Protecting the Elderly from Cybercrime:  
A Community Education Approach  
A master’s thesis  
Submitted to the Faculty of  
American Public University System  
by

Sydney Brazeau

In Partial Fulfillment of the

Requirements for the Degree of

Master of Science in Cybersecurity Studies

July 2020

Capstone Professor:

Dr. Elliott Lynn

The author hereby grants the American Public University System the right to display these

contents for educational purposes.

The author assumes total responsibility for meeting the requirements set by United States

copyright law for the inclusion of any materials that are not the author’s creation or in the

public domain.

© Copyright 2020 by Sydney Brazeau

All rights reserved

DEDICATION

I dedicate this project to my husband, whose patience, encouragement, and love helped make this project possible.

ACKNOWLEDGMENTS

I would like to thank Kathy Trump for fostering my critical thinking skills in middle school and high school and for her love and support along the way. I would also like to acknowledge my cat Luca’s contributions for sitting on my keyboard. Finally, I would like to thank my dogs, Rosie and Denali, for remining me to take breaks.

Table of Contents

[Table of Contents iv](#_Toc46074220)

[Introduction 1](#_Toc46074221)

[**Overview of Issue** 1](#_Toc46074222)

[**Project Overview** 2](#_Toc46074223)

[**Methodology** 2](#_Toc46074224)

[**Definitions** 3](#_Toc46074225)

[Literature Review 5](#_Toc46074226)

[**Generational Communication** 5](#_Toc46074227)

[**Use of Computers and the Internet by the Elderly** 8](#_Toc46074228)

[**Cybercrime Victimization of the Elderly** 11](#_Toc46074229)

[**Senior Citizen Cybersecurity Education Frameworks and Programs** 20](#_Toc46074230)

[Methodology 30](#_Toc46074231)

[**Variables** 30](#_Toc46074232)

[**Case Studies** 31](#_Toc46074233)

[**Data Collection and Sources** 31](#_Toc46074234)

[**Analysis Procedures** 32](#_Toc46074235)

[**Limitations and Bias** 32](#_Toc46074236)

[Analysis 32](#_Toc46074237)

[**H1. There are no generational barriers to effective communication with senior citizens.** 32](#_Toc46074238)

[**H2. Senior citizens see no benefit from the integration of technology into their lives.** 33](#_Toc46074239)

[**H3. There are no psychological factors that increase fraud victimization in the elderly.** 34](#_Toc46074240)

[**H4. Senior citizens do not engage in risky cybersecurity practices.** 35](#_Toc46074241)

[**H5. Senior citizens do not regularly encounter financially detrimental cybercrimes.** 36](#_Toc46074242)

[**H6. Senior citizens cannot mitigate cybersecurity issues by themselves.** 36](#_Toc46074243)

[**H7. Senior citizens do not encounter barriers when asking for help with cybersecurity issues.** 36](#_Toc46074244)

[Curriculum Packet 37](#_Toc46074245)

[**Sample Lesson Plan** 39](#_Toc46074246)

[**Cybercrime Handout** 41](#_Toc46074247)

[**How to…** 42](#_Toc46074248)

[Quiz 48](#_Toc46074249)

[**Quiz Answer Key** 49](#_Toc46074250)

[**Framework** 51](#_Toc46074251)

ABSTRACT

Protecting the Elderly from Cybercrime:  
A Community Education Approach

by

Sydney Brazeau

Master of Science in Cybersecurity Studies

American Public University System

Dr. Elliott Lynn, Capstone Professor

Cyber based scams and fraud disproportionately affect the elderly due to both increased targeting and psychological factors. The Internet serves as a resource for senior citizens to connect with friends and family, as well as access information about their health and finances The increased reliance on the Internet for communication and connection leaves senior citizens vulnerable to cybercrime, especially cyberfraud. Protecting the elderly from cybercrime requires interagency communication, accessible mental health resources, and community education. Through reviewing the relationship between senior citizens and cyber issues and analyzing the current frameworks, this project develops a cybersecurity community education program and adaptable framework tailored to the needs of senior citizens. The curriculum includes a lesson plan, a short quiz, a cybersecurity reference handout, an assisted notes handout, and a slide show presentation. The included framework will allow the curriculum to be updated as new cyber threats and scam trends emerge.

