the gap between the amounts of awareness importance being bigger than the amount portrayed by a person (awareness capability). The following describes the development of ISCAM which consists of five stages.

- Identifying a strong fundamental knowledge.
- Determining the detailed awareness points that could be rated.
- Altering the detailed awareness point to a practical level.
- Developing the survey items to collect awareness importance ratings.
- Establishing the rest of the model: Cyber Security Awareness (CSA) Strategy

A focused group discussion was conducted to collect information on the suggestion of cyber security awareness programs [8]. As a result, the researchers proposed an implantation structure that has three layers which are Strategic, Program Execution, and Content Development. The first is the strategic layer, which refers to the CSA's vision and how the plan is implemented. The national CSA forum is responsible for planning, strategizing and looking at the overall direction of CSA initiatives. The forum is collaboration among government bodies, the private sector, community organizations and experts from related industries to deliver the program contents in better ways to the target groups.

The second layer is the execution layer. The main purpose of this section is to provide a process that can be used to gather information and disseminate contents to the right target group. One of them is to use agencies and organizations as pathways to deliver awareness messages about cyber security. The third layer is content development layer which plays a role to identify the most effective materials and contents of cyber security awareness for the targeted group of participants. Although it is using the same topics of awareness, a responsible developer must understand that different materials are needed to reach different types of participants.

2.5Cyber security capability maturity model

This model allows nations, organizations or other entities to evaluate its current cyber security capacity. The objective of this model is to identify various ranges of level of capacity capability that might be found, if an organization was found to implement something at the lowest level, of which it indicates that non-existent or limited level of capacity whereas the highest indicates that both strategic method and an ability to optimize operational, threat, socio-technical and political [9].

This model defines five levels of scales; (1) start-up level is the lowest level which indicates that the organization has not taken any action to create cyber security awareness or it could be just initial discussion conducted with little evidence, (2) formative level which shows that some elements have started to grow and be formulated with clear evidence but may not be organized, weak in definition, (3) established level of which the components of the sub-factor are working but there is less consideration of the relative distribution of resources, (4) strategic level indicates that the company has made a decision on which element is important and less important for the organization, and (5) dynamic level indicates that the company already has a clear plan in the way to modify the strategies depending on fundamental conditions. Dynamic organizations have successfully established its approach for changing strategy including fast decision making, reform resources and give consistent attention to the changing environments.

2.6Information security awareness program (ISAPM) general model

A project that spreads awareness and education on cyber security through web system is done in order to educate users through the company's website which could drive to continuous education. In addition, it is the best way to reach out a bigger audience because the employees and students in the organization are the main users of the website [10]. This model is developed by taking into account the findings of the consumer education concept. Any organization wishing to run an awareness program should first learn about the goals of cyber security in the organization.

Firstly, the organizations need to identify what they want to achieve in cyber security within the company. Secondly, the design stage is focusing on identifying the needed program platform that is required for the security awareness program. Thirdly, the development stage is focusing on developing the website using programming languages. This development depends on the financial and human resources that are available in the company. The next stage is implementation where the organization chooses one out of the three ways to organize the program which is either to put it on the organization's website, or at the administrative tool menu, or on separate websites. The researchers recommend that developers post the program on the organization's website as it is much easier to be accessible to all users within the organization.

2.7The elderly's learning styles

The elderly's learning and information processing styles are not similar with the younger generations. This may occur due to age-related concerns, declination in cognitive capabilities and physical limitation such as vision and hearing impairments. Therefore, in order to deliver and develop learning materials for the elderly, personalized learning and teaching methodologies are needed. This also means that a customized education has to be there in helping the elderly [14]. Other researchers suggested in their studies that the use of digital tablets may help the elderly learn because they have to be connected, independent and autonomous [15].

