2-26-2024

Development of Technology Pilot Training to Reduce The Number of Senior Citizens Victimized by Computer Fraud Scams

James Eric Johnston
Walden University

Walden University

College of Health Sciences and Public Policy

This is to certify that the doctoral study by

James Johnston

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Linda Sundstrom, Committee Chairperson, Public Policy and Administration Faculty
Dr. George Kieh, Committee Member, Public Policy, and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2024

Abstract

Development of Technology Pilot Training to Reduce the Number of Senior Citizens Victimized by Computer Fraud Scam

by

James Eric Johnston

MPA, Grand Canyon University, 2013

BS, Excelsior College, 2011

Professional Administrative Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Public Administration

Walden University

February 2024

Abstract

The need in the public sector is to help people 60+ years of age in the safe, practical use of technology for business, personal use, and family interaction, as this group is targeted more than others for technology fraud. The practice-focused question centers around which topics need to be part of technology fraud pilot training to reduce the victimization of seniors 60+ years of age. This qualitative administrative study project was to include measures that will improve understanding and safe usage of basic technology used often in daily life. The project uses adult learning as its conceptual framework. Adult learners are motivated by personal interests as they learn new subjects. Sources of evidence include journal articles, government agencies, and document analysis of existing training in addition to best practices to address the gap in personal technology training for senior adults that put them at risk of technology fraud. Thematic analysis was used to answer the research question. Recommendations include a training program for seniors 60+ using adult learning theory that will teach them how to avoid fraud while utilizing the internet. This knowledge will help them to remain safer on the worldwide web. The implications for positive social change can result from expanding the course and using it as a model to help the community stay safe, stay aware of changes in technology, and to function faster as well as better in a constantly changing society.

Development of Technology Pilot Training to Reduce the Number of Senior Citizens Victimized by Computer Fraud Scams

by

James Eric Johnston

MPA, Grand Canyon University, 2013

BS, Excelsior College, 2011

Professional Administrative Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Public Administration

Walden University

February 2024

Acknowledgments

I want to thank the faculty and staff of Walden University for their help completing this study. Special thanks to Dr. Linda-Marie Sundstrom, and Dr. George Kieh for their part in helping as well as advising me, to make this study a reality. Without their help, I could not have accomplished this project.

Table of Contents

List of Tables

Section 1: Introduction to the Problem

According to the Federal Trade Commission (FTC, 2019), adults over 60 years old are five times more likely to report losing money through technology fraud than younger people. Fraud includes romance frauds (those seeking love and companionship), business fraud, investment swindles, tech support frauds, along with fraudulent lotteries, sweepstakes, and prizes; however, the largest of all the categories is for online shopping (AARP, 2019). All these acts of fraud committed against seniors cause them to unknowingly give away their property, money, and other valuables.

This qualitative study will focus on specific causes of technology fraud as it targets senior citizens over 60 years of age and develop a technology training program that helps reduce fraud against this target group. The training will cover the safe, practical, and basic operation of technology for adults age 60+. The term *technology* in this study refers primarily to personal computers and mobile devices. Adult learning (AL) was the framework to develop the training. By conducting this study and creating a training program for the organization, adults over 60+ as well as interested local community will be safer users of technology. The potential implications for public service practice are that the nonprofit will help those who are the focus of its work in the community to learn better ways to use technology. This study can also help others in the community by supplying information on basic, safe, practical, sensible use of technology.

Problem Statement

Problem the study focuses on

The problem addressed through this study is that adults over 60 years old are five times more likely to report losing money through technology fraud than younger people (FTC, 2019). The FBI advises that each year masses of Americans become the victim of fraud. In 2019, 66% of these occurrences were from romance frauds or those seeking love and companionship, 88% were business frauds, 84% were investment swindles, 55% were tech support frauds, and 35% were related to lotteries, sweepstakes, and prizes; however, the largest of all the categories was for online shopping at 129% (AARP, 2019). All these acts of fraud are committed against seniors causing them to unknowingly give away their property, money, and other valuables. Frequently, senior individuals are the focus of these fraud schemes because they often believe the offender who is working to harm them (FBI, 2018).

Defining technology fraud

Technology fraud is the use of a computer to steal, defraud, usurp, or take something of value away from another individual through misrepresentation, fear, or any false and unlawful means (Legal Information Institute, n.d.). Technology fraud is also known as computer fraud, cyber-fraud, and internet fraud. More information is provided by 18 USC sub-section 1030, relating that, whoever intentionally accesses a computer without authority and obtains information that is protected against unauthorized disclosure, and transmits the to another party unlawfully, can be fined $5,000 dollars or face imprisonment for up to 5 years. This includes financial records of a financial organization or a credit card company as specified in title 15 section 1609(n), consumer information explained in the Fair Credit Reporting Act, 15 USC 1681, use of any unauthorized government information, data from a secure computer, theft of real property, and more. The American Association of Retired Persons (AARP) reported that there are 10 distinct types of technology fraud committed on the internet: romance frauds, sweepstakes, prizes, lotteries, government frauds, business frauds, investment frauds, tech support frauds, online shopping frauds, family friendly fraud, timeshare frauds, and timeshare resales. In one case noted by the FTC a company based in Utah offered bogus tech support to the elderly selling needless antivirus and repair services. The company ran misleading diagnostic tests to trick customers into buying the products offered (FTC, 2019).

Impact of fraud and how study addresses problem

By allowing scammers remote access to their computer, people hand over control, and scammers can steal sensitive information and gain access to their bank accounts (Fletcher, 2019). Technology fraud has caused a worldwide economic loss of over $600 billion (about $1,800 per person in the US) to consumers, government, and business (Ali, 2019). The problem can be improved by the creation of a technology deliverable to aid interested adults over 60+ years old in the pursuit of safe operation of personal computing technology. The project may hold significance for other groups in that it creates a model for senior citizens, 60+ years, which could later expand to other regions of the country. Training senior citizens in computer technology creates a better sense of independence, fosters convenient commerce and interpersonal interaction, and improves digital citizenship.

How study addresses local problem

The organization aims to provide a service to the local community pertaining to technology. It was explained that interested older adults in the local community may profit from training in technology. Also, a member of the nonprofit revealed that the entity has not previously performed any service in technology. After this information was revealed to the entire organization, I gained permission to conduct a study for this entity that would focus on four areas giving adults 60+ a foundation to get started in this area and provide a safe way to operate (LaLande, 2021). This study addresses a gap that exists on technology fraud and creates a practical solution to the problem since no study in technology fraud has ever been studied in this nonprofit organization. A study may be beneficial to the residents of this local community, helping to reduce technology frauds.

Purpose

The client organization in this study is a 501(c)3 nonprofit organization in the eastern United States. It serves a small community and has been in operation for 50 years. It has a focus of education to help students in local schools succeed in life. It also strives to provide after-school assistance to students to help them get the best results possible from the local education system. In addition, its educational focus also assists those seeking vocational training and senior adults age 60+ with educational interests as well as other necessary assistance (Focus, 1979). The community served is 25% children (0-17 years old), 62% are adults (18-64 years old), and 13% over 64 years old (City Health Profiles, 2003). For this study's purpose and to ensure confidentiality, the nonprofit organization will be called The Organization.

Although The Organization currently serves a senior population, they currently have no training programs to help the senior citizens avoid becoming victims of technology frauds. The purpose of this qualitative study was to develop a computer technology pilot training program to reduce the number of senior citizens victimized by technology fraud. This study focuses on the needs of senior citizens 60+ as well as other interested persons in the local community. There has been no previous study addressing senior citizens 60+ and technology in the local community. This administrative study will supply basic technology training for seniors who want to gain a basic understanding of computer technology pilot training, which will supply a measure of safety while using the internet. The guiding research question for this study is “What are the important topics to address in the pilot training to prevent seniors from becoming victims of technology fraud?”

Nature of the Administrative Study

To address the research questions in this qualitative study, the specific approach of this study will include document analysis of the most common types of fraud targeting senior citizens and existing training and best practices to address the gap in technology training that put seniors age 60+ plus at risk of falling victim to technology fraud. Sources of data will include journal articles, government agencies, document analysis of existing training, as well as best practices to address the gap in technology training for senior citizens that put them at risk of technology fraud. The potential implications for public service practice are that this study will help those that are the focus of this issue to learn better ways to use technology. Every year, countless citizens aged 60+ become the target of technology fraud schemes, which cause the transfer of millions of dollars from unsuspecting individuals to criminals. It is thought that elderly persons have accumulated wealth, are naïve, have savings, may own property, and have excellent credit, which make them appeal to criminals (FBI, 2019; Munanga, 2019).

Significance

Key stakeholders are the seniors age 60+ who take part in the training, interested residents, and others seeking to improve their knowledge in this area. The study is significant in that it creates a model for computer technology pilot training directed at senior citizens that could later be expanded to other regions of the country. Training senior citizens in computer technology creates a greater sense of independence, fosters convenient commerce, improves interpersonal interaction, and increases digital citizenship. Wider potential contributions can make senior citizens more aware of safety when using technology, both in the community and in public administration. The potential for social change is that these technological skills would allow senior citizens to stay on top of circumstances that could change their personal situation. Added skills in this area would make a positive difference in the lives of seniors who want to preserve a decent quality of life.

Summary

Section 1 introduced my study, the problem statement, purpose, nature of the administrative study, and its significance. Section 2 will reintroduce the introduction, concepts, models, and theories to be used, and relevance of this study. It will also include the background, context, role of the DPA student/researcher, and summary.

Section 2: Conceptual Approach and Background

Adults over 60 years old are five times more likely to report losing money through technology fraud than younger people (FTC, 2019). They become victims of romance frauds (those seeking love and companionship), business fraud, investment swindles, tech support frauds fraudulent lotteries, sweepstakes, and prizes, and online shopping frauds (AARP, 2019). All these acts of fraud are committed against seniors causing them to unknowingly give away their property, money, and other valuables (Fletcher, 2019). This research seeks to determine the most common causes of fraud and the remedies to prevent seniors from becoming victims. A technology deliverable will be designed to aid interested adults 60+ in the pursuit of safe operation of personal computing technology and is a welcome change to supply safer operation of technology while online (SCC, 2021). The research question is "What are the important topics to address in the pilot training to prevent seniors from becoming victims of technology fraud?" The project creates a model for senior citizens 60+ that could later expand to other regions of the country. This section will present information on the conceptual framework needed to develop the training (specifically focused on learning styles of senior citizens), the relevance of the information to public and nonprofit organizations, and the role of the student researcher.