**Introduction**

The elderly are a common target for cybercriminals, as exploitation of the elderly presents less challenges for criminals than in comparison to other age groups. According to the Association of Certified Fraud Examiners, persons age 65 and over are often targeted for scams because they are more trusting, willing to listen, and are often lonely (ACFE, n.d.). This project develops a curriculum to teach the elderly how to protect themselves against cyber scams by focusing on effective communication techniques based on studies of generational and cultural communication styles. The result is a curriculum featuring a packet of information including handouts, a quiz, an adaptable lesson plan, and a slide show presentation. The packet will also include a framework for developing cybersecurity curriculum for senior citizens, which can be used to build, update, and adapt instructional materials to the cybersecurity and cybercrime landscape of the future.

**Overview of Issue**

Senior citizens often fall victim to fraud. José González of Utica College points out that even though senior citizens make up 15% of the United States population, they account for 30% of fraud victims (2019). Investment fraud, fake tech support, and romance scams are some of the commonly used schemes against the elderly in the U.S., according to the FBI’s Internet Crime Complaint Center’s (IC3) 2019 report (IC3, 2019). IC3’s 2019 report states that for the over 60 age group, there were 68,013 reported victims in the (United States?) with a total financial loss of $835,164,766 for some time period (IC3, 2019). The most common category of cybercrime was phishing, vishing, smishing, and/or pharming with 114,702 victims overall (IC3, 2019).

As for communicating with the elderly, Regis College compiled a list of 10 helpful tips for communicating with senior citizens. The list includes building rapport, showing proper respect, recognizing sensory difficulties such as hearing or vision loss, using plain language, and showing empathy (Regis, n.d.). The project integrates these concepts into the curriculum, such as allowing time to build rapport, defining unclear terms, avoiding the use of jargon, and providing large-print handouts of course content.

**Project Overview**

This project is a 1-hour cybersecurity curriculum for senior citizens that can be distributed to community education programs. The content focuses on how seniors can protect themselves from common cybercrimes and developing an increased cyber literacy. The project evaluates and builds educational material around the most effective communication methods, styles, and techniques for those over age 65. Effective communication will be combined with data from the most common and detrimental cybercrimes targeted at the elderly in order to provide an applicable curriculum. In addition to providing content relevant to the seniors of today, this project will provide an adaptable framework for future cybercrime education.

**Methodology**

The primary method of information collection will be through a literature review of the current state of the art research into generational communication. The project synthesizes the information gathered through the literature review and applies it in a curriculum packet which can then be distributed to senior citizen community programs.

**Literature Review.** The literature review uses peer reviewed papers and dissertations in order to gather data to support the methods and information contained in the curriculum packet. The literature review also draws from government agencies such as the FBI and senior citizen groups such as AARP. The data drawn from academic sources and relevant, trustworthy sources focuses on persons age 65+ in the United States. Data from other age groups or locations is presented in order to show contrast with the targeted group.

**Information Synthesis.** The literature review examines effective communication methods for the elderly, common scams targeted at them, and cybersecurity precautions that they can take to protect themselves. This information is condensed and applied in the curriculum packet. The literature review aims to answer the following questions:

1. Are there generational barriers to effective communication with senior citizens?
2. Do senior citizens benefit from the integration of technology into their lives?
3. Are there psychological factors that increase fraud victimization in the elderly?
4. Do senior citizens engage in risky cybersecurity practices?
5. Do senior citizens encounter financially detrimental cybercrimes?
6. Can senior citizens mitigate cybersecurity issues by themselves?
7. Do senior citizens encounter barriers when asking for help with cybersecurity issues?