Moreover, there is a program called the Elderly Empowerment Program conducted by a group of researchers with the objective of assessing whether the video can be used to provide the knowledge to the elderly effectively [16]. The program used three aspects of assessments; oral health education and physical performance education contents, appealing visual contents as well as easily-understandable video contents. According to the researchers, the elderly has difficulties in retrieving the knowledge from books and modules due to the declining capabilities because of aging-related illnesses [14]. The elderly prefers some activities together with their friends.

As a result of the program, too, an innovation was produced whereby educational videos were made based on visual and audio suitability to increase understanding and interest in watching educational videos. Visual learning style is a learning style that uses more vision and is suitable for parents with hearing problems. However, in making educational videos for the elderly, it is important to pay attention to the changes and decreased sense of functions, for example in vision, hearing, and memory. In vision, there is a decrease in vision ability so the elderly tends to use glasses as an aiding tool. In addition, these changes affect the absorption of colours on the light entering the eye. The elderly has the tendency to experience difficulties to distinguish colours, especially blue, green, and purple. Therefore, the right colour selection is important. As for the audio, the voice used in the video also needs to be considered as the elderly takes longer time to listen clearly and process incoming voices. The same consideration goes to memory [16].

3.Methods

There are four phases involved in developing the Organization, Social, and Individual Cyber Security Awareness Model (OSICSAM) namely feasibility study, Analysis of Existing Cyber Security Awareness Model, Analysis of the Elderly's Learning Style and Development of Organization, Social and

Individual Cyber Security Awareness Model (OSICSAM).

3.1Feasibility study

A literature review and feasibility study were undertaken to discover the current state of information security awareness and education, with a focus on discovering what if any methodologies, models and tools were available to measure awareness among the elderly. In addition, the elderly's learning styles were also studied. Section 2 presents all related literatures that were reviewed during this phase.

3.2Analysis of the existing cyber security awareness models

The existing cyber security awareness models were analysed based on the characteristics and implementation of the model. To have a clearer view of each model, the cyber security awareness models are summarized in terms of the approach used for delivering the messages of awareness. *Table 1* shows the comparison analysis of the existing cyber security awareness models.

Table 1 The comparison analysis of the existing cyber security awareness models

No	Cyber security awareness models	Approach for delivering the awareness
1	Situation Awareness-Oriented Cyber Security Education [4]	Conducting hands-on lab, suitable for the younger generation
2	Peer Education Model [5]	In groups with the same age
3	Security Awareness Model [6]	Conducting campaigns, focuses on the topics of cyber security and facilitated
4	Information Security Awareness Capability Model (ISACM) [7]	Conducting survey, organizing forum with experts, developing suitable materials for targeted group
5	Cyber Security Capability Maturity Model [9]	Suitable for large organizations, involves discussions, planning and resource distribution, too technical
6	Information Security Awareness Program (ISAPM) General Model [10]	Using web systems to disseminate information on cyber security awareness

3.3Analysis of the elderly's learning styles

Based on the literature studied in the first phase, the analysis of the elderly's learning styles [14, 15, 16] is presented in *Table 2.* The elderly's impairments or problem limitations are chosen as the main criteria that has to be considered in identifying the learning styles. This is important especially when it comes to the stages of designing or developing the materials for the elderly. The elderly's impairments are categorized into five (5) which are vision (colour), vision (sharpness), hearing, physical or movement and slow in processing information. The learning styles that are considered in this study did not include the approaches within written materials such as books or flyers. The learning styles are labelled as LS1 until LS5.

Table 2 The analysis of the elderly's learning styles

No	Elderly's impairment / limitation	Learning Style ID	Learning style
1	Vision (Colour)	LS1	Materials such as videos with appropriately designed learning materials (colour selection) and clear audio
2	Vision (Sharpness)	LS2	Videos with clear audio
3	Hearing	LS3	Materials with videos and images
4	Physical / movement	LS4	Using digital devices with appropriately designed learning materials
5	Slow in Processing the Information	LS5	✓Fun activities with friends ✓Simple videos with appropriately designed learning materials (less sentences)

3.4Development of organization, social, and individual cyber security awareness model (OSICSAM)

In order to develop the Organization, Social and Individual Cyber Security Awareness Model (OSICSAM), the cyber security awareness model was mapped to the elderly's learning styles. Based on *Table 3*, the Information Security Awareness Capability Model (ISACM), Information Security Awareness Program (ISAPM) General Model, Peer Education Model and Security Awareness Model were chosen as the components of the OSICSAM (refer *Figure 1*).

