**A black background with a black square

Description automatically generated with medium confidence**

**Assessment cover**

**STUDENTS, PLEASE COPY THIS PAGE AND USE AS THE COVER PAGE FOR YOUR FINAL SUBMISSION**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Module No: | **COMP6013** | | | Module title: | **BSc Computing Project** | |
| Degree Programme : | | **BSc Hons Computer Science for Cyber Security** | | | | |
| Project title : | | **WiseNet: Online User Guide for Elderly about Cyber Threats** | | | | |
| Supervisor : | | **Mr Muhmmad Hilmi Kamarudin,** | | | | |
| Due date and time**:** | |  | | | | |
| Estimated total time to be spent on assignment: | | | | | | **90 hours per student** |
| **Student No:** | | | **Student Name:** | | | |
|  | | |  | | | |

**Statement of Compliance *(please tick to sign)***

A green check mark on a black background

Description automatically generatedI declare that the work submitted is my own and that the work I submit is fully in accordance with the University regulations regarding assessments *(*[*www.brookes.ac.uk/uniregulations/current*](http://www.brookes.ac.uk/uniregulations/current)*)*

**Regulations governing the deposit and use of Oxford Brookes University Projects and Dissertations**

Copies of projects/dissertations, submitted in fulfilment of Modular Programme requirements and achieving marks of 60% or above, shall normally be kept by the Library.

**Statement of Permission *(please tick to sign)***

|  |  |
| --- | --- |
| A green check mark on a black background  Description automatically generated | **Thank you for agreeing to have your work (i.e. dissertation and associated deliverables) deposited in the Repository’s Undergraduate eDissertation collection.**  By depositing this work, you agree to the following Terms and Conditions:  You confirm that:   1. you are the copyright owner and/or have the right to grant us licence to hold your work in our institutional repository (currently RADAR).   We agree to:   1. add the work to the COMP6013 Collection so that it is available to Oxford Brookes University members for the lifetime of the institutional repository. 2. convert the work if necessary for long term preservation.   We reserve the right to remove third party copyright material that we may identify in the work.  We reserve the right to remove the work for any legal or administrative reason. |

**Use of AI Tools**

You are required to use this [form](https://docs.google.com/forms/d/e/1FAIpQLSfjGiLTf7NEGMVeaZe62ufUxUs7kmw6HayzYTNKKioz_D3G2Q/viewform) to declare which AI tools you have used and how you have used them. Please complete the form and attach it to your submission as an Appendix, if you have used such tools.

**LEARNING OUTCOMES**

|  |  |
| --- | --- |
| **On successful completion of this module, students will be able to achieve the module following learning outcomes (LOs):** | |
| 1 | Create, design, manage, plan, carry out, and evaluate a project involving the solution of a practical problem set in an appropriate social and economic context, taking into account other relevant factors such as risk |
| 2 | Apply practical and analytical skills acquired in the programme to the investigation of a substantial topic |
| 3 | Apply the scientific method and report findings using accepted formalisms |
| 4 | Identify and utilise trustworthy information sources, such as the ACM Digital Library to develop a coherent understanding of issues in the domain |
| 5 | Demonstrate the ability to carry out a substantial piece of work independently and critically evaluate the student’s achievements and their own personal development |
| 6 | Use appropriate technologies such as online libraries and databases to find, critically evaluate and utilise both non-specialist and technical information pertinent to the project |
| 7 | Demonstrate an awareness of and work in a manner guided by the legal, professional, ethical, security and social issues relevant to the IT and telecommunications industry |

|  |  |
| --- | --- |
| **Engineering Council AHEP4 LOs assessed (from S1 2022-23):** | |
| **B3** | Select and apply appropriate computational and analytical techniques to model broadly-defined problems, recognising the limitations of the techniques employed |
| **B4** | Select and evaluate technical literature and other sources of information to address broadly-defined problems |
| **B5** | Design solutions for broadly-defined problems that meet a combination of societal, user, business and customer needs as appropriate. This will involve consideration of applicable health & safety, diversity, inclusion, cultural, societal, environmental and commercial matters, codes of practice and industry standards |
| **B6** | Apply an integrated or systems approach to the solution of broadly-defined problems |
| **B7** | Evaluate the environmental and societal impact of solutions to broadly-defined problems |
| **B8** | Identify and analyse ethical concerns and make reasoned ethical choices informed by professional codes of conduct |
| **B9** | Use a risk management process to identify, evaluate and mitigate risks (the effects of uncertainty) associated with a particular project or activity |
| **B10** | Adopt a holistic and proportionate approach to the mitigation of security risks |
| **B13** | Select and apply appropriate materials, equipment, engineering technologies and processes |
| **B15** | Apply knowledge of engineering management principles, commercial context, project management and relevant legal matters |
| **B17** | Communicate effectively with technical and non-technical audiences |

**FORMATIVE FEEDBACK OPPORTUNITIES**

|  |
| --- |
| **Your supervisor will give you the following formative feedback:**   * Weekly, during project supervision meetings * Written feedback on Proposal (See Appendix A) * Written feedback on Progress Report (See Appendix B) * Feedback on presentation draft |