**Curriculum Packet.** The curriculum packet provides a lesson plan and content, a take-home handout, an assisted notes handout, a quiz, and a slide show presentation. The lesson plan discusses the target audience, learning objectives, supplies needed, technology requirements, preparation work, and class activities. The lesson plan is divided into time allotted for an activity, a description of the activity, and the purpose or expected outcome of the activity. The target audience of the lesson plan is the instructor of the community education program. The take-home handout provides a large print quick reference guide for senior citizens who have attended the training and their families and friends. It includes tips on how to avoid cybercrime along with steps to take in the case of cybercrime victimization. The assisted notes handout provides the class information in printed form along with areas to take notes. This provides a more active and involved learning experience. The quiz is intended to be taken at the beginning of the class and has ten questions to start the class thinking about cybersecurity and cybercrime. The slide show presentation provides the core content for the class and uses largeprint, easy to understand language. Technical terms will be defined at the beginning of the slide show presentation and will be revisited when they become relevant.

**Definitions**

**Anti-virus.** Anti-virus software scans for a computer known malware and suspicious activity on a computer and removes it (Christensson, 2010). Anti-virus software requires consistent updates to stay relevant (Christensson, 2010).

**Clickbait.** Clickbait is a headline or title that makes a reader want to click a link, especially a link that leads to malware or website of little value or interest (Merriam-Webster, n.d.).

**Cyber threat actors.**  Individuals or groups who seek to take advantages of vulnerabilities and persons with low cyber schema in order to access sensitive information (Canadian Centre for Cyber Security, 2018).

**Cybercrime.** A crime that involves the use of a computer or the internet (Dennis, 2019). Common cybercrimes include identity theft, fraud, intellectual property theft, or privacy violations (Dennis, 2019).

**Cybercriminal.** A person or group of people that commit cybercrime (Dennis, 2019).

**Malware.** According to the FTC, “Malware includes viruses, spyware, and other unwanted software that gets installed on your computer or mobile device without your consent” (2015). Malware in its various forms can crash devices, monitor online activity, remotely control computers, make a computer or mobile device vulnerable to viruses and adware, steal personal information, send spam, and commit fraud (FTC, 2015).

**Operating system.** The software that allows a computer or digital device to run programs (Christensson, 2016).

**Phishing.** Phishing is when scammer use e-mail or text messages to trick a victim into giving out personal information such as passwords or banking details (FTC, 2019).

**Ransomware.** Malware that encrypts a victim’s files and promises to send the decryption key if a ransom is paid (Fruhlinger, 2020). The ransom is commonly paid in Bitcoin (Fruhlinger, 2020).

**Social engineering**. Josh Frughlinger of CSO Online writes, “Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data” (2019).

**Literature Review**

The following literature review provides an understanding of how to effectively communicate with the elderly and understand the issues that make them vulnerable to cybercrime. It surveys how the elderly communicate and process information as compared to millennials and younger generations. The effect of generational identity and culture are considered. It also examines existing senior citizen cybersecurity frameworks and workshops. Furthermore, it lists guiding principles for presenting information to the elderly including text and content guidelines. The literature review draws from international and U.S. based sources, using peer reviewed academic sources, previous capstone and dissertation projects, and data from the U.S. government and the American Association of Retired Persons.

**Generational Communication**

Nadeza Sivricova and Elena Moiseeva of South Ural State Humanitarian Pedagogical University in Chelyabinsk, Russia explore inter-generational communication and values (2018). Sivricova and Moiseeva note that while generational theory attempts to explain numerous differences in how people work, learn, consume, and connect, scientific research often falls short on supporting these theories (2018). Generational identity is more so a reflection of the experiences of a community, culture, and country (Sivricova & Moiseeva, 2018). Generations refer both to the historical period and environment of a group of people (Sivricova & Moiseeva, 2018). To illustrate this point, in the United States, generations are apportioned into Veterans, Baby Boomers, Generation X, Generation Y, Generation Z (Sivricova & Moiseeva, 2018). In Russia, generational identities are divided into Soviet, transitional, and Post-Soviet (Sivricova & Moiseeva, 2018).