Table 3 The mapping of cyber security learning models and the elderly's learning styles

Cyber security awareness models	Learning styles				
	LS1	LS2	LS3	LS4	LS5
Situation Awareness-Oriented Cyber Security Education [4]					
Peer Education Model [5]	√	√	√	√	√
Security Awareness Model [6]	√	√	√	√	√
Information Security Awareness Capability Model (ISACM) [7]	√	√	√	√	√
Cyber Security Capability Maturity Model [9]					
Information Security Awareness Program (ISAPM) General Model [10]	√	√	√	√	√

4.Results

The Organization, Social, and Individual Cyber Security Awareness Model (OSICSAM) is designed based on the mapping analysis of the existing cyber security awareness models and the elderly's learning styles as presented in *Table 3*. *Figure 1* shows the development of the proposed model that composed of organization, social, individual and the cyber security awareness. The organization and the cyber security awareness are adopted based on the Information Security Awareness Program (ISAPM), Information Security Awareness Capability Model (ISACM) and Security Awareness Model. Meanwhile, the social and individual are representing the Peer Education Model. Brief discussion on the proposed model is discussed in Section 5.

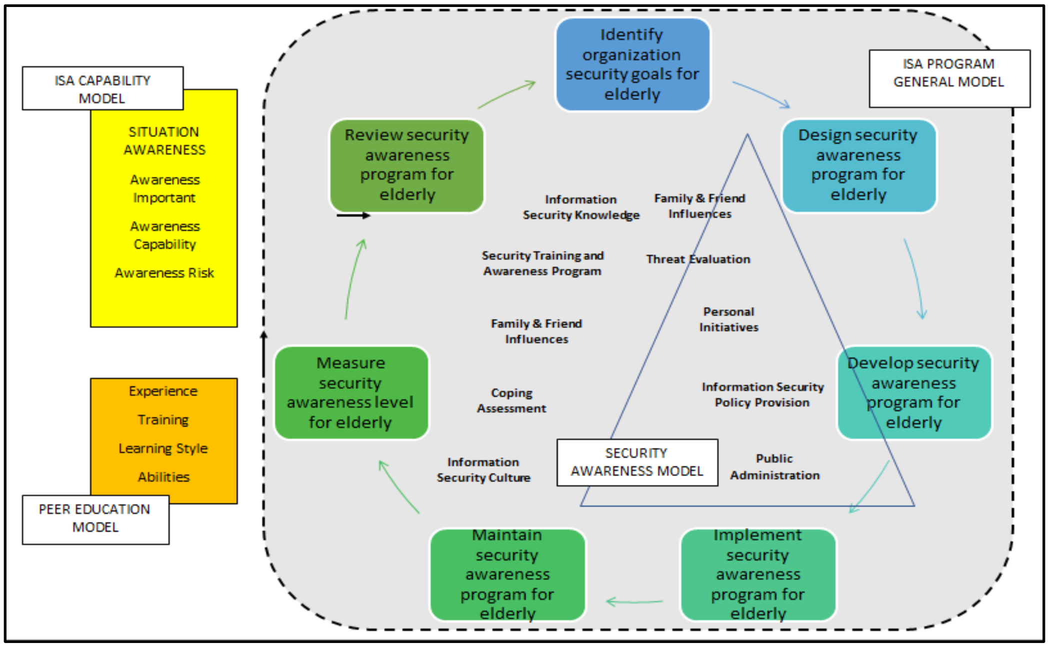
ISA CAPABILITY MODEL
SITUATION AWARENESS
Awareness Important
Awareness Capability
Awareness Risk
Experience
Training
Learning Style
Abilities
PEER EDUCATION MODEL
Identify organization security goals for elderly
ISA PROGRAM GENERAL MODEL
Review security awareness program for elderly
Design security awareness program for elderly
Information Security Knowledge
Family & Friend Influences
Security Training and Awareness Program
Threat Evaluation
Family & Friend Influences
Personal Initiatives
Measure security awareness level for elderly
Develop security awareness program for elderly
Coping Assessment
Information Security Policy Provision
Information Security Culture
SECURITY AWARENESS MODEL
Public Administration
Maintain security awareness program for elderly
Implement security awareness program for elderly