**SUMMATIVE FEEDBACK DELIVERABLES**

|  |  |
| --- | --- |
| **Deliverable description and instructions** | **Weighting out of 100%** |
| Presentation (see Appendix C) comprising:   1. presentation of software, with video URL 2. project slides 3. summary poster (i.e. the final project slide) | **10%** |
| Final Report (see Appendix D) comprising:   1. written dissertation 2. software artefact URL link to source code | **90%** |

**ASSIGNMENT IN DETAIL**

|  |
| --- |
| See Handbook Appendices A – D for assignment details and marking grid. |

BSc cOMputing Project

Muhamade Ashif Muhamade Muhajireen

19165527

WiseNet: online User guide for Elderly Individuals about cyber threats

Dissertation Course No:

Contents

[1. Glossary 8](#_Toc164469107)

[2. Abstract 8](#_Toc164469108)

[3. Acknowledgments 8](#_Toc164469109)

[4. Introduction 8](#_Toc164469110)

[4.1 Background of the Project 8](#_Toc164469111)

[4.2 Aims and Objectives 9](#_Toc164469112)

[4.3 Motivation 9](#_Toc164469113)

[4.4 Key Functions of Project 10](#_Toc164469114)

[4.5 Product Overview 10](#_Toc164469115)

[5. Literature Review 10](#_Toc164469116)

[5.1 Introduction 10](#_Toc164469117)

[5.2 What is Cyber Crime? 10](#_Toc164469118)

[5.3 Why Are Seniors more Vulernable to Cybercrime? 11](#_Toc164469119)

[5.4 Cyber Issues and Challenges Among the sENIORS 12](#_Toc164469120)

[5.4.1 Technology VS Age 12](#_Toc164469121)

[5.4.2 Factors Influencing Behaviour 12](#_Toc164469122)

[5.4.3 Health Factors 13](#_Toc164469123)

[5.4.4 INTERNET SKILLS Among the Elderly 13](#_Toc164469124)

[5.5 Reviews of Cyber-Attacks on the eLDERLY 13](#_Toc164469125)

[5.5.1 Phishing Scams 13](#_Toc164469126)

[5.5.2 Romance Fraud 14](#_Toc164469127)

[5.5.3 Government Impersonation Scams 14](#_Toc164469128)

[5.6 Summary Of Literature Review 15](#_Toc164469129)

[6. METHODOLOGY 15](#_Toc164469130)

[6.1 Questionnaire 15](#_Toc164469131)

[6.1.1 Qestionnaire Participants 16](#_Toc164469132)

[6.2 Agile Software Development 16](#_Toc164469133)

[6.2.1 Development Logs (Appendix A) 17](#_Toc164469134)

[6.2.1.1 Sprint 1 Log and Analysis 17](#_Toc164469135)

[6.2.1.2 Sprint 2 Log and Analysis 17](#_Toc164469136)

[6.3 Requirements 17](#_Toc164469137)

[6.3.1 Functional Requirements 17](#_Toc164469138)

[6.3.2 Non-Functional Requirements 18](#_Toc164469139)

[6.4 Specification 18](#_Toc164469140)

[6.4.1 Specification of the Functional Requirements 18](#_Toc164469141)

[6.4.2 Specification of the Non-Functional Requirements 19](#_Toc164469142)

[6.5 Software Design 19](#_Toc164469143)

[6.5.1 Initial Wireframe Designs 20](#_Toc164469144)

[6.5.1.1 Home Page 20](#_Toc164469145)

[6.5.1.2 About Page 21](#_Toc164469146)

[6.5.1.3 Cyber Threats Page 21](#_Toc164469147)

[6.5.1.4 Quizzes Page 22](#_Toc164469148)

[6.5.1.5 News Page 22](#_Toc164469149)

[6.5.1.6 Contact Us Page 23](#_Toc164469150)

[6.5.1.7 Choosen Topic Page 23](#_Toc164469151)

[6.5.2 uSE cASE dIAGRAMS 24](#_Toc164469152)

[7. RESULTS 25](#_Toc164469153)

[8. TESTING 25](#_Toc164469154)

[9. PROFESSIONAL ISSUES 25](#_Toc164469155)

[10. CONCLUSION 25](#_Toc164469156)

[11. REFLECTION 25](#_Toc164469157)

[Biblography 26](#_Toc164469158)

[Appendix 32](#_Toc164469159)

[Appendix B – Software Used in Dissertation 32](#_Toc164469160)

[Appendix B.1 – Visual Studio Code 32](#_Toc164469161)

[Appendix B.2 - cANVA 32](#_Toc164469162)

[Appendix B.3 – WireFrame.cc 32](#_Toc164469163)

[Appendix B.4 - Mendeley 32](#_Toc164469164)

# 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, 2021a).

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, 2021b), 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.*, 2023a). 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.*, 2022a).

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.*, 2022b). 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.*, 2023b). 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 Summary Of Literature Review

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

### 6.1 Questionnaire

To achieve the success of the project and accomplish project aims, a carefully crafted questionnaire was developed to explore the current level of awareness and the cybersecurity measures elderly individuals have implemented to defend themselves against cyber threats. The collected information will allow to see an insight from the elderly, focusing on their experience and knowledge gaps. The feedback data provided by the elderly individuals will be essential in the design phase, where customised educational materials and resources will be tailored for this vulnerable generation. This will involve incorporating real-time data from today's world and integrating it into the informative platform being developed.