The stereotypes of a person’s age and generation play into how society sees them and how they see themselves (Sivricova & Moiseeva, 2018). The idea of generational values creates a stereotype such as the stereotypes of youth and maturity (Sivricova & Moiseeva, 2018). For example, youth are expected to have the characteristics of activity and innovation while mature individuals are expected to be wise and experienced (Sivricova & Moiseeva, 2018). Youth prefer to use information technologies in order to communicate while the elderly prefer face to face communication (Sivricova & Moiseeva, 2018). This can create conflict between generations, because they are not adapted to the communication methods of other generations (Sivricova & Moiseeva, 2018). Technical developments have shaped how modern youth interact with the world (Sivricova & Moiseeva, 2018). This alienates senior citizens and creates tension due to lack of sympathy and misunderstandings (Sivricova & Moiseeva, 2018). Generational values, especially in Russia, reflect the political atmosphere of a person’s moral upbringing. For example, mature individuals may value collectivism while the youth value personal success and material prosperity (Sivricova & Moiseeva, 2018). When analyzing the values of generations, one must consider the dynamic nature of society (Sivricova & Moiseeva, 2018).

Information and communication technologies shape the way that younger learners absorb and disseminate knowledge (Candoni & Danowski, 2015). The adoption and integration of technology affects how generations think and communicate (Cantoni & Danowski, 2015). Millennials are also known as digital natives, since they grew up using computers and the Internet (Cantoni & Danowski, 2015). Within higher education, digital natives focus on high scores as opposed to finding fault with the teacher (Cantoni & Danowski, 2015). They also prefer discussions to lectures and enjoy trial-and-error learning as opposed to following a set list of instructions (Cantoni & Danowski, 2015). When looking at the digital divide, people who are adapted to a digital world are able to establish a presence within the digital world, while those who fail to adapt to a digital world essentially fall off the grid (Cantoni & Danowski, 2015). Technology can change the identity of humans and some anthropologists fear that hyper technologization turns people in to consumers of digital information as opposed to focusing on interpersonal communication and human connection (Cantoni & Danowski, 2015). Digital illiteracy also poses a threat (Cantoni & Danowski, 2015). Failure to apply critical thinking in a digital environment, especially in the context of social networking, is a manifestation of digital illiteracy (Cantoni & Danowski, 2015). Adoption of technology in an academic setting should not be solely for the sake of technology (Cantoni & Danowski, 2015). Rather, it should be used in an academic environment when it increases productivity and convenience (Cantoni & Danowski, 2015).

Richard Bridge writes in *Training Journal,* that the gap in tech-savviness between baby boomers and millennials can create tension between generations (2017). While warning that it can be easy to generalize generations, Bridge notes that generational differences and stereotypes may become a barrier to trust and respect (2017). When working with multiple generations, Bridge recommends involving all generations in decision making, creating cross-generational mentorship and talent partnering programs, investing in face-to-face interactions, and building trust (2017). Bridge warns against using digital solutions for the sake of using digital (2017). Instead, invest in the most appropriate platform for the objective (Bridge, 2017).

Jaynee Handelsman, 2016 president of the American Speech and Hearing Association, provides a few insights into cross-generational communication. Handelsman argues that baby boomers may be less tech savvy than millennials (2016). Baby boomers grew up with landlines, black and white television, and snail mail for their communications and entertainment needs (Handelsman, 2016). Millennials and Generation Z, on the other hand, rely on the Internet for communication and entertainment (Handelsman, 2016). She recommends integrating technology where it can maximize quality care, while being understanding of the frustrations of older generations (Handelsman, 2016).

**Use of Computers and the Internet by the Elderly**

In a 2015 article from Education Gerontology, Robert Zheng of the University of Utah’s Department of Educational Psychology and Jeffery Spears, Marilyn Luptak, and Frances Wilby of the University of Utah’s College of Social Work explore older adults’ perception of Internet use. Their factor analysis revealed that older adults use the Internet for social connection, financial information, and health information (Zheng, Spears, Luptak, & Wilby, 2015). In addition, positive self-efficacy has a high correlation to Internet use in the elderly (Zheng, et al., 2015). In 2014, the World Health Organization estimated that by 2025, over one billion people worldwide will be over the age of 60 (Zheng, et al., 2015). The Internet supports older adults by providing hobbies, banking services, entertainment, and helps foster intergenerational relationships (Zheng, et al., 2015). Internet related activities influence the social and emotional well-being the elderly (Zheng, et al., 2015).