Figure 1 The development of organization, social and individual cyber security awareness model (OSICSAM)

5.Discussions

The organization is responsible in planning, developing and later disseminating the materials for cyber security awareness for the elderly. The organization's responsibilities are applied in all chosen existing cyber security awareness models used as guidelines in developing the OSICSAM. The social and individual are related to peer education. As applied in Peer Education Model, the awareness is created by having activities in a group of people of the same age. For the elderly, they will be more comfortable to learn together with their peers. The cyber security awareness focuses on the approaches and the awareness materials. This is related to the elderly's learning styles based on their impairments or limitations.

5.1Limitation

However, this study did not gather the reviews from the cyber security and the elderly education experts. The experts' point of views are very important to ensure that the propose model suits well the objective of the proposed model; to enhance the cyber security awareness among the elderly.

6.Conclusion and future work

This paper concludes that the proposed model can be used to improve the cyber security awareness among the elderly. With the involvement from the organization and social along with the individual elements in the developed model can synergize the cyber security awareness in the elderly. In future studies, the proposed model may be assessed further using both qualitative and quantitative approaches. A preliminary survey should be conducted on the elderly to obtain the awareness ratings and the information obtained which will be analysed further. The analysis is important in order to prepare appropriate cyber security awareness materials and suitable approaches that can be used for the execution. In addition, the experts' reviews are required to verify and validate the proposed model.

Acknowledgment

Sincere appreciation goes to Universiti Teknologi MARA Cawangan Melaka for the support given to this research endeavour, TEJA: Internal Grant (GDT2020-20).

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] https://www.kpwkm.gov.my/kpwkm/uploads/files/Muat%20Turun/MOST/S4_P1_Tuan%20Hj_%20Fazari.pdf. Accessed 20 September 2020.

[2] Wang S, Bolling K, Mao W, Reichstadt J, Jeste D, Kim HC, et al. Technology to support aging in place: older adults' perspectives. In Healthcare 2019 (p. 60). Multidisciplinary Digital Publishing Institute.

[3] Parrish A, Impagliazzo J, Raj RK, Santos H, Asghar MR, Jøsang A, et al. Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In proceedings companion of the ACM conference on innovation and technology in computer science education 2018 (pp. 36-54).

[4] Dai J. Situation awareness-oriented cybersecurity education. In IEEE frontiers in education conference 2018 (pp. 1-8). IEEE.

[5] Baldassarre MT, Santa Barletta V, Caivano D, Raguseo D, Scalera M. Teaching cyber security: the HACK-SPACE integrated model. In ITASEC 2019:1-13.

[6] Kortjan N, Von Solms R. A conceptual framework for cyber-security awareness and education in SA. South African Computer Journal. 2014; 52(1):29-41.

[7] Poepjes R, Lane M. An information security awareness capability model (ISACM). Australian information security management conference. 2012; (pp. 1-8).

[8] Yunos Z, Ab Hamid RS, Ahmad M. Development of a cyber security awareness strategy using focus group discussion. In SAI computing conference 2016 (pp. 1063-7). IEEE.

[9] https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf. Accessed 20 September 2020.

[10] Maqousi A, Balikhina T, Mackay M. An effective method for information security awareness raising initiatives. International Journal of Computer Science & Information Technology. 2013; 5(2):63-72.