The questionnaire was optimised for senior respondents by prioritising simplicity and accessibility in its design. The questionnaire encompassed a diverse range of question types, including binary choices (yes/no), Likert scales to gauge levels of agreement or frequency, and multiple-choice questions (Surveying Older Adults - Age-Friendly World, 2024). The selection of this strategy was made to minimise ambiguity and guarantee that the queries could be comprehended and responded to without any aid.

Additionally, the development of the questionnaire was based on research suggesting the importance of providing adequate background information. As a result, the questionnaire will begin with a brief introductory paragraph that clearly explained its purpose to all participants. This ensured that respondents were well-informed before they started answering the questions, which included a mix of both open-ended and closed formats (Gault, 1907). This variety was intended to maintain engagement and prevent respondents from developing a repetitive response pattern throughout the survey. The questionnaire is designed with simple and direct question formats to provide precise data collection on the level of cybersecurity knowledge and practices among the elderly. This design not only increases the respondents' experience but also boosts the dependability of the insights gained, which is vital for customising educational resources to successfully safeguard this vulnerable group from cyber risks.

#### 6.1.1 Qestionnaire Participants

The study's questionnaire is designed to explicitly include elderly adults from diverse backgrounds, in order to provide a full picture of the issues experienced by this group across varied socioeconomic levels. The participants are chosen to offer valuable perspectives on the efficacy of existing cybersecurity measures and to pinpoint areas of deficiency in knowledge and readiness. Recruiting participants is carried out via community centres, family members, friends of family, and some organisations that directly serve the senior population.

The participants percentage how much male and female.

### 6.2 Agile Software Development

The software development aspect of the dissertation project will employ an Agile methodology. Agile is a software development methodology that focuses on flexibility, quick prototyping, and continuous feedback. It follows an iterative and collaborative approach. Agile is distinguished by its flexible and non-linear workflow, which involves brief development "sprints" that enable the project to rapidly adjust to evolving requirements and user needs. The key advantages of adopting an Agile approach for this project includes:

1. **Responsiveness to Change**: The iterative Agile process allows the development team to integrate feedback and adapt the product roadmap in accordance with changing user needs or new technological requirements.
2. **Early and Continuous Delivery**: Agile methodology enables the project to be divided into smaller, easily manageable sprints, resulting in more frequent releases of functional software. This approach ensures that consumers receive value from the programme at an earlier stage.
3. **Increased Collaboration**: It prioritises extensive cooperation among the development team, stakeholders, and end-users, resulting in improved alignment and expedited issue resolution.
4. **Improved Quality**: It prioritises testing, continuous integration, and iterative refinement to detect and resolve faults at an earlier stage in the development lifecycle.

Considering the nature of this dissertation topic, which entails the creation of a software application based on a website, the Agile technique is highly appropriate. The iterative Agile approach enables rapid adaptation of software design and functionality to address emerging demands discovered throughout the research phase. The rapid creation of prototypes facilitated by Agile sprints will be essential for the development and evaluation of functional iterations of the application with users at an early and frequent stage, guaranteeing that the end product corresponds to their anticipated requirements. Moreover, the cooperative aspect of Agile development will be crucial for incorporating the software component into the wider dissertation research. Furthermore, the consistent delivery of functional software increments will enable you to demonstrate tangible advancements to your dissertation committee.

### 6.2.1 Development Logs (Appendix A)

#### 6.2.1.1 Sprint 1 Log and Analysis

Check Appendix A.1 to see Sprint 1 Log and analysis.

#### 6.2.1.2 Sprint 2 Log and Analysis

Check Appendix A.2 to see Sprint 2 Log and analysis.

### 6.3 Requirements

#### 6.3.1 Functional Requirements

The functional requirements for this project are as follows:

1. The primary navigation menu should include access to the Home, About, Cyber Threats, Quizzes, News, and Contact Us.
2. On the main page, when user clicks on “Start the Guide”, should redirect user to “Cyber Threats Page”.
3. User should be able to view a list of the bespoke courses on the "Cyber Threats" page and be able to click on tiles to view information.
4. The “Test Me!” button should take user to related cyber threat quiz.
5. The "Quizzes" page must list all quizzes from “Cyber Threats” page, for users to choose and participate in.
6. For each quiz, when completed successfully, should display the user's score and provide options to retry the quiz or return to the quiz selection page, “Quizzes”.
7. The users must be able to fill out and submit a contact form on the "Contact Us" page. The system should validate input fields.
8. The project must implement security measures to prevent cheating during quizzes.
9. The users should be able to watch a video version about the specific cyber threat topic, if they want.

#### 6.3.2 Non-Functional Requirements

The non-functional requirements for this project are as follows:

1. The website design must be visually appealing with a consistent colour scheme.
2. The website should have readable text size for the elderly.
3. The website should have a responsive layout that is compatible with all screen sizes, including desktop, tablet, and mobile devices.
4. The navigation buttons and links should be clearly visible, minimising user effort to navigate through pages and find information.
5. All pages should load swiftly within 3 seconds or less.
6. The software uptime will be 99.99% each year, this results in an annual downtime of 52.60 minutes.
7. The maximum allowable response time for a smooth user experience is 2 seconds.
8. The website must guarantee cross-browser compatibility, operating flawlessly on the most recent iterations of prominent web browsers such as Chrome, Firefox, Safari, and Edge.

