BSc cOMputing Project

Muhamade Ashif Muhamade Muhajireen

19165527

online User guide for senor citizens about cyber threats

Dissertation Course No:

Contents

[1. Glossary 3](#_Toc163690781)

[2. Abstract 3](#_Toc163690782)

[3. Acknowledgments 3](#_Toc163690783)

[4. Introduction 3](#_Toc163690784)

[4.1 Background of the Project 3](#_Toc163690785)

[4.2 Aims and Objectives 4](#_Toc163690786)

[4.3 Motivation 4](#_Toc163690787)

[4.4 Key Functions of Porect 5](#_Toc163690788)

[4.5 Product Overview 5](#_Toc163690789)

[5. Literature Review 5](#_Toc163690790)

[5.1 Introduction 5](#_Toc163690791)

[5.2 What is Cyber Crime? 5](#_Toc163690792)

[5.3 Why Are Seniors more Vulernable to Cybercrime? 6](#_Toc163690793)

[5.4 Cyber Issues and Challenges Among the sENIORS 7](#_Toc163690794)

[5.5 Reviews of Cyber-Attacks on the eLDERLY 8](#_Toc163690795)

[5.6 Conclusion 10](#_Toc163690796)

[6. METHODOLOGY 10](#_Toc163690797)

[7. RESULTS 10](#_Toc163690798)

[8. TESTING 10](#_Toc163690799)

[9. PROFESSIONAL ISSUES 10](#_Toc163690800)

[10. CONCLUSION 10](#_Toc163690801)

[11. REFLECTION 11](#_Toc163690802)

[12. APPENDICS OR IN NEW TABLE 11](#_Toc163690803)

# 1. Glossary

# 2. Abstract

# 3. Acknowledgments

# 4. Introduction

### 4.1 Background of the Project

The exponential growth of the internet almost 65% of the world’s population has transformed communication and access to information, changing the whole dynamics of the traditional way (Liaqat and Liaqat, 2021). However, this traditional landscape transformation also presents significant challenges, particular for senior citizens. As they increasingly embrace online activities like social media, online banking, online shopping, and e-commerce (Ruangkana and Kessuvan, 2019). The COVID-19 pandemic increased cyber risk for the elderly as physical distance forced them with greater reliance on digital networks where they had their needs to be met (Lee, Hoong Lee and Ean Catherine Lee, 2021).

The significant gap experienced by many seniors, who grew up in an era before the widespread adoption of smartphones and computers, has profound consequences for their vulnerability to cybercrimes (Aleksandrova, Khramova and Kurkin, 2018). This generation is relatively inexperienced with digital technology (Lee, Hoong Lee and Ean Catherine Lee, 2021), this makes them prime targets for cybercriminals and complicates their ability in identifying and cautiously responding to online threats effectively.

With the ease of internet usage comes a corresponding rise in cybercrime (Prasad and Pennington, 2020). Criminals exploit the trust and potentially lower technical awareness of new online users, like senior citizens. Statistics paint a concerning picture. In the United Kingdom (UK) alone, an estimated 5.5 million cybercrimes occur annually (Hull, Eze and Speakman, 2018). Alarmingly, law enforcement resources may be stretched thin, with only 12% of these incidents investigated by local forces (Hull, Eze and Speakman, 2018). This highlights the importance of personal cybersecurity measures, particularly for vulnerable populations like seniors. By understanding cyber threats and implementing basic security practices, senior citizens can significantly reduce their risk of falling victim to online scams and exploitation.

As adults age, certain cognitive functions associated with decisions-making and pattern recognition gradually declines in the ageing process (Murman, 2015) – this can make older users more vulnerable to online social engineering tactics that play on emotions like fear, urgency, and trust. Seniors may struggle to become aware distinguishing between legitimate communications and cybercriminal attempts, such as phishing by attempting to steal personal and financial information (Alieyah *et al.*, 2023). This emphases for an educational tool to help seniors use technology safely without falling into any traps, throwing away their trust towards technology.

### 4.2 Aims and Objectives

The primary aim of this project is to develop, an accessible, online user-friendly guide tailored for senior citizens, coded with HTML, CSS, PHP, and JavaScript. The guide will provide comprehensive instructions and support navigating through digital data, understanding internet safety, and preventing oneself from attacks. By incorporating interactive quizzes, the project not only intends to be educational but also to keep users engaged, ensuring they can practice and reinforce their learned knowledge with questions. The overall goal of this project is to enhance cybersecurity awareness and resilience among older adult demographics.