Self-efficacy is defined as a person’s perception of their abilities to complete a course of action to manage a situation (Zheng, et al., 2015). People with a higher level of self-efficacy are more likely to use the Internet in order to satisfy personal and social needs than those who have lower self-efficacy. Essentially, if a person feels comfortable in their abilities to successfully operate a computer and navigate the Internet, the more likely they are to use the Internet to meet their needs (Zheng, et al., 2015). Online social connection provides a way for older adults to develop and maintain their social support networks (Zheng, et al., 2015). Strong social connections in older individuals help reduce stress, depression, and support immune and cardiovascular function by mitigating stress-related illness (Zheng, et al., 2015). When looking at the relationship between Internet use and psychological well-being, older adults who actively engage in online activities feel less stressed than those who do not (Zheng, et al., 2015). The Internet also empowers senior citizens to make informed decisions about their health and finances (Zheng, et al., 2015). However, web design accessibility issues create a roadblock for the elderly (Zheng, et al., 2015). Accessibility issues along with concerns about credibility prevent the Internet from becoming the primary medium for information on health and financial information for older adults (Zheng, et al., 2015). Regarding health information, the elderly use the Internet to explore what to expect in terms of aging (Zheng, et al., 2015). For financial information, the elderly use the Internet to research how to plan and maintain retirement (Zheng, et al., 2015).

In a survey of 395 older adults, Zheng, Spears, Lupta, and Wilby found that gender was not a significant predictor of older adults’ perceptions of Internet use (2015). Financial status, time on the Internet, and the perception of the computer’s role was found to significantly predict self-efficacy (Zheng, et al., 2015). Financial status is tied to a person’s confidence in their ability to operate and navigate computers and the Internet because they have the financial means to invest in new technologies (Zheng, et al., 2015). The ability to seek out information and form social connections using the Internet contributes to life satisfaction is older adults (Zheng, et al., 2015). The survey was limited to the United States and consisted of 80% white respondents (Zheng, et al., 2015). A possible area of further research is seeing if perceptions of the Internet differ between different countries and/or ethnic groups. Cultural differences may alter how older individuals perceive the Internet and its influence and means of social connection (Zheng, et al., 2015).

A pilot study from Yousara Javed, Mohamed Shehab, and Boyd Davis analyzes senior citizens’ media preferences vs. comprehension (2019). For the study, participants either listened or read a script on e-mail-based phishing (Javed, Shebab, & Davis, 2019). In the study of 34 senior citizens, they found that while seniors preferred text information to audio, the comprehension scores between the two types of media were not statistically significant (Javed, et al., 2019). The survey of participant demographics found that the majority of participants used Facebook for social media, were concerned about security and privacy when using the Internet, have been using the Internet for more than 5 years, and have been the victim of an Internet scam or attack one or more times (Javed, et al., 2019).