# 6.4 Specification

### 6.4.1 Specification of the Functional Requirements

We shall proceed in a sequential manner, regarding Requirement 6.3.1 for Functional Requirements.

1. The menu will be at top of every web page, implemented using HTML lists and styled with CSS for desktop and use a hamburger menu for mobile views, including all links labelled.
2. Button should be placed in middle of the first half of the index page, using anchor tag or java redirection to “Cyber Threats” page.
3. Cyber threats page should be created using HTML, and CSS, with clickable tiles with graphic, title of course. Clicking on each tile should redirect to correct page.
4. Button created for association with each cyber threat topic, on click the button should take user to corresponding quiz – implemented with JavaScript event listeners.
5. Quizzes will be listed on a dedicated “Quizzes” page, styled with a specific designed tiles associated with each cyber threat topic.
6. After completion of the quiz, user should be represented with score calculated by JavaScript scoring engine.
7. Contact form collecting respective fields, and include client-side validation with SOMETHING, before submission.
8. Disabling users to go back and change answers, and/or change answers after choosing.
9. Video element embedded on each cyber threat topic page, with clear play/pause/skip instructions. Will include a label/button regarding reading content or watch video.

### 6.4.2 Specification of the Non-Functional Requirements

We shall proceed in a sequential manner, regarding Requirement 6.3.2 for Non-Functional Requirements.

1. Aligns with colour scheme, using CSS for consistent measures across all pages.
2. Text sizes, above average size making sure legible for the elderly, can be fulfilled with CSS.
3. Utilising media queries in CSS to adjust layout for different scenes sizes and orientation.
4. Buttons and links clear and stand out, with appropriate spacing to prevent accidental presses.
5. Optimising pictures, reducing CSS and JavaScript files, and utilise efficient HTML structures, will ensure that sites load within a maximum of 3 seconds.
6. Ensuring reliable hosting, and if any issues resolve them promptly.
7. Designing backend systems to processes efficiently regarding any pages to load up, minimalizing “rubbish” code.
8. Employ HTML, CSS, and JavaScript that adhere to established standards in order to mitigate issues particular to different web browsers and conducting tests across them.

# 6.5 Software Design

The website's development will be based on a specific set of web design principles that are customised to adapt to the requirements of an older demographic. This will guarantee a user-friendly experience and effective communication. Here are some steps taken:

1. Professional Design - The website will be carefully constructed to cater to the requirements of the elderly, ensuring that each page offers explicit instructions to facilitate meaningful engagement and maximise the use of the website's resources.
2. Ease of Navigation - The purpose of this is to optimise the website's usability for senior users, reducing any potential confusion and facilitating them efficient access to essential information.
3. Enhanced Usability - The website will adopt a minimalist style to enhance user-friendliness:
   1. Colour Scheme – It will be designed for supporting across all users in the environment, with those with visual impairments, as mentioned in LITERATURE REVIEW SECTION OR AUTHOR.
   2. Typography – Text will be shown in large letter sizes and high-contrast typefaces to enhance legibility for users with different degrees of visual acuity.
   3. Visual Imagery – The graphics will be large, distinct, and appropriate to the corresponding text, aiding in the communication of information and generating an advantageous impression on the user.
   4. Read/Watch Flexibility – The users can choose either to read or watch regarding their preferences, ensuring accessibility for those with visual or auditory disabilities.
4. Accessible Content – Content displayed should be direct, relevant information, eliminating complex jargon for elderly individuals to comprehend information easier.
5. Accessibility of Devices – Since many elderly users may rely on tablets, smartphones, and various other devices. The website will feature a responsive design to ensure full functionality and a positive viewing experience on all devices.

### 6.5.1 Initial Wireframe Designs

The designs that were originally integrated into the website were all based on the core wireframe blueprints.

#### 6.5.1.1 Home Page

This is the educational websites home page where user will be able to navigate through:

A screenshot of a computer security

Description automatically generated

Figure 1: Initial Design of Home Page

#### 6.5.1.2 About Page

This is the educational websites About page where user will be able to read about the software:

A screenshot of a website

Description automatically generated

Figure 2: Initial Design of About Page

#### 6.5.1.3 Cyber Threats Page

This is the educational websites Cyber Threats page where user will be able to educate themselves:

A white sheet of paper with black text

Description automatically generated

Figure 3: Initial Design of Cyber Threats Page

#### 6.5.1.4 Quizzes Page

This is the educational websites about Quizzes where user will be able to test their newly learnt knowledge:

A white sheet of paper with text

Description automatically generated

Figure 4: Initial Design of Quizzes Page

#### 6.5.1.5 News Page

This is the educational websites about page where user will be able to view news regarding cyber:

A screenshot of a news page

Description automatically generated

Figure 5: Initial Design of News Page

#### 6.5.1.6 Contact Us Page

This is the educational websites “Contact Us” page where user will be able to contact any regarding queries:

A screenshot of a computer

Description automatically generated

Figure 5: Initial Design of Contact Us Page

#### 6.5.1.7 Choosen Topic Page

This is the educational websites chosen topic page skeleton where user will be able to read/watch and gain knowledge about the chosen cyber threat:

A paper with text on it

Description automatically generated

Figure 6: Initial Design of Model Page for Chosen Cyber Threat

### 6.5.2 uSE cASE dIAGRAMS

# 6.6 Implementation

The project was implemented using Visual Studio Code IDE this is a free, open-source software which is installed onto your computer and be able to create your own website. Here is a list of the software I used (Refer to APPENDIX B for more details):

* + 1. Visual Studio Code
    2. Canva
    3. WireFrame.cc
    4. Mendeley
    5. GitHub
    6. Google Drive

For development of the website, I used HTML, CSS, JavaScript, and PHP. HTML served as the framework and coding for web pages, while CSS improved their visual appearance and arrangement. JavaScript enhanced the user interface by introducing interaction and dynamic capabilities, hence enhancing the overall user experience. PHP facilitated server-side scripting, allowing for the development of dynamic content and interfaces with databases. Collectively, these technologies served as the basis for constructing a thorough and engaging online application as a component of my dissertation thesis.