The following objectives will be performed in order to complete this project:

* **Literature Review** – Composing a literature review on seniors facing issues with cybercrimes.
* **Questionnaire** – Complete collecting data from senior members regarding cyber measures.
* **Extract Requirements** – Complete a list of functional, and non-functional requirements.
* **Creation of Questionnaires** – Collect data for older citizens for the creating of solution of the project.
* **Initial Designs of Webpages** – Complete wireframe designs of the user guide where it meets almost all the requirements and with data collected.
* **Design Interface and Functionality** – Complete the interface and functionality, where seniors would easily navigate around the website.
* **Develop the User Guide** – Completion of user guide meeting all requirements.
* **Testing** – Complete testing throughout the whole website to ensure effectiveness, and both the functional and non-functional requirements are met.
* **Evaluation** – Complete an evaluation upon completion of the project, and include any the process and improvements, also future plans.

### 4.3 Motivation

As discussed in section 4.1, the rapid growth of technology has enhanced our lives, and particularly the older adults. Although, cyber security awareness campaigns are common, a significant gap exists in addressing the specific main needs of senior citizens. The leading cause for this issue is the lack of accessible resources not only hold backs their ability to fully benefit from technology but also leaves them more vulnerable to online threats like phishing scams and financial exploitation. These attacks can have a devastating emotional and financial impact.

The proposed online user guide aims to bridge this gap by offering clear, concise instructions and engaging learning elements tailored for seniors. This will empower them to navigate the online world confidently and securely, maximizing the benefits of technology in their lives.

### 4.4 Key Functions of Project

These functions will be vital in the project:

1. Provide users with clear online materials that anyone with no background knowledge will understand.
2. Provide an engaging multiple-choice quizzes to assess users’ knowledge.
3. Provide a user interface which ensures it is enjoyable and seamless experience whilst navigating through the online user guide.
4. Online user guide provides accessibilities, such as text to video.

### 4.5 Product Overview

An online user guide accessible from the world wide web tailored to senior citizens, which can take advantage off, as the website will guide comprehensive resources to detect and prevent cybercrimes effectively. This guide will offer interactive quizzes which are bespoke designed for seniors, to evaluate users understanding and readiness to tackle cyber threats head-on. Features for this online user guide will be implemented from the literature review, and from the questionaries constructed and given out to senior citizens in order to retrieve relevant information needed in real time. This product not only will be helpful and expand their knowledge, but also aims to safeguard users from making the same mistakes again. Furthermore, our online user guide will come with a dedicated section for news, and blog posts regularly updated, delivering timely insights into the ever-evolving tactics by cybercriminals.

# 5. Literature Review

### 5.1 Introduction

This chapter focuses on the types of cybercrimes and an in-depth analysis of the common attacks targeted towards the senior citizens. The literature has indicated that older people are more vulnerable to cybercriminals from the use of sociotechnical strategies by cybercriminals. This chapter will provide an in-depth analysis of common attack methods targeting the elderly, with the likes of government impersonation, romance frauds, and phishing. It also focuses on the growing threat of ransomware and how it can be a real threat for the elderly. The information presented in this chapter will identify the major online safety risks that seniors are facing today, and by understanding them can lead to effective countermeasures.

\*\*WHAT IS AN ELDERLY\*\*

### 5.2 What is Cyber Crime?

Cybercrime is a term which captures a wide range of illegal activities conducted through the digital landscape, through computers or any modern technology which utilizes the internet (Arshey and Angel Viji, 2021). The definition of cybercrime might vary depending on the specific sort of cyberattack that has occurred. The universal nature of technology in our daily lives, from online banking to social media, creates vulnerabilities that cybercriminals exploit for personal gain. These crimes can target individuals, businesses, and even government institutions, resulting in financial losses, data breaches, and disruption of critical infrastructure (Bendovschi and Al-Nemrat, 2016).