Concepts, Models, and Theories

Intro to theory

In AL theory Knowles (2005) argued that there are eight steps in the model of AL: a) learner training, (b) creating a helpful learning environment, (c) making tools for joint preparation, (d) finding learning needs, (e) creating content to fill needs, (f) design learning skills, and (g) leading or superior design using better methods and resources, (h) evaluating outcomes and reviewing needs. Further, according to Lindeman, a major contributor to the field of AL, (a) adult learning is life-long, (b) adult learning is not solely occupational, (c) adult learning focuses on situations rather than subject matter, and (d) adult learning is primarily focused on learner experiences (Nixon-Ponder, 1995). The aim is to help learners gain skill and knowledge in their target areas. AL can be adaptable to limitless formats and purposes such as technology and academic pursuits. Older adults want programs designed especially for them, and a need exists to set up technology programs specifically prepared for this group (Guo, 2017).

Characteristics of adult learning

Adult learners display various characteristics as they learn. They are practical, focusing on what applies to their personal learning needs, they bring all their former experiences, as well as all earlier knowledge, with them as they learn new subjects (Abdul-Aziz, 2014). Also, they are self-driven, moving toward what they need and want to learn. Based on AL, adult learners prefer to study subjects that offer a choice of how instruction takes place, self-sufficiency, self-directed learning, and a signal as to where the learning is going (Arghode, 2017). Moreover, learning cannot achieve the desired result unless it is appealing, useful, has an attractive arrangement, subject awareness, and theory knowledge which are central to good training (Arghode, 2017). Engagement is central to understanding ways in which people learn, which has been shown through engagement with computer games. More knowledge in this area can help understand what increases learning success (Whitton, 2011).

How AL can be used to improve training and outcomes

Gaining knowledge about AL improves training and can improve future research in adult education. AL can be used to create learning models that will further improve the coaching of adults (Shrivastava, 2017). AL can be used to lift the ability of those who want to learn about technology (Peng, 2017). In a laboratory safety study, AL helped improve participants use laboratory equipment, decrease penalties for improper use of equipment, and save lives of laboratory workers (Gabraith, 2007). The key to teaching technology is collaboration among teachers, which differs from instruction in other subjects (Wisanugom, 2019).

Benefits of technology

Technology improves learning for adults, and the internet provides benefits (Abdul-Aziz, 2014). Learning is now free and available to anyone with access to the internet (Klein, 2020). Senior adults can use technology for entertainment, personal instruction, and regular tasks (Lawhon, 1996).

Relevance to Public Organizations

Seniors ages 60 + are the most vulnerable group affected by technology fraud. Technology fraud against seniors 60+ can range from people pretending to be relatives asking for financial help to sophisticated email activity requiring user identification and passwords. They are three times more likely to be exploited than adults ages 19 to 59. Recently, mature adults 60+ lost over $399 million in 2018 and filed more than 249,000 reports of fraud (Barry, 2019). Moreover, feelings of separation due to the COVID-19 pandemic have worsened the fraud situation. Nevertheless, technology does aid mature adults in remaining connected to family members (Jargon, 2021). There have been no previous efforts to address technology fraud in this organization. This is the first time a specialized study has been conducted for this nonprofit on any subject. Also, no strategies or standard practices have previously been used to address the problem of reducing the number of senior citizens attacked using technology fraud at this nonprofit entity.

Organization Background and Context

The Organization is a 501(c)(3) nonprofit organization whose mission in the community is education, to senior citizens who live in the eastern United States. The Organization was formed 50 years ago with a focus toward improving schools and public education in the local area. Further, there are several areas of community action that The Organization directs its energy for the community: (a) to inform the residents on community affairs, (b) prepare the neighborhood people for school reorganization through town hall meetings, (c) develop leadership skills to improve community schools in connection with the parent association and school boards, (d) create education teams in local block and civic associations and (e) work to create programs for preschool, elementary schools, higher education, vocational and technical studies, as well as basic adult education (Forum, 1979, p. 2).

The lack of computer technology training to reduce the number of adults 60+ victimized by technology fraud is an issue that has not been considered in The Organization. Technology fraud training is necessary to protect this group who are considering using technology. This training can be included in the nonprofit training;

however, it remains the choice of the board as to when it will be utilized (see LaLande, 2021).

Role of the Doctor of Public Administration Student/Researcher

My role is as an observer-participant and creator of this study for the nonprofit. I have no professional relationship with the nonprofit, neither am I a board member nor an employee or one who receives any form of salary or compensation for the creation of this study or for any reason do I receive any sort of gain or payment of any kind. In full disclosure, my sister is a member of the board of the organization. She suggested I contact the organization's founder in the hope of getting a study for the nonprofit.

My motivations are to aid the nonprofit in addressing the issue of technology fraud and to create a deliverable program that improves this issue for residents of the neighborhood as well as the greater nonprofit community. One potential bias is that I am an individual 60+ that is the target of technology fraud. Also, I live close to this community and desire to help people in my age group to improve this situation in any way possible. Taking on this research can aid others in this age group to expand their knowledge in the safer use of technology.

Summary

Section 2 addressed key concepts to the study, relevance to public organizations, organization background and context, and the role of the DPA student researcher. These sections provide a background for the remaining parts of the study. In Section 3, I will provide the data collection process and analysis for the study. Section 3 will address details as to how the study will proceed.

Section 3: Data Collection Process and Analysis

The problem addressed through this study is that adults over 60 years old are five times more likely to report losing money through technology fraud than younger people (FTC, 2019). By allowing scammers remote access to their computer, people hand over control, and scammers can steal sensitive information and gain access to their bank accounts (FTC, 2019). This research seeks to determine the most common causes of fraud and the remedies to prevent seniors from becoming victims. The problem can be improved by the creation of a technology deliverable to aid interested adults over 60+ years old in the pursuit of safe operation of personal computing technology. This section will discuss the practice-focused question, the sources of evidence, the research methodology, and data analysis process.

Practice-Focused Research Question

Adults over 60+ years old are five times more likely to report losing money to technology fraud than younger people (FTC, 2019), losing sensitive information and access to their bank accounts (Fletcher, 2019). Since no study in technology fraud has ever been studied in this nonprofit organization, a gap in knowledge exists. This study will address that gap and create a practical solution to the problem. A study may be beneficial to the residents of this local community, helping to reduce technology fraud. My practice-focused question is “What are the important topics to address in the pilot training to prevent seniors from becoming victims of technology fraud?”

Operational Definition of Technology Fraud

For this study's purposes, the word technology refers to the operation of a personal computer using the worldwide web, also known as the internet. The word *fraud* refers to misleading another person through false representation, false information, failing to disclose information, abuse of position, and perversion of truth to induce another to part with something of value (Eissa, 2014). For this study's purposes, the term technology fraud refers to the use of a personal computer to induce another to part with something of value or to surrender a legal right in the process. Technology fraud is the use of technology to commit cybercrime, and specified as any illegal act using the internet, a public, private, or in-house computer system. Further, it is a plan to conduct varied events conducted by one or more persons, to steal something of value and garner personal increase from these activities ("Technology Theft," n.d.).

Sources of Evidence

The sources of evidence I relied on were those that provided safe and practical operation of technology for seniors 60+. This included a document analysis from sources that specialized in the safe use of technology. Examples of these sources came from large nonprofit organizations, government resources, state, city, and university resources. These sources offered approaches to safe technology use and steps to follow when harm has been done.

This evidence aligns to the purpose as it addresses what others have done in this area of focus. Further, the evidence focuses on the needs of adults 60+ who have a desire to study the information that is the focus of this project. To reduce the number of seniors 60+ affected by technology fraud it is necessary for them to gain knowledge that will reduce the risk involved with using technology. Here, I examined the most common types of technology fraud. Then from the literature, I determined how others have solved this problem in their nonprofits, government agencies, educational institutions, and others. From this I gathered the best practices to incorporate into the study to reduce technology fraud for seniors 60+.

Published Outcomes and Research

The databases and search engines used to find outcomes and research related to the practice problem were Public Policy & Administration, Public Policy & Administration databases, and Soc INDEX with full text. Terms included *scams* OR *fraud, online* OR *internet* OR *web* OR *computer* OR *social media* OR *digital*, and *older adults* OR *older age* OR *elderly* OR *seniors* OR *geriatric* OR *60+* OR *65+*. This search gave me eight results.

Also, a quick search of *Scams Against Older Adults* resulted in an FTC report entitled "Scams and Older Consumers: Looking at the Data." According to the FTC, seniors 60+ are often defrauded by people pretending to be employers of the Social Security Administration (SSA) or the Internal Revenue Service (IRS). In a 12-month review between July 1, 2018, and June 30, 2019, more than 100 consumers aged 60+ reported that they lost more than $1,000 while interacting with people pretending to be federal FTC employees. These so-called employees promised grants, money, and prizes to unsuspecting consumers who paid a fee for service (FTC, 2019). Furthermore, internet fraud involving adults 60+ is quickly rising and includes deceitful telemarketers (Munanga, 2019). Moreover, individuals respond over the internet to misleading invitations, requests, notices, or they are misled into supplying confidential information or else capital, that initiates suffering a loss which is monetary, non-monetary or causes a type of damage to the intended victim (Cross, 2016).

Protections (Ethical Procedures)

Per Walden University requirements the research procedures were private during the data collection process. The data came from sources not directly connected to the agency being studied. They consisted of best practices and applied to my study. Privacy was maintained during the data collection process. The information was maintained on a separate drive and a personal journal. Also, this information will be stored for 5 years.

I also had a memorandum of understanding from the nonprofit giving me permission to conduct the study. Should any other forms be necessary in the future, I will obtain them with IRB approval (Walden University, 2022). My plan to share the results of the participants is via email. It will be shared only with those who need to know in the nonprofit agency.

There are no potential psychological, relationships, legal, economic/professional, physical, or other risks associated with this study. This study examined an issue not addressed and is not part of the organization. Therefore, there is no threat to the organization. Further, no threat existed regarding loss of privacy, distress, mental harm, monetary loss of damage to anyone concerning professional character or psychological harm. No conflicts of interest existed, and nothing in the study was designed to expose internal information concerning the entity. I hope this study will add something positive that the organization does not have now.

Analysis and Synthesis

The information in the articles were systematically analyzed using a thematic analysis, which helps identify specific observations using suitable language to discover meaningful ideas (Rosalia, 2022). Thematic analysis is a method for methodically recognizing, establishing, and introducing understanding into samples of meaning (themes) across a data set. This method identifies what is common to the way a topic is talked or written about and makes sense of those shared aims (Braun & Clarke, 2012). Using this method, TA permits the researcher to see and understand collective or shared meanings and experiences. In order to conduct the analysis, I completed the steps for qualitative data analysis (Adu, 2019): (a) get familiar with the data, (b) create initial observations, (c) look for facts, (d) review the information, (e) define or spell out what each idea is about, and (f) write up or report your findings (Maguire, 2017). I coded the data, developed categories and themes, and used those themes to develop the topics for the technology fraud protection training program The Organization can conduct for the senior citizens.