The functional requirements were implemented within the Agile development process during consecutive sprints. The analysis undertaken at the end of each sprint, as described in Appendix C.1 – C.11, shows that the user stories were executed and completed, which helps meet both the functional and non-functional project requirements.

# 6.7 Version Management

Version control is crucial during development to monitor the progress of the project and provide a backup in case of any issues. It is necessary to store any modifications or additions to files on the local workstation using GitHub and Google Drive. GitHub is an optimal approach to version control that effectively safeguards against the loss of progress. Branches can be utilised to modify an alternative version of the source code without making changes to the primary version. By utilising a platform like GitHub, one may constantly upload successive versions of a project to the online repository, allowing for a transparent record of the development process from start to finish. It is advisable to regularly back up the complete file to Google Drive on a weekly basis, especially for files that may not be compatible with GitHub.

GitHub Link – <https://github.com/A7HXF/Dissertation>

Google Drive Link - <https://drive.google.com/drive/folders/1vEN69hU8V3I_srOCZygGtSVhhM4N2hSq?usp=drive_link>

# 6.8 Testing

The website completed testing utilising a Test-Driven Development (TDD) technique. This involved creating tests in parallel with the specification throughout each Agile sprint, guaranteeing the program's optimal functionality from the beginning. The test-first methodology involves conducting tests for each user narrative prior to moving on to the next one, therefore preventing the occurrence of problems in the latter stages. The testing process, which is thoroughly described in Appendix C.1 – C.11, included the verification of both functional and non-functional requirements. This was done through the implementation of a comprehensive test plan and ongoing evaluations, which were recorded in the Google Drive folders for each sprint.

# 7. RESULTS

# 8. TESTING

# 9. PROFESSIONAL ISSUES

# 10. CONCLUSION

# 11. REFLECTION

# Biblography

Alawida, M. *et al.* (2022) ‘A deeper look into cybersecurity issues in the wake of Covid-19: A survey’, *Journal of King Saud University - Computer and Information Sciences*, 34(10), pp. 8176–8206. Available at: https://doi.org/10.1016/J.JKSUCI.2022.08.003.

Aleksandrova, N.A., Khramova, M. V. and Kurkin, S.A. (2018) ‘Computer Safety Basics Training for the Older Generation’, *Proceedings of the 2018 International Conference ‘“Quality Management, Transport and Information Security, Information Technologies”’, IT and QM and IS 2018*, pp. 542–544. Available at: https://doi.org/10.1109/ITMQIS.2018.8525098.

Alieyah, N. *et al.* (2023a) ‘Development of a New Synergistic Cyber Security Awareness Model for The Elderly in Malaysia (SCSAM-Elderly)’, *2023 IEEE 8th International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, pp. 1–8. Available at: https://doi.org/10.1109/ICRAIE59459.2023.10468097.

Alieyah, N. *et al.* (2023b) ‘Development of a New Synergistic Cyber Security Awareness Model for The Elderly in Malaysia (SCSAM-Elderly)’, *2023 IEEE 8th International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, pp. 1–8. Available at: https://doi.org/10.1109/ICRAIE59459.2023.10468097.

Arshey, M. and Angel Viji, K.S. (2021) ‘Thwarting Cyber Crime and Phishing Attacks with Machine Learning: A Study’, *2021 7th International Conference on Advanced Computing and Communication Systems, ICACCS 2021*, pp. 353–357. Available at: https://doi.org/10.1109/ICACCS51430.2021.9441925.

Banovic, S., Zunic, L.J. and Sinanovic, O. (2018) ‘Communication Difficulties as a Result of Dementia’, *Materia Socio-Medica*, 30(3), p. 221. Available at: https://doi.org/10.5455/MSM.2018.30.221-224.

Bendovschi, A. and Al-Nemrat, A. (2016) ‘Security countermeasures in the cyber-world’, *2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016* [Preprint]. Available at: https://doi.org/10.1109/ICCCF.2016.7740440.

Bhattacharjee, P., Baker, S. and Waycott, J. (2020) ‘Older adults and their acquisition of digital skills: A review of current research evidence’, *ACM International Conference Proceeding Series*, pp. 437–443. Available at: https://doi.org/10.1145/3441000.3441053.

Costilla-Reyes, O. *et al.* (2021) ‘Age-Related Differences in Healthy Adults Walking Patterns under a Cognitive Task with Deep Neural Networks’, *IEEE Sensors Journal*, 21(2), pp. 2353–2363. Available at: https://doi.org/10.1109/JSEN.2020.3021349.

van Deursen, A. and van Dijk, J. (2010) ‘Internet skills and the digital divide’, *http://dx.doi.org/10.1177/1461444810386774*, 13(6), pp. 893–911. Available at: https://doi.org/10.1177/1461444810386774.