The landscape of cybercrimes is influenced in many ways. Some research emphasises the opportunistic nature of cyber-attacks, where attackers exploit vulnerabilities in victims or leverage social engineering tactics to create them (Reuben *et al.*, 2023). The attacks take place strategically, waiting for opportunistic moment, such as gaining trust appearing as reputable company, social media, or public events to maximise their impact. In contrast other researchers argue that cybercrime isn't entirely novel, Peter N. Grabosky argues that cybercrime is a continuation of traditional criminal activities, with a simple modification of adopting new tools and techniques (Grabosky, 2001). This perspective highlights the underlying similarities between cybercrime and its physical-word counterparts. Criminals have always sought to exploit weaknesses and optimise financial gains, and the era of digital technology has just furnished them with even more fresh opportunities to accomplish this. Additionally, Greg Stratton supports this idea by examining the difficulties that conventional criminal justice systems encounter when trying to adjust to cybercrime (Stratton and Cameron, 2014). In addition, gaining insights to these ongoing patterns and behaviours can be advantageous in developing investigation methods to enhance the effectiveness of combating cybercrime (Thangiah, Basri and Sulaiman, 2012).

### 5.3 Why Are Seniors more Vulernable to Cybercrime?

Cybercrimes against the elder generation are escalating in both frequency and severity, presenting significant challenges to digital security and the wellbeing of older adults. According to the research conducted by (Narayanan *et al.*, 2021). Peter Lošonczi discusses how older individuals often utilise the internet for recreational purposes, communication, financial transactions, and public encounters, despite their limited understanding of computer terminology. Consequently, they are vulnerable to security threats that can strike unpredictably (Lošonczi, 2018). Another study also conduct that it has revealed that seniors are viable targets and are more fearful to crime (Riek, Böhme and Moore, 2016), as they are less tech savvy than the current generation, polite, trustworthy and susceptibility to heightened levels of cognitive decline (Fdic, 2021).

Dr. Vasileios Karagiannopoulos discusses a poll undertaken by Age UK, which found that 53% of the participants were victims of internet fraud, and that 1 in 12 individuals fell for the scam. Furthermore, 33% of those affected lost more than £1000 (Karagiannopoulos *et al.*, 2021). This alarming statistic underscores the vulnerability of older internet users to cybercriminals. The study emphasizes the need for enhanced digital literacy among this demographic, advocating for targeted educational programs that address the specific challenges and threats they face online (Javidi and Sheybani, 2018). Furthermore, seniors "generally lack the know-how for such fraudulent activities" highlighting the critical need for proactive measures to educate and protect this group from increasingly sophisticated cyber threats (Sugunaraj, Ramchandra and Ranganathan, 2022a).

Furthermore, cognitive decline associated with aging can exacerbate vulnerability. Studies by (Costilla-Reyes *et al.*, 2021) suggest that seniors may experience diminished cognitive abilities that affect their judgment and impulse control. This can make them more susceptible to falling for urgent requests (Sugunaraj, Ramchandra and Ranganathan, 2022a) or convincing narratives employed by cybercriminals. Additionally, some seniors might be hesitant to admit cognitive difficulties, further hindering their ability to recognize and respond to cyber threats effectively (Banovic, Zunic and Sinanovic, 2018).

### 5.4 Cyber Issues and Challenges Among the sENIORS

While internet usage among seniors is rapidly increasing over time with an increase of 41% between the years 2000 and 2016, showing strong growth over the next coming years (Hunsaker and Hargittai, 2018), their lack of digital literacy leaves them vulnerable (Oh *et al.*, 2021). The increase in number of senior users on the internet has triggered the need of investigating to understand the challenges, and attacks that are aimed towards the elderly. Several aspects from literature about the involvement of the elderly in cybercrime incidents are described under various headings as follows:

#### 5.4.1 Technology VS Age

Contrary to younger consumers, the majority of seniors experience the "grey digital divide" in the sense that they do not dedicate as much time to using the Internet (Rengamani *et al.*, 2010), resulting in a potential knowledge gap about online safety compared to younger individuals who were exposed to this technology from a young age. Due to their limited experience (Tilley, 2003), individuals may encounter difficulty in identifying and addressing online hazards independently. Johan Frishammar talks about the absence of self-assurance can provide challenges for certain elderly individuals where they get “scared” when it comes to carrying out crucial internet activities with adequate knowledge and security measures (Frishammar *et al.*, 2023). Lack of familiarity with these technologies can make even basic actions appear intimidating (Lozoya *et al.*, 2022).