Steps in the Data Analysis

Became Familiar with the Data/Prepared to Code

After locating all the articles, I printed out each article and read the documents line by line looking for information on safe operation as well as fraud that is harmful to seniors using the internet. I highlighted the information I found looking for evidence pertinent to my study. Initially the information was broad. I found 34 sources of safe operation and 40 sources of fraud harmful to seniors using the internet. These sources came from government resources, journal articles, and news reports that have found safe ways for seniors to operate on the internet. For instance, fraudulent information demonstrates what to avoid staying safe while using the internet; harmful information can lead to theft of resources such as taking over a person's bank account. As I came across information regarding fraud or remedies, I highlighted the information to be used later in the analysis.

Looked for Facts/Review/Manually Assigned Codes to the Data

I developed two overarching categories: fraud and remedies. I developed a table in a Word document. One table was used for articles that contained information regarding a form of fraud, and one table was used for articles that contained information regarding a remedy (e.g., means to prevent fraud). I entered each article in the table (some articles were listed in both tables if they contained both causes of fraud and remedies). I listed the authors, title of publication, journal, year of publication, details, and topics. I looked for information that is useful for completing the thematic analysis like creating strong passwords, using chunks of data that support the research question, look for comparisons in the text that relate to safe operation like using secure websites, update your browser regularly, use anti-virus software, and communicating with known websites and more (Department of Homeland Security, 2012). It also includes things like avoiding romance fraud, where criminals pretend to be interested in starting a relationship; grandparent fraud, where the caller claims to be a grandchild asking for financial assistance; or the home repair fraud where persons ask for money up front to perform home repairs and more (FBI, 2019).

Reviewed Information/Developed Categories and Themes

Articles were coded into categories for the type of fraud identified (such as phishing, romance fraud, etc.). Each article was then sorted into specific categories and the information was explored in more detail. The data were recorded in a personal notebook, within my study document, and by a thumb drive. Collection of this data took place over 10 months between January and October of 2023. The data is also in the chart form that appears in this study. The 74 documents that I included in the study were broken into two groups: fraud and safe operation. These two groups were researched for the types of fraud that target senior citizens age 60+ as well as ways to protect those seniors who have little to no experience using internet devices using safe operation, which includes ways to keep seniors safer while using the internet. The data were recorded using thematic analysis.

Variations in the Data

There are no variations in the data. The data aligns to the subject and the research method. There were 40 sources related to fraud and 34 sources related to safe operation of internet devices that seniors use while working on the world wide web. In addition, there are no unusual circumstances encountered in the collection of the data mentioned in the previous section. All the data is collected from the documents I read while researching this subject. Further, there are no interviews since this study uses thematic analysis as the source of data collection.

Data Integrity

The credibility of the data will be the measure of success it demonstrates in keeping seniors 60+ safe while using technology. If the data proves valid in reducing technology fraud, then it is credible. Also, the data are credible if the nonprofit and participants believe the study provided appropriate value to the organization and the individual participants.

The measure of transferability is determined by how well the data obtained works in the local nonprofit. Another factor is whether others outside of this entity can use the same information and make it work for them. If so, then the data are both useful as well as transferable. Dependability relates to how consistently my data is applied to reveal the best sources of information to help seniors 60+ navigate technology more efficiently and effectively. If done effectively my goal will be achieved. Finally, the confirmability of the data will be determined by how the participants feel about what they have received from the study. The stated value given by individuals involves positively stating how they feel about the study, the researcher, and the information received, which lends confirmability to the study.

Summary

Section 3 discussed the practice-focused question, operational definition of technology, sources of evidence, protections, data integrity, and analysis and synthesis. Section 4 covers the study and results.

Section 4: Evaluation and Recommendations

The problem addressed in this study is that adults over sixty years old are five times more likely to report losing their money through technology fraud than younger people (FTC, 2019). By allowing scammers to gain remote access to their computers, senior adults hand over control, and scammers were then able to steal sensitive information and gain access to their bank accounts (Fletcher, 2019). The problem can be mitigated by the creation of a technology deliverable to help interested adults over age 60+ years of age in the search of safe operation of personal computing technology. The purpose of this qualitative study was to develop a computer technology pilot training program to reduce the number of senior citizens victimized by technology fraud. The practice-focused question is "What are the important topics to address in the pilot training to prevent seniors from becoming victims of technology fraud?" The project may hold significance for other groups in the creation of a model for senior citizens, 60+ years old, that could later expand to other areas of the country. Training senior citizens in computer technology creates a better sense of independence, fosters convenient commerce, interpersonal interaction, and prudent digital citizenship.

Findings and Implications

Data Related to Technology Fraud

I found and read 40 articles on fraud involving seniors age 60+. These sources were separated into groups with similar characteristics. For example, phishing appeared 10 times in the literature, romance fraud appeared seven times, tech support appeared seven times, identity theft appeared six times, impostor fraud and government fraud is combined as they have similar characteristics and appeared four times. Also, lottery fraud appeared four times, malware and ransomware combined as they have similar characteristics, and this category appeared four times in the literature. Moreover, credit card fraud appeared four times, and social media fraud appeared four times in the literature. Table 1 contains a summary of the information found during the document review process.

Table 1

Summary of Document Findings

Author	Year	Concepts	
Cross, M.	2020	Romance Fraud Exploitation Fear	Nancy and Brad are trying to trace how Rochelle got under the spell of a seductive caller. (p. 1)
Blackwood-Brown, C.	2021	Phishing Email Fraud Unsecured Wireless Internet Use Perceived risk of identity theft	Phishing targets internet users by going around safety measures resulting in damaging losses and theft. (pp. 1,2)
Cross, C.	2016	Phishing Email Fraud Romance Fraud Investment Fraud Advanced Fee Fraud Inheritance Fraud Lottery Fraud	They were defrauded during what they thought was a romantic relationship. (p. 3)
Sugunaraj, N.	2022	Tech Support Fraud Phishing Email Fraud Confidence-Sweetheart-Romance Fraud Identity Theft Fraud	Fraud is conducted via 6 general types: Sweepstakes, Tech Support, Confidence-Sweetheart-Romance, Phishing, Identity Theft, Overpayment (p.1)
Burnes, D.	2017	Elder Financial Abuse (Funds improperly used by trusted person) Elder Financial Fraud Scams (Acts perpetrated by a stranger)	"…elder financial abuse happens when the elder persons resources are used improperly or illegally" (p. e14)
Payne, B. K.	2020	During Covid-19 Unscrupulous Contractor Fraud Fraudulent Lenders Fake Charities Fraud Elder Abuse Fraud Patient Abuse Fraud Impostor Fraud Romance Fraud Online Shopping Fraud	Fraud is common after tornadoes, hurricanes, and other disasters. Unscrupulous contractors, fraudulent lenders, and fake charities surface after these events (p. 2)
Yuxi Shang	2022	Consumer Fraud False Claims About the Past Trust Level	older persons might be overly accepting of false claims about the past, like "you forgot to pay me"
FBI	2018	Telemarketing Credit Card Scam	A telemarketing credit card fraud defrauded 60,000 victims many elderly of more than $18 Million
Fletcher, E.	2019	Romance Fraud	Fraudsters use phony internet profiles, fake photos, false names, and are active on dating sites. People 40-69 reported losing money via romance frauds at extremely high rates (p. 1, 2)
Burton, A.	2022	Phishing Email Fraud False Emails Fraudulent Text Messages Financial Fraud	Phishing emails take users to websites that download viruses, steal passwords, banking specifics, and sensitive information.
Ali, M. A.	2019	Stolen Personal Information Fraud Phishing Email Fraud Private Information Transfers Card Payment Fraud Ransomware Fraud Mobile Payment Fraud Unauthorized Access to Data Fraud	Debit/Credit Card Fraud, email hacking, social media hacking, disclosing confidential information (p. 409)

Author	Year	Concepts
Lee, N. M.	2018	Phishing Email Fraud Imposter Email Fraud Fraudulent Fundraisers Fake Survey Fraud Social Media Not Fact Checked Fraud Distorted Facts Fraud Misinformation Fraud Political Polarization Fraud
Teller Vision	2019	Fear Mongering Fraud Pop-Up Claiming Computer is Infected with Viruses or Malware Fraud Fraudsters Add Malware or Steal Financial Accounts
Sannd, P. & Cook, D.	2018	Phishing Email Fraud, Ransomware Fraud, Limited Digital Experience
Teller Vision	2023	Online Shopping Fraud Lottery Fraud Investment Fraud Bogus Cryptocurrency Fraud Sweepstakes Fraud
Schmidt, M. K., Stowell, N F., Pacini, C., & Patterson, G.	2022	Financial Fraud- A Trusted Adult Knowingly Takes the Funds, Assets, or Property of Another With the intent to deprive the vulnerable adult of use
Banerjee, S., Kapatanaki, A. B., & Dempsey, L.	2022	Mistaking Misinformation as Truth Purposely Confusing Disinformation, Inaccurate Information as Truth Causing Poor Decision Making
Alvarez, L.	2023	Person on the phone fraud Romance Fraud Tech Support Fraud Government Imposter Fraud Cryptocurrency Fraud
Munanga, A.	2019	Telemarketer Fraud Government Official Fraud Desperate Email Fraud
Meder, T.	2022	Nigerian Scam 2.0 Email Fraud Mail Fraud
Cowood, F.	2022	Government Imposter Fraud Energy Fraud (Grants for Solar Panels) Green Fraud Pension Fraud Investment Fraud
White, C. M., Gummerum, M., Wood, S., & Hanoch, Y.	2017	Offenders use information gathered in chat rooms using social media, Networking Websites, and Lifestyle-Routine Activities for bad purposes. Cybercrime is most likely to take place when the subject is close to determined criminals. Targets do not have proper protection in place.
Wild, K., Marcoe, J., Mattek, N., Sharma, N., Loewy, E., Tischler, H., Kaye, J., & Karlawish, J.	2022	Financial Activity and inadequate thinking online can make older adults a target of financial fraud.
Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L.	2010	Poorly Controlled Settings Provide Inadequate User Support and Weak Observation Toward the Protection of Assets. (Ex. Libraries, Senior Centers or in the home).
Crosman, P.	2021	Social Media Fraud Ongoing Theft from a bank account by a trusted inner circle member