Dickerson, S., Apeh, E. and Ollis, G. (2020) ‘Contextualised Cyber Security Awareness Approach for Online Romance Fraud’, *Proceedings of 2020 7th IEEE International Conference on Behavioural and Social Computing, BESC 2020* [Preprint]. Available at: https://doi.org/10.1109/BESC51023.2020.9348307.

Ebner, N.C., Pehlivanoglu, D. and Shoenfelt, A. (2023) ‘Financial Fraud and Deception in Aging’, *Advances in geriatric medicine and research*, 5(3). Available at: https://doi.org/10.20900/AGMR20230007.

Everett, C. (2016) ‘Ransomware: to pay or not to pay?’, *Computer Fraud & Security*, 2016(4), pp. 8–12. Available at: https://doi.org/10.1016/S1361-3723(16)30036-7.

Fdic (2021) ‘MONEY SMART for Older Adults Resource Guide Money Smart for Older Adults Resource Guide Welcome to Money Smart for Older Adults!’ Available at: https://vtechworks.lib.vt.edu/ (Accessed: 6 April 2024).

Frishammar, J. *et al.* (2023) ‘Older Individuals and Digital Healthcare Platforms: Usage Motivations and the Impact of Age on Postadoption Usage Patterns’, *IEEE Transactions on Engineering Management*, 70(8), pp. 2903–2919. Available at: https://doi.org/10.1109/TEM.2022.3187792.

Gault, R.H. (1907) ‘A History of the Questionnaire Method of Research in Psychology’, *Pedagogical Seminary*, 14(3), pp. 366–383. Available at: https://doi.org/10.1080/08919402.1907.10532551.

Grabosky, P.N. (2001) ‘Virtual criminality: Old wine in new bottles?’, *Social and Legal Studies*, 10(2), pp. 243–249. Available at: https://doi.org/10.1177/A017405/ASSET/A017405.FP.PNG\_V03.

Gupta, B.B., Arachchilage, N.A.G. and Psannis, K.E. (2018) ‘Defending against phishing attacks: taxonomy of methods, current issues and future directions’, *Telecommunication Systems*, 67(2), pp. 247–267. Available at: https://doi.org/10.1007/S11235-017-0334-Z.

Hu, Q. *et al.* (2014) ‘Why individuals commit information security violations: Neural correlates of decision processes and self-control’, *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 3234–3243. Available at: https://doi.org/10.1109/HICSS.2014.400.

Hull, M., Eze, T. and Speakman, L. (2018) ‘Policing the cyber threat: Exploring the threat from cyber crime and the ability of local law enforcement to respond’, *Proceedings - 2018 European Intelligence and Security Informatics Conference, EISIC 2018*, pp. 15–22. Available at: https://doi.org/10.1109/EISIC.2018.00011.

Hunsaker, A. and Hargittai, E. (2018) ‘A review of Internet use among older adults’, *https://doi.org/10.1177/1461444818787348*, 20(10), pp. 3937–3954. Available at: https://doi.org/10.1177/1461444818787348.

Javidi, G. and Sheybani, E. (2018) ‘K-12 Cybersecurity Education, Research, and Outreach’, *Proceedings - Frontiers in Education Conference, FIE*, 2018-October. Available at: https://doi.org/10.1109/FIE.2018.8659021.

Karagiannopoulos, V. *et al.* (2021) ‘Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study’, *computer law & security review*, 43, p. 105615. Available at: https://doi.org/10.1016/j.clsr.2021.105615.

Karim, H.A., Lokman, A.M. and Redzuan, F. (2017) ‘Older adults perspective and emotional respond on robot interaction’, *Proceedings - 2016 4th International Conference on User Science and Engineering, i-USEr 2016*, pp. 95–99. Available at: https://doi.org/10.1109/IUSER.2016.7857941.

Lee, C.K., Hoong Lee, A.S. and Ean Catherine Lee, C. (2021a) ‘Internet Usage Among Senior Citizens During Covid - 19’, *International Conference on Research and Innovation in Information Systems, ICRIIS* [Preprint]. Available at: https://doi.org/10.1109/ICRIIS53035.2021.9617031.

Lee, C.K., Hoong Lee, A.S. and Ean Catherine Lee, C. (2021b) ‘Internet Usage Among Senior Citizens During Covid - 19’, *International Conference on Research and Innovation in Information Systems, ICRIIS* [Preprint]. Available at: https://doi.org/10.1109/ICRIIS53035.2021.9617031.

Liaqat, A. and Liaqat, F. (2021) ‘Covid-19 Impact on the Internet, User Experience and Economy in Pakistan’, *IMTIC 2021 - 6th International Multi-Topic ICT Conference: AI Meets IoT: Towards Next Generation Digital Transformation* [Preprint]. Available at: https://doi.org/10.1109/IMTIC53841.2021.9719774.

Lošonczi, P. (2018) ‘Importance of Dealing with Cybersecurity Challenges and Cybercrime in the Senior Population’, *Security Dimensions*, 26(26), pp. 173–186. Available at: https://doi.org/10.5604/01.3001.0012.7249.