#### 5.4.2 Factors Influencing Behaviour

The daily routine of an elderly individual can be described using five key indicators: 1) the proportion of time spent lying down, 2) the proportion of time spent sitting, 3) the proportion of time spent standing, 4) the proportion of time spent away from home, and 5) the daily count of falls (Msaad *et al.*, 2021). The Gottfredson and Hirschi (Hu *et al.*, 2014), poor self-control theory posits that individuals with low self-control have a lack of long-term planning and tend to prioritise immediate gratification. Yuxi Shang goes more in detail stating that elderly are less inclined to adopt precautions to safeguard themselves from potential danger while engaging in certain endeavours. Consequently, a lack of self-control may heighten the likelihood of older persons falling victim to fraud.(Shang *et al.*, 2022).

In addition, psychology also plays a role, as emotional vulnerabilities and the human desire for connection might increase the elderly's susceptibility to romantic frauds (Shang *et al.*, 2022). Scammers manipulate these psychological factors, frequently establishing false profiles to develop virtual connections with their victims. Based on data provided by the Federal Trade Commission, romance scams resulted in a cumulative loss of $1.3 billion in 2022, with an average financial loss of $4,400 per victim (Alieyah *et al.*, 2023). The convergence of loneliness, a longing for friendship, and occasionally cognitive deterioration (Ring *et al.*, 2013) facilitates the exploitation of victims by criminals, who deceive them into believing they are engaged in an authentic (Ebner, Pehlivanoglu and Shoenfelt, 2023).

#### 5.4.3 Health Factors

As mentioned in section 5.3, Cognitive plays a big role on senior citizens on the virtual side of the world and are much more liable to cyber-attacks. Johan Frishammar conducts in this study that cognitive load presents a notable challenge for elderly individuals, as they are more prone to cognitive impairments, disabilities, and chronic ailments compared to younger individuals. Moreover, a decrease in memory and cognitive abilities can negatively impact their ability to acquire proficiency in utilising Information and Communication Technologies (ICTs) (Frishammar *et al.*, 2023). The study conducted by M.J. Rodriguez-Fortiz, explores the wider scope of cognitive health in older individuals, highlighting the advantages of cognitive stimulation in decelerating or perhaps reversing cognitive deterioration associated with ageing. Their research highlights that aged adults may undergo a decline in cognitive abilities, characterised by diminished problem-solving skills and memory impairment, which are significant aspects to consider for preserving cognitive well-being (Rodriguez-Fortiz *et al.*, 2016).

#### 5.4.4 INTERNET SKILLS Among the Elderly

A study conducted by Alexander van Deursen and Jan van Dijk highlights a subtle "digital divide" that disproportionately affects the elderly. Their research transitions the emphasis from mere access concerns to discrepancies in digital abilities, revealing that although older persons may possess fundamental operational and formal internet skills, they notably lack in knowledge and strategic skills that are crucial for effective online usage. The study indicates that seniors who lack advanced digital abilities may experience increased exclusion, resulting in limited access to information and reduced ability to actively check for a threat on the go (van Deursen and van Dijk, 2010).

The research conducted by Bhattacharjee, Baker, and Waycott (Bhattacharjee, Baker and Waycott, 2020), also highlights the obstacles that prevent older persons from actively participating in digital activities. These hurdles encompass a variety of factors, including physical and cognitive limits, feelings of low self-confidence, and societal attitudes. Similar to the research conducted by van Deursen and van Dijk (van Deursen and van Dijk, 2010), this work indicates that the digital gap goes beyond mere access to technology. It highlights the importance of providing specific assistance and education to develop self-assurance and proficiency in digital skills.

### 5.5 Reviews of Cyber-Attacks on the eLDERLY

Add sutting here!!!

#### 5.5.1 Phishing Scams

Phishing is “one of the most serious crimes in the digital world” (Gupta, Arachchilage and Psannis, 2018), and this type of security breach targets consumers by manipulating them into providing personal data, such as credit card information, or other account credentials, through false websites or emails for financial gains. Phishing sites sometimes act out as genuine ones, making it difficult for consumers to determine their legitimacy (Patil and Dhage, 2019). Based on a 2016 survey from the United Kingdom, 53% of elderly adults are vulnerable to becoming victims of fraudulent email schemes (Everett, 2016).