[11] https://cltc.berkeley.edu/wp-content/uploads/2019/04/CLTC_Underserved_Populations.pdf. Accessed 20 September 2020.

[12] https://www.cotansw.com.au/MediaPDFs/Peer%20Education%20-%20Group%20Organiser%20Info%20Sheet.pdf. Accessed 20 September 2020.

[13] https://humanrights.gov.au/our-work/legal/inquiry-cybersafety-senior-australians-2012. Accessed 20 September 2020.

[14] Teets C, Grimes K. Assessment of learning styles and learning retention among the elderly population in Frankfort, Kentucky. Kentucky State University. 2019.

[15] Gatti FM, Brivio E, Galimberti C. "The future is ours too": a training process to enable the learning perception and increase self-efficacy in the use of tablets in the elderly. Educational Gerontology. 2017; 43(4):209-24.

[16] Ramadhani A, Bramantoro T, Khotimah FK, Santosa LM, Sudiartha NC, Mudara IK, et al. SEIMUT PERSIA: promoting dental and oral health care and physical performance in elderly. Indonesian Journal of Dental Medicine. 2020; 3(1):10-12.

Alya Geogiana Buja is a Senior Lecturer at the Faculty of Computer and Mathematical Sciences in Universiti Teknologi MARA (UiTM) Cawangan Melaka. She is a PhD holder in the field of Information Security and graduated from Universiti Teknikal Malaysia Melaka (UTEM), MSc in Computer Science and BSc in Netcentric Computing from Universiti Teknologi MARA (UiTM). Her research interests are Networking and Information Security, Cryptanalysis and Cyber Security.
Email: geogiana@uitm.edu.my

Siti Daleela Mohd Wahid is a senior lecturer at Faculty of Business Management, Universiti Teknologi MARA (UiTM) Cawangan Melaka. She is a PhD holder in the field of social entrepreneurship and graduated from The National University of Malaysia. Her research interests are Social Innovation, Social Entrepreneurship, and Elderly Innovation.
Email: sitid365@uitm.edu.my

Teh Faradilla Abdul Rahman is a Senior Lecturer at the Centre of Foundation Studies in Universiti Teknologi MARA (UiTM) Dengkil campus. She is currently doing a PhD in the field of Health Information System at Universiti Kebangsaan Malaysia (UKM). Her research interests are Health Information System, Mobile Therapy, and Topic Modelling.
Email: tehfaradilla@uitm.edu.my

Noor Afni Deraman is currently a lecturer at Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM) Melaka. She obtained her Bachelor’s degree in Computer Science majoring in Software Engineering from Universiti Sains Malaysia (USM). She completed her Master’s degree in Science (Computer Science) in 2006. Her research interest is in Data Science and Artificial Intelligence.
Email: noora465@uitm.edu.my

Mohd Nor Hajar Hasrol Bin Jono was born in 1978 in Klang, Selangor. He obtained his PhD in 2016. At present, he is working as a senior lecturer at the Faculty of Computer Science and Mathematics at Universiti Teknologi MARA (UiTM) Melaka, Malaysia. Now in the field of administration, he currently holds the position of Deputy Rector of Student Affairs UiTM Melaka. Previously, he was the Head of Training Division, Head of Systems Division and also Fellow at the i-Learn Center under the Academic Affairs Division, UiTM Shah Alam.
Email: hasrol@uitm.edu.my

Azlan Abdul Aziz is a senior lecturer at the Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM) Melaka. He is a PhD holder in the field of Multimedia Education and graduated from Universiti Pendidikan Sultan Idris (UPSI), Masters of Info. Tech. in Information Science and B.Ed TESL from Universiti Kebangsaan Malaysia (UKM). He has contributed in several researches, publication and innovation competitions both national and internationally. His research interests are in the area of e-Learning, Educational Technology, Adult Learner and Distance Education, Computer Science Education, Multimedia and Gamification.
Email: azlan225@uitm.edu.my