Author	Year	Concepts
DeLiema, M., Deevy, M., Lusardi, A., Mitchell, O. S.	2017	Invested after a free meal Purchased a fraudulent investment recommended by a third party Someone used or attempted to use an individual account without permission
van Paridon, E.	2022	Senior Care Services Scams Provide Healthcare Scams, Sell Antiques Scams Offer Pension Insurance Scams Help in Making Investments Scams
Azam, N. A., Buja, A. G., Darus, M. Y., Sahri, N. M.	2022	Phishing Email Fraud Identity Theft Fraud Romance Scams Tech Support Fraud Credit Card Fraud
Godfrey, D.	2020	Sweepstakes Scams, Business Opportunity Scams Tech Scams Imposter Scams
Karagiannopoulos, D. V., Kirby, D. A., Oftadeh,-Moghadam, S., & Sugiura, D. L.	(2021)	Hacking Accounts, Malware, Ransomware, Phishing, Virus, Insurance Fraud, Fake Emails, Poor Cyber Literacy, Lack of Understanding the Risks
Kemp, S., & Erades Perez, N.	2023	Telemarketing Scams, Investment Scams, Lottery Scams, Tech Support Scams, Banking Fraud, Bait and Switch Fraud, Fake Invoice Fraud, Fake Government or Service Provider Fraud
Ianzito, C.	2022	Account Takeover Fraud, New Account Fraud, Identity Theft, Phishing, Malware
Daily Record	N, D.	Identity Fraud, Synthetic Identity Fraud (Combining Real and Fictitious Information to Create New Identities)
Friedman, A. B., Pathmanabnan, C., Glickman, A., Demiris, G. Cappola, A. R., McCoy, M. S.	2022	Shadow Health Record (Browsing histories are linked to purchase histories and publicly accessible data sets like names and email addresses which can connect with the actual identity of the web searcher)
Wattles, J.	2017	Tech Fraud (Pop-Up adds that inform people that their computers are falsely infected with viruses)
Huey, L., & Ferguson, L.	2022	Identity theft, Advance Fee Fraud, Illegal Access to Individual Information, Loss of Privacy, Information Misuse
Sugunaraj, N., Ramchandra, A. R., Ranganthan, P.	2022	Sweepstake Fraud, Technical Support Fraud, Phishing, Identity Theft, Overpayment Fraud, Confidence/Sweetheart/ Romance Fraud
Faluyi, B. I., Fele, T., & Ayeni, A. O.	2022	Phishing
Parti, K., & Tahir, F.	2023	Winnings Schemes (Imposters inform the mark that they have won something) Buying Schemes (Fraudster pretends to want to buy something from the mark, but the mark should pay them some cash in advance) Company Fraud (Imposter poses as a well-known company, bank or organization and asks for payment in gift cards, money or pay for offered service) IT Support Scam, Grandparent Scam, Romance Scam, Identity Check Scam (An email tells the reader that they will be detained if they fail to pay a ransom)
Computer & Internet	2018	Investment Fraud, Identity Theft, Trusted

Lawyer		Family Member, Caretaker of Guardian Theft	
Research Summary for Safe Operation			
Department of Homeland Security	2020	Create passwords that mean something to you. Use strong passwords eight at least characters. Secure your surroundings. Limit the sharing of personal information and use privacy settings. Install a security program and update regularly. Never use a public computer for banking information (libraries, hotels).	Passwords, Social Media Limit online personal information (p. 1)
FBI	n.d.	When an internet offer is made resist acting too fast check it out online for comments from others about fraudulent activity. Fraud actors like to create the need for urgency. Identify fraud efforts online search for the name, phone, email, and address of the contact. Make certain your antivirus, spyware, malware, and security information are constantly updated. Disconnect and shut down your device if you are attacked by pop-up messages.	Know your contactor, obtain contact information, call police if you feel threatened (p. 1)
Ianzito, C.	2022	Do not reuse passwords. Choose passwords that are meaningful to you as well as illogical to others. Create a unique username (User I.D.). Use your email address for a username only if necessary. Create an alert when transactions are made from your accounts. Review your three credit bureaus regularly every three months to make certain no one has used your personal information. Learn about the newest fraud and fraud activity.	Never use the same password on every website (p.5-8).
Fletcher, E.	2019	Do not connect to any links or pop-ups on screen advising you of a computer issue. Reject calls from people offering tech-support. Do not rely on caller ID if it can be deceived. At no time give over control of your computer or reveal passwords to anyone calling you. Keep security software updated. For assistance personally contact your own technician. Do not trust an online search. If you were defrauded change your passwords, run a software scan for malware. If you shared your credit card number with a scammer, call your card issuer immediately. See if the card company will reverse or remove the bogus charges. Check your card statement to verify the removal of the charges.	Avoid pop-ups, tech-support calls, unreliable caller ID (p. 2,3).
Blackwood-Brown, C.	2021	Senior citizens are one of the highest at-risk classes of internet users that are susceptible to cyberattacks. This is mostly because of their reduced knowledge and skills concerning the internet. For this reason, computer security (safety) training is needed to combat or deter the incidents they encounter.	Computer Security training is needed to deter the attacks encountered (p. 195).
Burton, A.	2022	Cybersecurity awareness training 1-2 hours face to face. Workshops, presentations, videos, demonstrations, and hands on activities.	Skills against attacks increased. Cyber-Guardians (instructors) to collaborate with participants most helpful. (p. 10).

Author	Year	Concepts	
Schmidt, M.	2022	In financial firms' meaningful technology can be used to detect unusual flag activity thereby preventing cyberfraud (internet fraud, stealing	One program is the EverSafe App used by several financial firms (p. 1234).

		from client investment accounts).	
Azam, N. A.	2022	A program to improve the cyber-awareness of senior citizens. There are five basic cyber-attacks on seniors: Phishing, identity theft, romance frauds, tech support fraud, and credit card fraud. Seniors have five learning styles in this study: Through a questionnaire the research team mapped the learning styles. They are Vision color-based, vision sharpness-based, hearing-based, physical, or movement-based, and information processing-based.	The study seeks to reduce attacks by making seniors more aware using theory, education, and practical means to reduce attacks.
Wattles, J.	2017	The FTC (Federal Trade Commission) says that it is initiating 16 more administration activities, along with complaints, settlements, indictments, and guilty pleas against tech fraudsters. …" there are still more scammers out there, and regulators need the public's help to catch them."	"The only way we're going to stop this is if you report it." (p. 1,2).
Beijing Review	2022	China started a national initiative to stop fraudsters posing as technical support analysts defrauding senior citizens. Appropriate agencies should investigate these crimes and, if fraud is found, act. Also, an efficient way to prevent and prevent these crimes needs implementation. Seniors should report these crimes to other seniors if it happens to them. Also, they should immediately report the crimes to the proper authorities. Children should look out for grandparents who are not as tech savvy.	Seniors should create anti-fraud teams. Communities and local governments should work together to stop these crimes. (p. 1,2).
Alvarez, L.	2023	Speak to older family members and explain the exact approaches that fraudsters may use to attempt to steal their money. Communicate with them not to give out any confidential information to unfamiliar persons online or by telephone. Tell them never to send money to anyone until they contact you first. To report fraud, call the National Elder Fraud Hotline: 1-833-372-8311.	Do not provide personal information even when they know you
Sugunaraj, N.	2022	Using strong passwords, multi-factor identification (two or more), antivirus software, pop-up blockers, and Federal Trade Commission blacklists aid seniors in preventing fraud online.	Strong passwords, MFA's, Antivirus software, Pop-up blockers, FTC blacklists (p. 625).
Karagiannopoulos, D. V.	2021	Family and friends are a helpful asset to have in combating online fraud. One person stressed the help on local police in his area who had been helpful. The most often helpful tool noted in this study is anti-virus software.	Expert help is helpful in the fight against cybercrime (p. 5).
Guha E. M.	2020	To become a safe Facebook user and protect your account against cybercrime: Use strong passwords that combine capital as well as small letters, including numbers 0-9 and characters like % * ^ &. Also use two factor notification such as email and a registered cell phone. Do not send or ask for friend requests from unknown people. Change the password three or more times per month. Never log in on another person's device. Limit the number of people for each post. Never share a One Time Password or Facebook password. Delete One Time Passwords after using.	Safety Tips for Facebook use (p. 122).

Author	Year	Concepts	
Buja, A. G.,Siti Dealeela, M. W., The	2021	To help the elderly learn about online security a program was developed called (OSICSAM)	Conducting hands-on lab. Gathering groups of the same age. Campaigns

Faradilla, A. R., Deraman, N. A., Mohd Nor Hajar, H. J., & Azian, A. A.		organization social and individual cyber security awareness model. It has six steps and considers the learning styles of older adults. (1) Situation Awareness-Oriented Cyber Security Education, (2) Peer Education Model, (3) Security Awareness Model, (4) Information Security Awareness Capability Model (ISACM), (5) Cyber Security Capability Maturity Model, (6) Information Security Awareness Program (ISAPM) General Model.	centered on cyber security along with instruction. A forum with experts with materials for the target group etc. (516).
Kisekka, V., Chakraborty, R., Bagchi-Sen, S., & Rao, H. R.	2015	Another issue that arises in online safety for seniors is self-efficacy, or personal belief that an individual can complete a certain task. In this case self confidence in safely using the internet. For example, if many pop-ups occur and the person does not manually disable third party cookie by default, a lack of safety exists on the current website. Also, if the website asks for too much personal information to use the website this too is a safety issue or unsafe condition, and the person should not use the site.	Safety of a website (p. 161).
Soomro, T. R., & Hussain, M.	2019	To prevent phishing, user friendly methods such as OTP's (one-time passwords) and CAPTCHA's, digital certificates, as well as generic and characteristic designed and anti-phishing processes. These are easy to use and provide defense against phishing attacks.	Preventing Social Engineering and Phishing (p. 13).
Guha, E. M.	2020	In case you get logged out of the social media account, you can select 3 to 5 friends to help you recover your account. Create strong passwords. Two step verification is a way to keep safe online (example: password and phone call or coded message by cellphone). Face recognition is an additional way to have a safer online experience.	Security features (p. 119).
Azam, N. A. (19)	2022	Online security consciousness involves making internet users aware of online threats as well as improving their safety so they can be fully on guard while using the internet. Information Security Awareness Capability Model (ISACM) is a blend of online safety awareness and best practices. It involves awareness risk, awareness capability, and awareness importance. Awareness risk means determining whether awareness import is greater than awareness capability. Awareness import means taking steps to avoid becoming a victim. Awareness capability means a person's skill in avoiding a problem.	ISACM is an educational program to help older adults be safer on the internet (p. 119).
Holguin-Alvarez, J. (20)	2021	This study revealed that digital competencies can be improved through didactic training (training with the motive to teach something). In this study digital competencies (digital technologies for information and basic problem solving) were increased 30 points through this digital training. Training provides safer and more informed internet experiences.	Training improved digital competencies (p. 188, 193).