The study by Sannd and Cook (Sannd and Cook, 2018) investigates into the significant impact of ransomware assaults and social engineering tactics on older adults, a demographic that is increasingly becoming a major part of the online community. This gap in digital proficiency makes them particularly vulnerable to cybercrime, including phishing and ransomware attacks. Similarly, the research conducted by (Sugunaraj, Ramchandra and Ranganathan, 2022b) highlights the susceptibility of elderly individuals in the United States to phishing scams, in which criminals impersonate trustworthy organisations in order to obtain personal information. The study highlights the key indicators of phishing, such as unrequested verification appeals and emails containing grammatical errors, while emphasising the significance of vigilance and proper cyber hygiene habits. Scams are becoming more sophisticated due to the utilisation of advanced estrategies like as artificial intelligence and social engineering (Shalke and Achary, 2022).

#### 5.5.2 Romance Fraud

\*\*CAN I INCLUDE NEWS, HONEY TRAP MP\*\*

Relationships are needed for humans, and it’s not to be surprised that elderly try to get close in any ways possible, as they mostly want to “reduce loneliness” (Karim, Lokman and Redzuan, 2017). According to Action Fraud they disclosed financial losses incurred due to romance fraud escalated to 50 million pounds in 2018, indicating a 27% increase compared to the previous year, despite the implementation of heightened awareness and guidance on the subject. The reason why cyber criminals go for older seniors or known as, “lonely-hearts swindles”, is because usually they have failed relationships, and have money saved up and are easier targets, by which females are much more prone, and have a percentage of 63% to romance scams (Dickerson, Apeh and Ollis, 2020).

Love scammers also target vulnerable elderly people who are widowed or recently divorced. These individuals are isolated from family and friends who can already recognize signs of clowning. Even online, scammers can undermine victims’ safety and judgment with bait and gifts (Robinson and Edwards, 2024). It is important to teach the warning signs of elderly romance scams, such as asking for money without meeting in person, video chats that cannot be accessed, and information that never matches public records Adults should also be warned to never be strangers so send money to those you met strictly online. Increased awareness could help arm this high-risk group against criminals involved in cyber-romantic crimes (Saad, Huda Sheikh Abdullah and Murah, 2018).

#### 5.5.3 Government Impersonation Scams

In world of cybercrime, fraudster may call, email, or send an official-looking text message indicating that the victim’s identity or account has been compromised also as known as smishing (Alawida *et al.*, 2022). Yu and colleagues have added that the financial scams and fraud are targeting seniors, and this pose crucial public health as well as economic threat (Yu *et al.*, 2023). In addition to that, their study has claimed that various older adults that includes those who do not have cognitive impairment are also vulnerable to the scams and frauds. Along with that, the latest sentinel data gathered by Federal Trade commission revealed that the older adults filed approximate to half a million frauds that are reported in the year 2022 with experiencing collective loss of approximately $1.5 billion.

Government Impersonation fraud is more effective because it exploits the tendency of the elderly to follow the law and respect authority. Fraudsters also know that many older people worry about identity theft and fall for the benefit of fraud (Robb and Wendel, 2023). By posing as trustworthy agencies that investigate such cases, they build trust and convince victims that they need money immediately to prosecute claims as discussed in the study (Wilson *et al.*, 2023). Although, taxpayer calls are sometimes made by government agencies, they will never demand immediate payment of taxes without first filing government documents. Authentic departments also do not ask for sensitive data or invisible patterns of behaviour for any kind of process (Shu, Yao and Bertino, 2015).

### 5.6 Conclusion

In a summary, the chapter has discussed about the basic understanding of cybercrime and its role in domains, later on the literature has identified about the higher vulnerability of cyberthreats towards the seniors in study. It has been found that lack of awareness and modern technology handling is making the seniors more vulnerable towards threats. In addition, the study has discussed about various threats and types along with social engineering techniques which shed light on various aspects at which the seniors are lacking and more work is required to be done. Even older adults with little experience with their cybersecurity by translating risks into easy-to-follow security course tailored to their technical perspectives and needs freedom of the subject. As a result, this whole literature review discusses several initiatives aimed at addressing the unsatisfied requirement of seniors in terms of cybersecurity skills, required technical practices, and the creation of urgent online user guide.

# 6. METHODOLOGY

# 7. RESULTS

# 8. TESTING

# 9. PROFESSIONAL ISSUES

# 10. CONCLUSION

# 11. REFLECTION

# 12. APPENDICS OR IN NEW TABLE