James Morgan explores how senior citizens perceive cybersecurity and data privacy in his 2015 doctoral dissertation at Capella University. His study of seventeen participants analyzes the understanding and thought processes of senior citizens around cybersecurity topics. He found that the majority of study participants thought of themselves as being at the novice or moderate level of computer experience (Morgan, 2015). All of those who self-reported an advanced level of experience had previously worked in the IT industry (Morgan, 2015). Participants acknowledge that there was at least some of their personal information on the web, but the majority had no idea how it ended up there (Morgan, 2015). Some participants postulated that maybe online surveys and social media were to blame for their personal information being on the Internet (Morgan, 2015). Participants who had googled themselves were surprised by the amount of information they were able to uncover (Morgan, 2015). Participants had varied opinions of cyber risk management (Morgan, 2015). Some participants thought that avoiding behaviors such as responding to phishing e-mails would keep them safe while others took a more fatalistic approach, feeling like they were at risk no matter what they did (Morgan, 2015). Other participants expressed anxiety over not knowing how their data could be exploited or what data was already available to threat actors (Morgan, 2015). Morgan’s study found that senior citizens had a general understanding of malware but lacked understanding of viruses and how they work (Morgan, 2015). There was also a perception that hackers were “lonely teenage boys” or identity thieves looking to steal social security and credit card numbers (Morgan, 2015). As for anti-virus software, only ten out of seventeen participants could name an anti-virus product or company (Morgan, 2015). On a positive note, participants seemed to have a good understanding that the anti-virus software needed to do regular scans and updates (Morgan, 2015). Three out of the seventeen participants had no idea how to recognize cybersecurity issues, but others listed warning signs such as poor performance, missing files, the blue screen of death, or warnings from their anti-virus software (Morgan, 2015). Ten participants had participated in online surveys while 5 participants took part in social media (Morgan, 2015). Two participants believed that their online survey data had been sold to marketing firms (Morgan, 2015). One participant stated that they thought Facebook probably made some money from people’s private information (Morgan, 2015). Participants primarily received cyber threat information from the news media such as television and newspapers and from friends and family (Morgan, 2015). Cyber literacy in the elderly is generally low, but they will take precautions if given clear, concise directions (Morgan, 2015).

**Cybercrime Victimization of the Elderly**

University of Washington’s Albert Munanga explains the role of nurses and healthcare professionals in the prevention and mitigation of cybercrime. He notes that cybercriminals in the United States exploit almost $40 billion from the elderly every year and cybercrime victimization of the elderly is growing every year (Munanga, 2019). A common tactic is government official impersonation, specifically IRS impersonation (Munanga, 2019). In Washington state, cybercrime is a reportable form of elder abuse and requires health care workers to report it to the Department of Social and Health Services (Munanga, 2019). The Department of Social and Health Services lacks the capacity to investigate cybercrimes, so such investigations often meet dead-ends (Munanga, 2019). Health care providers should encourage victims to contact the FBI’s Internet Crime Complaint Center (IC3), since IC3 is the central force in measuring and combatting cybercrime in the United States (Munanga, 2019).

Social media allows older adults to connect with friends and family, but also serve as a platform for cyberbullies and scammers (Munanga, 2019). Munanga saw the effects of cybercrime on the elderly in his role as a gerontological health care provider (2019). One of his colleagues had a patient in a nursing home who fell victim to the common family emergency scam, where a victim receives an e-mail from a scammer pretending to be a family member experiencing an emergency in a foreign country (Munanga, 2019). The scammer then asks for money (Munanga, 2019). The scammer in this case was successful in exploiting the elderly patient (Munanga, 2019). The elderly are prime targets for cybercrime and fraud because of their generally favorable credit history and the trusting and helpful nature of their generation (Munanga, 2019). They are also less likely to report cybercrimes (Munanga, 2019). Munanga’s article refers to the FBI’s recommendations for senior including avoiding shopping online, using telephones with caller ID, only visiting trustworthy websites, and checking for malware frequently (Munanga, 2019). Cognitive decline decreases a person’s ability to responsibly manage their finance (Munanga, 2019). If the police are notified of a cyberfraud against an elderly person, Munanga recommends they contact Adult Protective Services (2019). The elderly need cybercrime education, widespread reporting, and psychological support for incidents (Munanga, 2019). Nurses and other healthcare professionals who work with the elderly to report cybercrime against the elderly to the relevant stakeholders (Munanga, 2019).

Cassandra Cross of Queensland University of Technology looks at senior citizens’ attitudes towards identity crime. Identity crime is commonly used as a tool to carry out other criminal acts (Cross, 2016). To illustrate this point, a phishing e-mail can come from a legitimate source asking for personal information or banking details (Cross, 2016). These details can then be used to open new lines of credit or empty a victim’s bank account (Cross, 2016). The Internet is used for legitimate communication and business reasons (Cross, 2016). Sharing personal details are a common aspect of this environment (Cross, 2016). For this reason, cybercrime must be analyzed in the context of a legitimate information environment (Cross, 2016).