Author	Year	Concepts	
Lemos, R. (21)	2017	Despite knowledge of cyber-attacks and security breaches many online users still do not use a two-factor authentication to log in to their internet accounts. In addition, many people are unaware of this type of online protection that is available to help reduce cyber-attacks. This means receiving a text or SMS message to a registered cell phone as a second authentication.	Two-factor authentication (p. 1, 2).
States News (22)	2018	Cyberpatriot, a program of the United States Airforce and United States Space Force, created a program teaching cybersecurity for seniors, adults, teenagers, and all interested persons. The program teaches tips and tricks to guard against online threats (cyberthreats). It also informs the public about cybersecurity problems, cybersecurity breaches and more. The presentation can be found at www.uscyberpatriot.org or 877.885.5716.	The US Airforce and US Space Force issue a new program called Cyberpatriot (p. 3,4).
Zulkipli, N. H. N. (23)	2021	To mitigate cybersecurity for the elderly the writer recommends the following: Education in use of the internet is effective especially for everyday users. Keep updating software. Installing and using anti-virus and spyware is crucial to protect the elderly online. Secure access to accounts. This means establishing two-factor authentication (login) when it is offered. Do not send personal information to strangers. Use strong passwords, a combination of upper- and lower-case letters, numbers, and symbols. Do not use social security numbers, birthdates, or ID numbers or guessable passwords. Avoid answering emails that request your personal information. Avoid suspicious links in an email. If a financial institution requests information calls them and discuss issues over the phone.	Education in use of the internet, keep software updated, use anti-virus and spyware program, establish two-factor authentication (p. 1779).
Kisekka, V. et al.	2015	Web browsing safety efficacy (WSE) among older adults is the focus of this study. Efficacy is the ability to achieve an intended result. WSE among older adults is the individual's belief that he/she can achieve the intended skill or action required to use the internet safely. To improve online safety for older adults the author suggests the use of visual cues. Examine the URL (universal resource locator or web address), to see if the user's personal information will not be misused. Install spyware or third-party cookie that tracks browsing behavior. Many browsers warn about malware or if an https certificate has expired. Also, if too many pop-ups are launched then there is a lack of safety on the website. Install anti-virus program.	Examine the URL, install spyware, install third party cookie that tracks browser behavior (p. 161).
Bach, E.	2022	2020 was a year that over 3 million dollars was lost to cyberattack fraud. The participants in the study have a basic knowledge of cybersecurity. However, some will still face cyberattacks in the future due to lack of knowledge. Furthermore, the students stated that if they had a class while they were in school dealing with this subject their understanding of this subject would be greater than it is currently. So, more education is needed to improve cybersecurity.	Lack of digital education (p. 9).

Author	Year	Concepts	
Coventry, L.	2022	This study demonstrated that for this group of seniors, they were knowledgeable about proactive checking for risk, generating strong passwords, securing their device when idle (locking the screen).	Proactive checking for risk, generating strong passwords, securing the device when it is idle (p. 9).
Rogoyski, A.	2018	Passwords should be 12 characters long. They need to consist of numbers, symbols, capital, and lower-case letters. These should never be a dictionary word, combination, or words, or substitute a 0 (zero) for the letter O. Also, the time will come when passwords are no longer necessary. Fingerprint, iris, and facial recognition will control future access to systems.	Password Safety (p. 1, 2).
Shillair, R.	2022	Some things that have improved cybersecurity are cybersecurity education, awareness raising and training (CEAT) have made a noticeable improvement.	Improvement in cybersecurity (p. 2).
Narayanan, V.	2021	Seniors using social media are attacked using misinformation/disinformation attacks. A way to improve safety here is to fact-check the information that was received. Also, use a dynamic network that captures how the information evolved over time, a method to discover information attacks. This is an orderly way to help those individuals subject to information attacks.	Improve information attacks on social media (p. 299).
Frik, A.	2019	Among older adults' difficulty in using technology whether due to user-unfriendliness (difficulty for users to understand) or to personal lack of knowledge (unfamiliarity with the information) leads to a lack of confidence using technology. Removing the barriers to using technology is an important part in enabling older adults to use technology more easily and securely.	Remove the barriers to safety (p. 31).
Irshad, S., & Soomro, T. A.	2018	Safety (Prevention Techniques) 1)Never display personal or financial information online. If you choose to post pictures of documents, blur out both names and identifying numbers. 2) Do not use automatic log in for any reason. Never let browsers remember your log in information. This blocks fraudsters from getting access to your confidential information. 3) Do not post locations or physical locations online. Doing so let's criminals know you are not home and puts you at risk. 4) Arrange privacy settings so that only you or people you trust can see your photo, birthdate, workplace, and name. 5) Use two-factor authentication (log in) for example a password and a code number. 6) Use strong passwords combining alphanumeric features and special characters to thwart criminals. 7)Use different passwords for each of your personal accounts and keep them in a safe place. 8) Never save credit card information online to avoid identity theft. 9) Prevent use of geo-tagging (tagging) photos. This is a form of tracking to show people where you have traveled. 10) Use identity protection services like LifeLock and others to guard against identity theft. 11) Some social media services provide alert detection when someone logs on to your account. Use this to prevent unwanted access to your account.	Stay safe using social media (pp. 50, 51).

Author	Year	Concepts	
Huey, L., & Ferguson, L.	2022	Digital competences could improve general safety in understanding the strength of retired individuals regarding both financial as well as non-financial fraud.	Obtaining digital knowledge.
Cain, A. A., Edwards, M. E., Still, J. D.	2018	In this study the authors found that the following items need improvement to raise digital safety.: Older and younger people share too much personal information on social media, do not check their privacy settings, share their phone numbers and addresses. Also, authors found that more than 90% of people create passwords eight or more characters long, more than 80% use upper- and lower-case moticharacters, and more than 70% use special characters. Further, more than 80% use personal information when creating passwords.	Results (pp.39, 43).
Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N.	2022	Higher cyber security awareness improves digital security. Cybersecurity awareness can be described as low, medium, and high. Low awareness involves not paying close attention to or ignoring security alerts. These alerts are provided by the application when using Wi-Fi with laptop computers or mobile devices. Medium awareness involves carelessness caused by improper technological operation. High awareness is demonstrated by knowledge of cyber threats and skilled action to prevent harm.	Security hazard awareness (p. 83).

Technology Fraud Concepts

The concepts for Fraud are Phishing, Romance, Tech Support, Identity Theft, Impostor Fraud/ Government Impostor Fraud, Lottery Fraud, Malware/ Ransomware Fraud, Credit Card/ Social Media Fraud a total of seven concepts. Phishing, Romance, Tech Support, and Impostor/ Government Impostor fraud represent a theme that causes the mark (senior citizen) to provide valuable information to the fraudster to steal something of value from the senior citizen. This theme causes fear and exploitation of elderly victims (Cross, M. 2020; Cross, C. 2016). There are multiple ways that seniors can be harmed while using the internet by the above examples of Phishing, Romance Fraud, Tech Support Fraud, and Impostor/Government Impostor Fraud. I will explain what each one of these examples can mean in terms of danger while using the internet.

Phishing Fraud. This is delivered in the form of email messages. To further explain and email messages are free to send and are sent to an inbox instead of a mailbox. To send a message you need to include a From, To, and a date, and one of the email client products that come installed on a personal computer. Phishing is targeted at internet users and circumvents security measures resulting in theft and financial losses. Further, Phishing fraudsters use email to direct targets to websites that use viruses, steal passwords, banking information and other sensitive information causing serious harm to victims. Also, fraudsters hack email accounts, social media, debit, and credit card information, as well as disclose other confidential information. Those using this type of fraud to attack seniors also engage in fraudulent fundraisers, fake surveys, distorted facts, misinformation, political polarization, and social media fraud that is not fact checked for accuracy (Lee, 2018; Pallen, 1995; Blackwood-Brown, 2021; Burton, 2022; Ali, 2019).

Romance Fraud. To explain further Romance Fraud is where two people meet over the internet looking for a positive romantic connection. They may use a dating website and add a short biography of personal information they choose to share with anyone who is also looking to make a romantic connection for love, companionship or more. Further, Romance Fraud can take place on dating sites on the worldwide web. After a while, the fraudster will share with the online love interest that they have fallen on challenging times. This news of falling on tough times is accompanied by the request for financial assistance like cash, gift debit cards or more. At this stage of the relationship the mark has developed feelings for the fraudster and complies with the request for the items of value. This fraud can continue for a period of time accumulating to hundreds or thousands of dollars in lost valuables. In some cases, the mark is so embarrassed and ashamed that they do not report the crime to the proper authorities. They accept the loss, shame, and disillusionment as their own fault (Cross, 2020; Cross, 2016; Payne, 2020; Fletcher, 2019; Alvarez, 2023; Azam, 2022; Sugunaraj, 2022; Faluyi, 2022).

Impostor/Government Impostor Fraud. This takes place when a fraudster pretends to be a well-known or popular company (Impostor) or a well-known government agency (Government Impostor). To elaborate, the person using this fraud will contact the intended target on very official looking messages. They will for example use a fraudulent letterhead of a government agency with a fake return address. Due to the official look of the message, the receiver of the message is more likely to respond to the message and get entangled in fraud. Online offenders often employ this type of fraud. The email catches the mark off guard since the message is official and legitimate in its appearance. The person receiving the message needs to examine it carefully for misspelled words and grammar errors. Also, verify the return address of the sender. The offender will ask for money by credit card claiming the senior citizen owes taxes, and that the senior must respond immediately to avoid additional penalties or a lawsuit. These are fear tactics used by offenders to get you to comply with their request for immediate payment. However, government agencies always use US Mail to conduct official business. All official correspondence shows the agency, address, and on some a penalty for fraudulent use on the front of the envelope (Alvarez, 2023; Munanga, 2019; Cowood, 2022; Kemp, 2023; Meder, 2022).