Lozoya, S.V.M. *et al.* (2022) ‘Use of Technologies and Self-Efficacy in Older Adults’, *Revista Iberoamericana de Tecnologias del Aprendizaje*, 17(2), pp. 125–130. Available at: https://doi.org/10.1109/RITA.2022.3166870.

Msaad, S. *et al.* (2021) ‘Detection of changes in the behaviour of the elderly person’, *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, pp. 6995–6998. Available at: https://doi.org/10.1109/EMBC46164.2021.9630971.

Murman, D.L. (2015) ‘The Impact of Age on Cognition’, *Seminars in Hearing*, 36(3), p. 111. Available at: https://doi.org/10.1055/S-0035-1555115.

Narayanan, V. *et al.* (2021) ‘Securing social media for seniors from information attacks: Modeling, detecting, intervening, and communicating risks’, *Proceedings - 2021 3rd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2021*, pp. 297–302. Available at: https://doi.org/10.1109/TPSISA52974.2021.00053.

Oh, S.S. *et al.* (2021) ‘Measurement of Digital Literacy Among Older Adults: Systematic Review’, *Journal of Medical Internet Research*, 23(2). Available at: https://doi.org/10.2196/26145.

Patil, S. and Dhage, S. (2019) ‘A Methodical Overview on Phishing Detection along with an Organized Way to Construct an Anti-Phishing Framework’, *2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019*, pp. 588–593. Available at: https://doi.org/10.1109/ICACCS.2019.8728356.

Prasad, R. and Pennington, L. (2020) ‘Designing the Curriculum for a Minor in Cyber Criminology’, *2020 9th IEEE Integrated STEM Education Conference, ISEC 2020*, 2020-January. Available at: https://doi.org/10.1109/ISEC49744.2020.9397830.

Rengamani, H. *et al.* (2010) ‘Protecting senior citizens from cyber security attacks in the e-health scenario: An international perspective’, *ACM International Conference Proceeding Series* [Preprint]. Available at: https://doi.org/10.1145/1852666.1852759.

Reuben, N. *et al.* (2023) ‘Raising Cyber Security Awareness to Reduce Social Engineering Through Social Media in Indonesia’, *Proceedings - 2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System: Responsible Technology for Sustainable Humanity, ICE3IS 2023*, pp. 138–141. Available at: https://doi.org/10.1109/ICE3IS59323.2023.10335454.

Riek, M., Böhme, R. and Moore, T. (2016) ‘Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance’, *IEEE Transactions on Dependable and Secure Computing*, 13(2), pp. 261–273. Available at: https://doi.org/10.1109/TDSC.2015.2410795.

Ring, L. *et al.* (2013) ‘Addressing loneliness and isolation in older adults: Proactive affective agents provide better support’, *Proceedings - 2013 Humaine Association Conference on Affective Computing and Intelligent Interaction, ACII 2013*, pp. 61–66. Available at: https://doi.org/10.1109/ACII.2013.17.

Robb, C.A. and Wendel, S. (2023) ‘Who Can You Trust? Assessing Vulnerability to Digital Imposter Scams’, *Journal of Consumer Policy*, 46(1), p. 27. Available at: https://doi.org/10.1007/S10603-022-09531-6.

Robinson, J. and Edwards, M. (2024) ‘Fraudsters target the elderly: Behavioural evidence from randomised controlled scam-baiting experiments’, *Security Journal*, pp. 1–24. Available at: https://doi.org/10.1057/S41284-023-00410-4/TABLES/4.

Rodriguez-Fortiz, M.J. *et al.* (2016) ‘Serious games for the cognitive stimulation of elderly people’, *2016 IEEE International Conference on Serious Games and Applications for Health, SeGAH 2016* [Preprint]. Available at: https://doi.org/10.1109/SEGAH.2016.7586261.

Ruangkana, V. and Kessuvan, A. (2019) ‘Factors Affecting the Elderly’s Adoption of Online Purchasing’, *2019 International Conference on Engineering, Science, and Industrial Applications, ICESI 2019* [Preprint]. Available at: https://doi.org/10.1109/ICESI.2019.8862993.

Saad, M.E., Huda Sheikh Abdullah, S.N. and Murah, M.Z. (2018) ‘Cyber romance scam victimization analysis using Routine Activity Theory versus apriori algorithm’, *International Journal of Advanced Computer Science and Applications*, 9(12), pp. 479–485. Available at: https://doi.org/10.14569/IJACSA.2018.091267.

Sannd, P. and Cook, D.M. (2018) ‘Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and Phishing Attacks.’, *14th International Conference on Information Processing: Internet of Things, ICInPro 2018 - Proceedings* [Preprint]. Available at: https://doi.org/10.1109/ICINPRO43533.2018.9096878.

Shalke, C.J. and Achary, R. (2022) ‘Social Engineering Attack and Scam Detection using Advanced Natural Langugae Processing Algorithm’, *2022 6th International Conference on Trends in Electronics and Informatics, ICOEI 2022 - Proceedings*, pp. 1749–1754. Available at: https://doi.org/10.1109/ICOEI53556.2022.9776697.

Shang, Y. *et al.* (2022a) ‘The psychology of the internet fraud victimization of older adults: A systematic review’, *Frontiers in Psychology*, 13. Available at: https://doi.org/10.3389/FPSYG.2022.912242/FULL.