In Australia, identification information is defined as information relating to a person that is capable of being used to identify a person (Cross, 2016). This applies to living, dead, real, and fictitious people (Cross, 2016). This is a broad definition, which makes identity crime rationale difficult for senior citizens to navigate (Cross, 2016). Cross writes that the majority of identity crime prevention looks to absolve corporations and the government from liability for breaches and compromises (2016). This shifts the blame for breaches from the collective to the individual (Cross, 2016). A political trend in Australia is the concept of prudential citizen (Cross, 2016). This means that citizens should be aware of how and why their actions impact their future and take appropriate risk management steps (Cross, 2016). Of course, this requires that citizens be aware of the potential impact of their actions (Cross, 2016). Some senior citizens do not connect their choices to send identification information to phishing e-mails with the risk of identity crime (Cross, 2016).

In a study of 85 seniors across Queensland, Australia, Cross analyzed the opinions of seniors towards revealing identity information to phishing e-mails (2016). One respondent, Max, replied to an e-mail for a fraudulent job opportunity with a color copy of his passport (Cross, 2016). A while later, Max was contacted by the Australian Department of Immigration when a person attempted to enter the country using a falsified passport with his information (Cross, 2016). Max did not think that sending a color copy of his passport could lead to identity crime because he was unaware of the skills of the threat actor(s) (Cross, 2016). Cross’ research also found that senior citizens perceived a difference between being asked from money vs being asked for identification information (2016). Some senior thought it harmless to send identity information since a significant amount of the information could already be obtained through open sources on the Internet (Cross, 2016). Another respondent, Roberta, states that she would not give out her banking or passport details to strangers on the Internet, but she thought that name, address, e-mail, address, and date of birth were okay to divulge (Cross, 2016). Respondent Patrick, who fell victim to inheritance fraud and sent a copy of his passport, bank account details, and personal information to a scammer (Cross, 2016). The alarm bells only started to go off in his head when the scammer asked him to send money (Cross, 2016).

Study participant Harold responded to a fraudulent lottery notification with his personal information including bank account details, driver’s license number, and address (Cross, 2016). Harold did not understand the value of his information and how it could be used by a threat actor (Cross, 2016). Harold’s reasoning was that if a scammer tried to access his bank account, they would not find anything and therefore providing the details was a low-risk activity for a potentially high reward (Cross, 2016). He was unaware that the information he provided along with the banking details could be used to open new lines of credit or accounts (Cross, 2016). Respondent Vivian took a more conservative approach to handing out her personal information as opposed to Max and Patrick, but she still responded to a phishing e-mail with personal information (Cross, 2016). She responded to the e-mail with her name, address, and date of birth, her reasoning being that the information is widely available and therefore harmless to reveal (Cross, 2016). Another respondent, Mavis, responded to a fraudulent email despite knowing full well it was fraudulent (Cross, 2016). Mavis responded with the requested identification because she was curious how long it would take for the fraudsters to ask her for money (Cross, 2016). She divulged her name, address, phone number, and occupation (Cross, 2016). Mavis did not understand the risk of divulging her personal information, therefore it did not factor into her risk analysis (Cross, 2016).

Genealogy websites provide a plethora of personal information (Cross, 2016). Cross notes that some older adults are quite willing to give out their personal details for the sake of establishing family links (2016). One respondent, Loretta, states she felt comfortable giving out personal information about herself and her family, including information such as her mother’s maiden name, on genealogy websites because it was password protected (Cross, 2016). Loretta was surprised that people would give out their personal information on a platform other than an ancestry website, because strangers could access it (Cross, 2016). Context played a large role in why respondent Lillian gave out her and her family’s information (Cross, 2016). While ancestry websites are a different context from phishing e-mails, the outcome of identity fraud is the same (Cross, 2016). Lillian later recognized the risk that her years of genealogy research and input placed on her and her family but feels it’s too late to regain control of her personal information (Cross, 2016). Senior citizens should exercise a more conservative level of trust when interacting with genealogical websites (Cross, 2016).