Ransomware. This takes over control of the target computer and the fraudster demands payment to release control of the computer back to the owner. Ransomware places a virus, or it corrupts the computer of the target making the device unusable. I placed Ransomware and Malware in a theme together as both target the computer in the fraud. In this way they behave similarly. Ransomware is a virus that takes control of a computer. It is aimed at individuals but can be sent to businesses or agencies as well. It is intended to harm an individual or computer system. Its goal is to seize, or grab hold of a computer, holding the device for ransom not allowing the user to do anything on the device until a ransom is paid to the attacker for release of the device functionality. Ransomware comes in the form of a virus or software that takes over control of the target device rendering it useless until the requested payment is paid to the offender. Once the ransom is paid, the sender of the attack may return control of the device to the owner. The device may operate normally after the release is paid or may require the assistance of an expert (Ali, 2019; Karagiannopoulos, 2021).

Malware. It is sent to a device to damage the target computer. Like Ransomware it is a virus or type of software sent by an offender. However, in this case the purpose is not to take over control of the device. To explain further the purpose of a Malware attack is to damage the target device so that it cannot be used at all. However, an expert can repair the damage and make the device operate normally again (Ianzito, 2022; Teller Vision, 2019).

Identity Fraud. The attacker illegally obtains personal identification documents such as a driver license or passport to gain access to the target individuals’ finances or credit. Identity Fraud/Identity Theft is another type of dangerous attack that can take place during internet usage. It can happen to anyone, and senior citizens are often targeted using this type of strike. It is thought that because seniors have lived a long time, they have acquired an abundance of resources. For this reason, seniors are singled out for this type of fraud. To clarify, perpetrators obtain information about specific individuals over the dark web. The dark web is a place on the internet where sensitive personal information is obtained and sold for a price. For example, a fraudster may buy information on the dark web such as a person's driver license. They will then use that information to create a fake driver license substituting their own photo on the license then use that identification to make large or small purchases pretending to be the person whose identity was stolen. In addition, the offender may use the same information to make a false passport or to open a credit card account. The senior citizen may not be aware that this theft has happened until they receive notification from the police, a bank, a car dealership, or some other entity that someone has attempted to use their information to facilitate some type of business transaction. At this point, after checking further the senior citizen is thrown into a panic and now must notify his/her creditors that yes, he/she is a victim of fraud. Now, all the pieces of private property and information must be changed to avoid further damage to protect the senior citizen (Sugunaraj, 2022; Azam, 2022; Ianzito, 2022; Daily Record, n.d.; Huey, 2022; Computer & Internet Lawyer, 2018).

Credit Card Fraud. This takes place when a fraudster takes possession of your credit card information or the physical card itself. To further explain, senior citizens are targeted as it is thought that these individuals have obtained significant resources over many decades of working and living. Obtaining the card information can happen by means of a trusted family member or friend who gets the information and makes purchases that the owner does not know about. This fraud can also happen by means of the dark web, by skimming the card information at the point of sale in a store, or by wirelessly gathering the numbers on the card by someone in close proximity to the owner of the card while it is on his/her person (FBI, 2018; Ali, 2019; Azam, 2022).

Social Media Fraud. When personally identifiable information is posted on social media platforms. For example, when anyone posts addresses, dates, times, places and other valuable information, fraudsters can use it to attack personal assets. This data can be researched to help an offender to commit a crime. Moreover, no person should ever post when they are going on vacation and when they are returning. Also, it is not safe to store credit card data online, and user identification and passwords should not be stored online. Many people use Social Media platforms. Performing these unsafe practices can easily result in the loss of money and property. Also, when setting up any Social Media account or other online account the best practice is to use strong passwords. It is best to use eight or more characters when setting up a password. The stronger the password, the better your personal safety online is. Furthermore, I think do not store account numbers or passwords on the device itself. These items should be kept in a safe place that is not located on the device for personal protection (Lee, 2018; White, 2017; Crosman, 2021).

Forty sources of fraud were acquired in the research. These forty were reduced to ten sources based on similarity or likeness to each other. In addition, these were placed into a table of fraud sources and are found in ‘Table 1’ which appear in this study. These sources were the most prevalent that I obtained in the research. Moreover, I am moving on to Safe Operation and examine the data further. The concepts for Safe Operation further clarify what is needed to determine the best items to include in my study to keep seniors safer while they are using the world wide web.

Safe Operation Concepts

I found thirty-four different articles on Safe Operation. These were separated into themes. The themes were further reduced to Passwords, Security, and Training. These categories are the most important part of staying safer while using the internet.

A password is like a key that opens a door. Passwords must open an internet account to send or receive messages. So, passwords need to be strong, including eight or more characters in length. When you create a password, it should mean something to the person who created it. Also, never share a password with others (Department of Homeland Security, 2012). Further, do not reuse a password. This means that a different password should be created for each account. At the same time, create a unique User ID which is separate from a password. Never use your email address for a User ID unless required by the website. Make certain that the password you select is personal and do not use it for another account. A password needs to include capital letters, lower case letters, numbers, and symbols such as %, *, ^, and & (Ianzito, 2022; Guha, 2020).

Security is also important when seniors or anyone uses the internet. It is good practice to take the following steps for personal security. These steps are especially important and can make a difference regarding personal safety on the worldwide web. If seniors take these precautions, they will be safer as they conduct their affairs while using the internet. Seniors should not quickly accept any offers made on the internet. This is dangerous. First, they should see what others are saying about the offer, do some fact checking to see if this is a legitimate offer, legitimate company, product and learn all they can before accepting it. Further, it is advisable to know the contactor, and to look for the name, phone number, and email address of the one making the offer or making the contact. Moreover, it is best to use antivirus, spyware, and malware programs to minimize the danger of the internet. Also, make certain that these programs are continuously updated (FBI, n.d.).

Pop-ups are another issue that occurs on the internet. These pop-ups may look like small clouds that suddenly appear on your computer screen offering to fix problems on your device. The sender will offer to fix a problem that does not exist. Seniors should not reply to these messages. Pop-ups and technology support (tech support) requests should be avoided. Seniors should not connect to any links sent to them for this purpose. All security programs such as antivirus or spyware and the like should be constantly updated. If a senior age 60+ does become defrauded on the internet, he/she should run a malware scan and if a credit card number was shared the credit card company should be called as soon as possible to see if they will reverse the charges (Fletcher, 2019).

Also, seniors need help from knowledgeable people to explain the exact approaches that fraudsters may use to attempt to steal their valuables. In addition, in China a nationwide initiative was conducted to stop those people who prey on seniors posing as Technical Support analysts. Seniors should report these crimes to other seniors if it happens to them, and they should immediately report these crimes to the proper authorities. Further, it was determined that children should support or assist their grandparents that are not technology savvy (van Paridon, 2022). Seniors need to be reminded not to give any personal information online or by telephone. In addition, they should never send money to anyone unless they speak to a trusted friend or family member first and report all crime to the National Elder Fraud Hotline. Moreover, the local police department is a helpful source in combating fraud involving senior citizens (Alvarez, 2023; Karagiannopoulos, 2021).

Further, about security online for seniors, two factor identification should be employed for internet accounts, change the password often, do not login on another individual's device, never share a one-time or a Facebook password, and delete one-time passwords after using. To increase safety, one-time passwords and CAPTCHA’s, digital certificated, and anti-phishing processes should be employed as they are easy to use against phishing attacks (Guha, 2020; Soomro, 2019).

Computer security training is necessary to lessen or deter the attacks that senior citizens experience on the internet. Since seniors are one of the highest risk groups of internet users that are susceptible to cyber-attacks due to insufficient knowledge concerning the internet, for this reason computer security training is needed to fight against the attacks they face while online (Blackwood-Brown, 2021).

Also, the basic cyber-attacks on seniors using the internet are phishing, identity theft, romance fraud, tech support fraud, and credit card fraud. Seniors have five learning styles, vision color based, vision sharpness-based, hearing based, physical or movement based, and information based. Programs that improve cybersecurity are using in person training 1-2 hours, workshops, presentations, and hands on activities improve online skills (Burton, 2022; Azam, 2022).

In addition, digital education improves cybersecurity for seniors. Digital knowledge can be mitigated by hands-on training with the aim of teaching something useful. One study found that digital training for basic problem solving improved by one third through appropriate training. Also, a program teaching cybersecurity instructing all interested persons, teaches tips and tricks to guard against cyber-threats, problems, breaches, and other related problems (Holguin-Alvarez, 2021; States News, 2018).

Moreover, some students state that if they had taken a class while they attended school dealing with this subject, their understanding would be greater than it is currently. Hence, more training is required to improve the security of seniors suing the internet. Subjects like cybersecurity education, awareness raising, and training have made visible increases in this area (Bach, 2022; Shillair, 2022).

Recommendations

Using Adult Learning Theory, the training for senior citizens should be a course that will teach them how to avoid fraud while utilizing the internet, as well as what to employ regarding safe operation using the internet. This knowledge will help them to remain safer on the worldwide web. There are eight steps in the Adult Learning Theory (AL) model. The steps are (a) learner training, (b) creating a helpful learning environment, (c) making tools for joint preparation, (d) finding learning needs, (e) creating content to fill needs, (f) design learning skills, (g) leading or superior design using better methods and resources, (h) evaluating outcomes and reviewing needs. The point is to help learners gain skill and knowledge in their target areas. AL is flexible and can adjust to limitless purposes. It is also useful in technology and academic pursuits (Knowles, 2005).

AL has many uses for instructing older adults. At the same time, it allows for flexibility as it considers that people have different learning styles. A survey conducted over a year and a half on learning discovered that older adults want programs designed specifically for them, and a need exists to design technology programs specifically for this group. Adult Learners like to study subjects that offer a choice of how instruction takes place, self-sufficiency, self-directed learning, a clue as to the direction the learning is taking as well as its desired result appeal and usefulness. Other considerations include course appeal, arrangement, subject and theory knowledge which are central ingredients to good training. Further, AL can be employed to create learning models depending on the purpose and acquiring understanding about AL improves training and future study in adult education. AL concepts can be employed to create learning models and improve the training of adults. allAdult learners focus on their personal need for learning, they are practical, they use all their personal capabilities and previous knowledge as they learn new skills. Also, AL in concert with technology uncovered that a need exists to attain abilities that can solve daily challenges. Currently, AL is targeted at learning centered on professional as well as personal requirements. In addition, senior adults can use technology (computers) for personal instruction, entertainment, and knowledge of technology is useful to all people who need to know how to use it. Moreover, AL is life-long, not exclusively work-related, situational rather than subject oriented, focuses on learner skills (Guo, 2017; Arghode, 2017; Shrivastava, 2017; Peng, 2017; Abdul-Aziz, 2014; Klein, 2020; Lawhon, 1996; Nixon-Ponder, 1995).

Course Outline

1.What is the internet? – 10 minutes

a. How does it work? – 10 minutes

2. What is internet fraud? – 10 minutes

a. What are the dangers of internet fraud? – 15 minutes

3. What is safe operation on the internet? – 15 minutes

a. How does safe operation work?