Shang, Y. *et al.* (2022b) ‘The psychology of the internet fraud victimization of older adults: A systematic review’, *Frontiers in Psychology*, 13. Available at: https://doi.org/10.3389/FPSYG.2022.912242/FULL.

Shu, X., Yao, D. and Bertino, E. (2015) ‘Privacy-preserving detection of sensitive data exposure’, *IEEE Transactions on Information Forensics and Security*, 10(5), pp. 1092–1103. Available at: https://doi.org/10.1109/TIFS.2015.2398363.

Stratton, G. and Cameron, P.A. (2014) ‘Crime and Justice in Digital Society: Towards a “Digital Criminology”? 1’, *Justice and Social Democracy*, 6(2), pp. 17–33. Available at: https://doi.org/10.3316/INFORMIT.195813913578876.

Sugunaraj, N., Ramchandra, A.R. and Ranganathan, P. (2022a) ‘Cyber Fraud Economics, Scam Types, and Potential Measures to Protect U.S. Seniors: A Short Review’, *IEEE International Conference on Electro Information Technology*, 2022-May, pp. 623–627. Available at: https://doi.org/10.1109/EIT53891.2022.9813960.

Sugunaraj, N., Ramchandra, A.R. and Ranganathan, P. (2022b) ‘Cyber Fraud Economics, Scam Types, and Potential Measures to Protect U.S. Seniors: A Short Review’, *IEEE International Conference on Electro Information Technology*, 2022-May, pp. 623–627. Available at: https://doi.org/10.1109/EIT53891.2022.9813960.

*Surveying Older Adults - Age-Friendly World* (no date). Available at: https://extranet.who.int/agefriendlyworld/afp/surveying-older-adults/ (Accessed: 16 April 2024).

Thangiah, M., Basri, S. and Sulaiman, S. (2012) ‘A framework to detect cybercrime in the virtual environment’, *2012 International Conference on Computer and Information Science, ICCIS 2012 - A Conference of World Engineering, Science and Technology Congress, ESTCON 2012 - Conference Proceedings*, 1, pp. 553–557. Available at: https://doi.org/10.1109/ICCISCI.2012.6297307.

Tilley, S. (2003) ‘Computer documentation for senior citizens’, *ACM Special Interest Group for Design. of Commun.; SIGDOC 2003: Finding Real-World Solutions for Doc.: How Theory Informs Pract. and Pract. Informs Theory. Proc. of the 21st Annu. Int. Conf. on Doc.*, pp. 143–146. Available at: https://doi.org/10.1145/944868.944899.

Wilson, S. *et al.* (2023) ‘A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia’, *Journal of Financial Crime*, ahead-of-print(ahead-of-print). Available at: https://doi.org/10.1108/JFC-06-2023-0151/FULL/PDF.

Yu, L. *et al.* (2023) ‘Vulnerability of Older Adults to Government Impersonation Scams’, *JAMA Network Open*, 6(9), pp. e2335319–e2335319. Available at: https://doi.org/10.1001/JAMANETWORKOPEN.2023.35319.

# Appendix

### Appendix B – Software Used in Dissertation

#### Appendix B.1 – Visual Studio Code

I used Visual Studio Code as the main Integrated Development Environment (IDE). The lightweight nature of the software, together with its significant features such as flexible language support and strong debugging capabilities, greatly simplified coding, integration with version control systems such as GitHub allowed me to assure software version control. The ability to customise the interface and the wide range of extensions available significantly improved productivity and optimised workflow efficiency, ultimately leading to the successful completion of my project. (<https://code.visualstudio.com/>)

#### Appendix B.2 - cANVA

Canva is a powerful application for graphic designing. I purchased Canva premium, in order to produce top quality work with its features, intuitive interface and vast library of templates enabled me to create compelling visuals, such as logo’s, tile images for courses and quizzes bespoke made with nice consistent appearance, and used for presentation designing as well. As a result, Canva significantly enhanced the visual appeal and effectiveness of my research findings and presentations. (<https://www.canva.com/>)

#### Appendix B.3 – WireFrame.cc

Wireframe.cc played a crucial role in the early stages of design development. It’s simple and intuitive interface allowed me to quickly sketch out wireframes for web pages – getting an idea of the website. By creating clear and concise wireframes, Wireframe.cc laid the foundation for the visual and interactive aspects of my research project. (<https://wireframe.cc/>)

#### Appendix B.4 - Mendeley

Mendeley played a crucial part for reference management, aiding in arranging and citing research papers, and websites. Mendeley also generated within the software bibliographies and formatted references. (<https://www.mendeley.com/>)

#### Appendix B.5 - GitHub

GitHub played a crucial role in facilitating version control and cooperation in the field of software development. The portal allowed effortless monitoring of project modifications and cooperation with team members. The tools provided by GitHub greatly aided the efficient management of code, allowing for good organisation of projects and collaboration during the dissertation process. (<https://github.com/>)

#### Appendix B.6 – Google Drive

Google Drive served as a versatile platform for document storage where sprints, some codes, and dissertation is saved at. Its cloud-based nature allowed for easy access to files from anywhere, fostering seamless collaboration with peers and advisors. With features like real-time editing and commenting, Google Drive facilitated efficient document management throughout the dissertation process. (GoogleDrive)