Break – 10 mins

b. How to send and receive email – 10 minutes

c. How to create a word document – 10 minutes

d. How to pay bills online – 15 minutes

Questions

End

The course should be ninety minutes twice a week and should be in person. Students will need some personalized attention to make a good start. This is a basic course for those who do not have a lot of internet experience. However, if the student cannot attend in person, they can attend using Zoom for convenience.

Implications for Positive Social Change

The implications for possible social change are that this course can be used as a guide to help those who need this information to succeed where they were not able to before. In addition, the course can be expanded, improved, and used as a model and a springboard to help the community stay safe, stay abreast of changes in technology, and to function faster as well as better in our constantly changing society. Further, the course and document can be used as a template to apply for grant money which will help the organization and the community grow and thrive. This can assist them in getting their fair share of the American Dream, which is to prosper, and to pursue happiness.

Strengths and Limitations of the Project

The study is only as strong as the accuracy and validity of the sources provided in the project. This project aims to help adults 60+ to use the internet in a prudent, safe, and productive way. It provides 40 sources of fraud which are to be avoided while on the internet. While no effort to protect is one hundred percent guaranteed this effort is a good beginning to provide knowledge of the internet and safety while using the worldwide web.

Limitations of the project are that this information is basic and does not cover all circumstances that may arise while a senior citizen is operating a device which connects to the internet. However, the project allows for future improvements on this topic from those who participate in it as well as those who are interested in creating something that benefits seniors 60+ and other interested people with an interest in this subject.

Section 5: Dissemination Plan

This study will be disseminated with my recommendations and findings to the nonprofit with an executive summary. I will provide a synopsis of the problem along with my findings and my recommended solution to improve on the current situation. In addition to the executive summary, I will provide a draft basic course on safe operation on the internet which also entails four basic internet operations. This course can be used at the discretion of the nonprofit.

The study and its findings will also be shared with a larger audience who has a comparable need within their own organization and find that they could benefit from a program for their nonprofit or their community residents. The organization can use this information to expand whatever is next for them and the community. Further, the study can be shared and published through board direction, classes at the nonprofit location, and other necessary means of dissemination that benefit the nonprofit organization and academia.

Summary

This study focuses on creating a way to help senior citizens 60+ with little or no knowledge of internet safety to operate more carefully while using the internet. Many seniors have been hurt mentally, emotionally, and financially by using the internet in an unsafe manner. While no one can guarantee complete safety on the internet, this study provides information that will help to make internet operation safer, better, and easier for seniors 60+ who use the worldwide web.

References

Abdul-Aziz, M., Ibrahim, M., Jono, H. Asarani, N. (2014). Incorporating instructional design and adult learning theory in the e-content development of an interactive multimedia course. In *International symposium on technology management and emerging technologies* (pp. 296–301). https://doi.org/10.1109/ISTMET.2014.6936522

Adu, P. (2019). *A step-by-step guide to qualitative data coding*. Routledge Publishing.

Ali, M. A., Azad, M. A., Centeno, M. P., Hao, F., & van Moorsei, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems*, *100*, 408–427. https://doi.org/10.1016/j.future.2019.03.041

Alvarez, L. (2023, February 8). The elderly are targets. My family learned too late how to fight scams. *Washington Post*. https://www.washingtonpost.com/opinions/2023/02/08/elderly-scams-protections-targets-finances/

Anderson, R., & Gilbert, S. (2022). Legislating for online safety. *Intermedia (0309118X)*, *50*(2), 8–12. https://www.bennettinstitute.cam.ac.uk/publications/online-safety-bill/

Arghode, V., Brieger, E. W., & McLean, G. N. (2017). Adult learning theories: implications for online instruction. *European Journal of Training and Development*, *41*(7), 593–609.

Azam, N. A., Georgiana-Buja, A., Darus, M. Y., Masri Sahri, N. (2022). SCAM-elderly:

A new synergistic cyber security model for the elderly for IR4.0 readiness in Malaysia. In *2022 IEEE 12th symposium on computer applications & industrial electronics* (pp. 117–122). https://doi.org/10.1109/ISCAIE:54458.2022.9794521

Bach, E. (2022). *The impact of digital literacy on the cyber security of digital citizens.* Varazdin Development and Entrepreneurship Agency (VADEA).

Banerjee, S., Kapetanaki, A. B., & Dempsey, L. (2022). Older people's online information search during the pandemic. In *2022 16th International Conference on Ubiquitous Information Management and Communication* (pp. 1–6). https://doi.org/10.1109/IMCOM53663.2022.9721773

Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2021). Cybersecurity awareness and skills of senior citizens: A motivation perspective. *Journal of Computer Information Systems 61*(3), 195–206. https://doi.org/10.1080/08874417.2019.1579076

Buja, A. G., Siti Daleela, M. W., The Faradilla, A. R., Deraman, N. A., Mohd Nor Hajar, H. J., & Azalan, A. A., (2021). Development of organization, social and individual cyber security awareness model (OSICSAM) for the elderly. *International Journal of Advanced Technology and Engineering Exploration, 8*(76), 211–519. https://doi.org/10.19101/IJATEE.2020.762185

Burnes, D., Henderson Jr, C. R., Sheppard, C., Zhao, R., Pillemer, K., & Lachs, M. S. (2017). Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis. *American Journal of Public Health, 107*(8), e13–e21. https://doi.org/10.2105/AJPH.2017.303821

Burton, A., Cooper, C., Dar, A., Matthews, L., & Tripathi, K. (2022). Exploring how, why, and in what contexts older adults are at risk of financial cybercrime victimization: A realist review. *Experimental Gerontology, 159*. https://doi.org/10.1016/j.exger.2021.111678

Cain, A., Edwards, M., & Still, J. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*. 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

City Health Profiles. (2003). Community health profiles. https://www1.nyc.gov/assets/site/doh/pdf/data-publications/profiles-2003-community-health-profiles.page

Cowood, F. (2022, November 27). Four scams targeting older people – and how to beat them. *The Telegraph Online.* https://www.telegraph.co.uk/christmas/2022/11/27/four-scams-targeting-older-people-how-beat/

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches [5th ed]*. Sage Publications.

Crosman, P. (2021). Small bank pilots' software to protect older customers from fraud. *American Banker*, *186*(212), 5–7.

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends & Issues in Crime & Criminal Justice, 518*, 1–14. https://aic.gov.au/publications/tandi/tandi518

Cross, M. (2020). Watch out for the elder fraud web. *Kiplinger's Personal Finance,* *74*(1), 40–45.

DeLima, M., Deevy, M., Lusardi, A., & Mitchell, O. (2017). Exploring the risks and consequences of elder fraud victimization: Evidence from the health and retirement study. https://deepblue.lib.umich.edu/bitstream/handle/2027.42/142373/wp374.pdf?sequence=4

Department of Homeland Security. (2012). Cybersecurity and older Americans. https://cisa.gov/sites/default/files/publications/Cybersecurity%20and%20Older%20Americans.pdf

Eissa, A., Wells, K. C. C., & Rudoff, N. (2014). *Fraud: A practitioner's handbook*. Bloomsbury Publishing.

Faluyi, B., Fele, T., & Ayemi, A. (2020). Impact of ICT-facilitated fraud on Sustainable Socio-economic Development in Nigeria. *Journal of Education and Social Development*, (December 2020) 23-27. Doi: 10.5281/zenodo.4362253

Fair, L. (2019). Scams and older consumers: Looking at the data. Retrieved from: Scams and older consumers: Looking at the data | Consumer Advice (ftc.gov).

Federal Bureau of Investigation. (2018). Elder Fraud. Senior Citizens Victimized in Telemarketing Scheme. Retrieved from: https://www.fbi.gov/news/stories/senior-citizens-victimized-in-telemarketing-scheme-112618.

Fletcher, E. (2019). Older adults are hardest hit by tech support scams. Retrieved from: http://www.ftc.gov/news-events/blogs/data-spotlight/2019/03/older-adults-hardest-hit-tech-support-scams.

Forum. (1979). Social Concern Committee of Springfield Gardens, Inc. *Special anniversary edition. A decade of community service.* 4 (3) Summer/Fall 1979.

Friedman, A., Pathmanabhan, C., Glicksman, A., Demiris, G., Cappola, A., McCoy, M. (2022). Addressing online Health Privacy Risks for Older Adults: A Perspective on Ethical Considerations and Recommendations. Gerontology and Geriatric Medicine. 2022;8. Doi:10.177/23337214221095705

Frik, A., Nurgalieva, L., Bernd, J., Lee, J., Schaub, F., & Egelman, S. (2019). Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)* (pp. 21-40). Retrieved from: https://www.usenix.org/system/files/soups2019-frik.pdf

Federal Trade Commission. (2019). Scams and the older consumer: Some surprising findings. Retrieved from: https://www.ftc.gov//business-guidance/blog/2019/10/scams-older-consumer-some-surprising-findings

Federal Trade Commission. (2019). Scams and older consumers: Looking at the data. Retrieved from: https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2018-2019-report-federal-trade-commission/p144401_protecting_older_consumers_2019_1.pdf

Federal Trade Commission. (2022), Use Two-factor Authentication to Protect Your Accounts. Retrieved from: https://consumer.ftc.gov/articles/use-two-factor-authentication-protect-your-accounts#Turn

Gailbraith, D. D., & Fouch, S. E. (2007). Principles of Adult Learning. *Professional Safety, 52(9),* 35-40.

Godfrey, D. (2020). Scams Targeting Older Consumers. *The Voice of Experience,* NA. Retrieved from: https://link.gale.com/apps/doc/A628079444/EAIM?u=minn4020&sid=ebsco&xid=ba4618fd

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older Adults' Knowledge of Internet Hazards. *Educational Gerontology, 36*(3). 173-192. Retrieved from: https://doi.org/10.1080/03601270903183065

Guha, E. M. (2020). A Study on Facebook Security Features updated with its development and Popularity. *Research Journal of Engineering and Technology, 11*(2), 118-122. Retrieved from: https://doi.org/10.5958/2321-581X.2020.00021.5

Guha, E. M. (2020). A Study on Facebook Security Features updated with its development and Popularity. *Research Journal of Engineering and Technology, 11*(2). 118-122. https://doi.org/10.5958/2321-581X.2020.00021.5

Guo, P. (2017). How Adults Ages 60+ Are Learning to Code. *Communications of the ACM, 60 (8),* 10-11.

Huey, L., & Ferguson, L. (2022). What do we know about senior citizens as cybervictims? A rapid evidence synthesis. *CrimRxiv*. Retrieved from: https://www.crimrxiv.com/pub/itssosrv

Holguin-Alvarez, J., Garay-Rodriguez, P., Amasifuen-Sanchez, V., Acha, D. M. H., Castillo, F. F. L., Cruz-Montero, J., & Ledesma-Perez, F. (2021). Digital Competences in the Elderly and University Students: Didactic Interaction from the Use of Social Networks. *International Journal of Emerging Technologies in*

Learning, 16(4), 188-200. https://doi.org/10.3991/ijet.v16i04.18519

Ianzito, C. (2022). Money can be stolen from your bank account: Here’s how to lower your risk. Retrieved from: https://www.aarp.org/money/scams-fraud/info-2022/bank-account-theft.html?intcmp=AE-FRDSC-MOR-R2-POS3

Irshad, S., & Soomro, T. R. (2018). Identity theft and social media. *International Journal of Computer Sciences and Network Security 18*(1). 43-55. Retrieved from: http://Identity-Theft-and-Social-Media.pdf (researchgate.net)

Jargon, J. (2021). How to Protect Seniors From Online Fraud and Phone Scams. Retrieved from: http//wsj.com/articles/how-to-protect-seniors-from-online-fraud-and-phone-scams-11611410401

Kampfen, F., & Maurer, J. (2018). Does education help “old” dogs learn “new tricks”? The lasting impact of early-life education on technology use among older adults. *Research policy. 47*(6), 1125-1132.

Karagiannopoulos, D. V., Kirby, D. A., Oftadeh-Moghadam, S., & Sugiura, D. L (2021). Cybercrime awareness and victimization in individuals over 60 years: A Portsmouth case study. *Computer Law & Security Review, 43,* N.PAG. https://doi.org/10.1016/j.clsr.2021.105615

Kemp. S., & Erades Perez, N. (2023). Consumer Fraud against Older Adults in Digital Society: Examining Victimization and its Impact. *International Journal of Environmental Research and Public Health. 20*(7). Retrieved from: https://doi.org/10.3390/ijerph20075404

Kisekka, V., Chakraborty, R., Bagchi-Sen, S., & Rao, H. R. (2015). Investigating Factors

Influencing Web-Browsing Safety Efficacy (WSE) Among Older Adults. *Journal of Information Privacy & Security, 11*(3), 158-173 https://www.proquest.com/scholarly-journals/investigating-factors-influencing-web-browsing/docview/17322126245/se-2.

Knowles, M. S., Holton, E. F., & Swanson, R. A. (2005). *The adult learner. [electronic resource}: the definitive classic in adult education and human resource development* (6th ed.). Elsevier.

Lee, N. M. (2018). Fake News, Phishing, and Fraud: A Call for Research on Digital Media Literacy Education beyond the Classroom. *Communication Education, 67*(4), 460-466.

Lemos, R. (2017). The Vast Majority of Users Don't Use Two-Factor Authentication: Survey. *EWeek*, 1.

Maguire, M., & Delahunt, B. (2017). Doing a Thematic Analysis: A Practical, Step-by-Step Guide for Learning and Teaching Scholars. Dundalk Institute of Technology. Retrieved from: http://ojs.aishe.org/index.php/aishe-j/article/view/335

Meder, T. (2022). THE NIGERIAN SCAM 2.0 How an improved online scam trick made an unsuspecting Dutch man over 20,000 euros poorer. *Studies in Oral Folk Literature / Estudis de Literature Oral Popular, 11.* 47-60 Retrieved from: https://doi.org/10.17345/elop202247-60

Munanga, A. (2019). Cybercrime: A New and Growing Problem for Older Adults. Retrieved from: https://doi.org/10.3928/00989134-20190111-01

Nixon-Ponder, S. (1995). Leaders in the Field of Adult Education. Retrieved from:

www.files.eric.ed.gov/fulltext/ED380667.pdf

Narayanan, V., Robertson, B. W., Hickerson, A., Srivastava, B., & Smith, B. W. (2021). Securing social media for seniors from information attacks: Modeling, detecting, interviewing, and communicating risks. *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2021 Third IEEE International Conference on, TPS-ISA 297-302.* Retrieved from: https://doi.org/10.1109/TPSISA52974.2021.00053

NYSED. (2020). Demographic Information. Retrieved from: https://data.nysed.gov/enrollment.php?year=2020&county=34

Office of Justice. (1976). Federal Prison System, 1976/ Office of Justice Programs. https://www.ojp.gov/ncjrs/virtual-library/abstracts/federal-prison-system-1976

Parti, K., & Tahir, F. (2023). “If We Don’t Listen to Them, We Make Them Lose More than Money.” Exploring Reasons for Underreporting and the Needs of Older Scam Victims. *Social Sciences (2076-0760). 12*(5), 264. Retrieved from: https://doi.org/10.3390/socsci12050264

Payne, B. K. (2020). Criminals Work from Home during Pandemics Too: a Public Health Approach to Respond to Fraud and Crimes against those 50 and above. *American Journal of Criminal Justice, 45(4), 563-577.* https://doi.10.1007/s12103-020-095532-6

Peng, C. Cao, L., & Timalsena, S. (2017). Gamification of Apollo lunar exploration missions for learning engagement. *Entertainment Computing, 10,* 53-64.

Range, L. M. (2021). Case study methodologies. In *Salem Press Encyclopedia of Health.*

Rogoyski, A. (2018). A password to the future. *Computer Fraud & Security. 2018*(3). 8-10. Retrieved from: https://doi.org/10.1016/S1361-3723(18)30023-X

Rudestam, K. E., & Newton, R. R. (2015). *Surviving your dissertation: A comprehensive guide to content and process (4th ed).* Sage.

Sannd, P., & Cook, D. M. (2018). Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and Phishing Attacks. *2018 Fourteenth International Conference on Information Processing (ICINPRO). Information Processing (ICINPRO). 2018 Fourteenth International Conference On*, 1-5.

Schmidt, M. K., Stowell, N. F., Pacini, C., & Patterson, G. (2022). Senior financial exploitation through wills, trusts, and guardianship: basics, red flags, and prevention measures. *Journal of Financial Crime, 29*(4). 1222-1240. https://doi.org/10.1108/JFC-10-2021-0225

Shillair, R., Esteve-Gonzalez, P., Dutton, W., Creese, S., Nagyfejeo, E., von Solms, B. (2022). Cybersecurity education awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, Volume 119, 2022. Retrieved from: https://doi.org/10.1016/j.cose.2022.102756.

Shrivastava, S. R., & Shrivastava, P. S. (2017). Employing Adult Learning Theories in Designing a Module. *Research and Development in Medical Education*, 2, 64

Sookhanaphibam, K. (2020). Cybersecurity Awareness Learning System via Thai

MOOC. *2020 IEEE 2nd Global Conference on Life Sciences and Technologies (Life Tech), Life Sciences and Technologies (Life Tech), 2020 IEEE 2nd Global Conference On*, 398-399. https://doi.org/10.1109/LifeTech48969.2020.1570620294

Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. *Appl. Comput. Syst. 24*(1), 9-17.

Special to The Daily Record. (n.d.). Fraud Facts: A new form of theft Synthetic Identity Fraud. *Daily Record, The (Rochester, NY).*

States News (2018). Cyberpatriot launches senior citizens' cyber safety initiative. Retrieved from: https://link.gale.com/apps/doc/A564312192/EAIM?u=minn4020&sid=ebsco&xid=05d220dc

Sugunaraj, N., Ramchandra, A. R., & Ranganathan, P. (2022). Cyber Fraud Economics, Scam Types, and Potential Measures to Protect U. S. Seniors: A Short Review. 2022 *IEEE International Conference on Electro Information Technology (EIT). Electro Information Technology (EIT). 2022 IEEE Informational Conference On, 623-627*. https://doi.org/10.1109/elT53891.2022.9813960

Technology theft. (n.d.). https://fraud.net/d/technology-theft/#:~:Technologytheftcanbedescribed,personalbenefitfromthoseactions

Teller Vision. (2019). Fraud Alert: Tech Support Scams Target the Elderly. *Teller Vision, 1506*.8.

Teller Vision. (2023). FTC Looks at Age Factors in Scam Activities. *Teller Vision, 1548,* 8.

van Paridon, E. (Ed.) (2022, June 15). How to protect seniors from online fraud? *Beijing Review*. https://www.bjreview.com/China/202206/t20220615_800297004.html

Wattles, J. (2017). Don't fall for this computer virus scam. *CNN Wire.*

White, C. M., Gummerum, M., Wood, S., & Hanoch, Y. (2017). Internet Safety and the Silver Surfer: The Relationship Between Gist Reasoning and Adults Risky Online Behavior. *Journal of Behavioral Decision Making, 30*(4), 819-827. Retrieved from: https://doi.org/10.1002bdm.2003

Whitton, N. (2011). Game Engagement Theory and Adult Learning. *Simulation & Gaming, 42(5),* 596-609

Wild, K., Marcoe, J., Sharma, N., Loewy, E., Tischler, H., Kaye, J., & Karlawish, J. (2022). Online monitoring of financial capacity in older adults: Feasibility and initial findings. *Alzheimer's & Dementia: Diagnosis Assessment & Disease Monitoring, 14*1), 1-5. Retrieved from: https://doi.org/10.1002/dad2.12282

Wisanugom Nammungkhun, Napaporn Yutthaisong, & Wanphakorn Jumphonnoi. (2019). What Teachers learned from STEM Education Project: Case Study of High School Teachers. *Journal of Physics: Conference Series. 1340(1).* 1.

Yuxi Shang, Zhongxian Wu, Xiaoyu, Du, Yanbin Jiang, Beibei Ma, & Meihong Chi. (2022). The psychology of internet fraud victimization of older adults: A systematic review. *Frontiers in Psychology, 13.* https://doi.org/10.3389/fpsyg.2022.912242

Zheng, Y., Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., Briggs, P. (2022).

Exploring Age and Gender differences in ICT Cybersecurity Behavior. Human Behavior and Emerging Technologies. Hindawi. Retrieved from: https://doi.org/10.1155/2022/2693080

Zulkipli, N. H. N., Md Rashid, M. A. Zolkeplay, A. F., & Buja, A. G., (2021). Synthesizing Cybersecurity Issues and Challenges for the Elderly. *Turkish Journal of Computer and Mathematics Education, 12*(5), 1775-1782. https://www.proquest.com/scholarly-journals/synthesizing-cybersecurity-issues-challenges/docview/2623049570/se-2

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge, and Behavior: A Comparative Study, Journal of Computer Information Systems, 62:1, 82-97. https://doi.org/10.1080/08874417.2020.1712269