For a government or company to expect citizens to accept individual responsibility for post-breach identity protection, individuals must have adequate risk management strategies and actions (Cross, 2016). In Cross’ interviews of senior citizens, it became apparent that seniors lack a comprehensive understanding of the capabilities of threat actors and the vulnerabilities associated with certain web actions such as interaction with genealogical websites (2016).

In a 2017 article in *Frontiers in Psychology,* Rebecca Judges, Sara Gallant, Lixia Yang, and Kang Lee explore the role of cognition, personality, and trust and how it plays into the fraud victimization of older adults. They note that, as of 2014, the world bank estimates that 16% of the population from high income countries consisted of individuals age 65 or over (Judges, Gallant, Yang, & Lee, 2017). The researchers point out that studies on the demographics of individuals who fall victim to fraud are mixed (Judges, et al., 2017). The Federal Trade Commission found that Native Americans, African Americans, and Hispanic Americans were more likely to fall victim to fraud than Non-Hispanic Caucasian Americans (Anderson, 2013). A different study from 1995, published in *Crime & Delinquency* found that there was no significant effect of race or ethnicity when it came to fraud victimization (Titus, Heinzelmann, & Boyle, 1995). It should be noted that the Anderson study from the FTC is much more recent.

Through extensive study, cognitive decline has been linked to poor financial literacy and financial decision-making skills (Judges, et al., 2017). Looking at the brain, one of the first parts to undergo age-related decline is the ventromedial prefrontal cortex, also known as vmPFC (Koestner, Hedgcock, Halfmann, & Denburg, 2016). The vmPFC plays a role in social processing, regulation of fear and anxiety, and learning safe behaviors (Fossati, 2012). The vmPFC causes younger adults to dwell on negative information while in older adults it creates a positivity effect, where seniors tend to dwell on the positive aspects of presented information (Leclerc & Kensinger, 2008). Persons with damaged vmPFCs tend to be more suggestable and gullable and are more likely to trust misleading advertisements as compared to those without vmPFC damage (Rogalsky, Vidal, Li, & Damasio, 2012).

Judges, Gallant, Yang, and Lee analyzed the factors of cognitive decline, agreeableness, conscientiousness, honesty and humility, emotionality, extraversion, trust, and openness to experience and how they factor into fraud victimization of the elderly (2017). For the cognitive measures, they looked at overall cognitive ability, language, verbal memory, and attention (Judges, et al, 2017). They surveyed 151 primarily Caucasian, female respondents from Southern Ontario, Canada. The respondents were between the ages of 60 and 90, looked after their own finances, and had not been diagnosed with neurological disorders or cognitive impairment (Judges, et al., 2017).

The characteristic most significantly associated with fraud victimization was overall cognitive ability (Judges, et al., 2017). Cognitive ability was measured using the Multiple Ability Self-report Questionnaire (MASQ) (Judges, et al., 2017). The measurement of overall cognitive ability was able to uniquely predict fraud victimization, while the other factors that were present in fraud victimization were unable to uniquely predict victimization (Judges, et al., 2017). The data shows a person is around 11 times more likely to be a victim of fraud for every 10-point decrease in overall cognitive ability (Judges, et al., 2017). Victims were also significantly less conscientious than non-victims (Judges, et al., 2017). This means that they took less time to consider their financial actions, were less detail oriented, and did not carefully consider the possible consequences of their actions (Judges, et al., 2017). Victims were found to be significantly less honest and humble than non-victims (Judges, et al., 2017). The researchers postulate that this may be because of a heightened sensitivity to fairness (Judges, et al., 2017). Interestingly, researches did not find a significant relationship between trust and fraud victimization (Judges, et al., 2017). They note that fraud victims tend to act on impulse and may be easily swayed by false promises and quick-talking fraudsters (Judges, et al., 2017). They state that there is objective evidence that adults experiencing cognitive decline who report a decrease in their overall self-confidence of their abilities often do not report decreased confidence in their ability to manage their finances (Judges, et al., 2017). They mention the possibility of cognitive training techniques as a possible method to prevent fraud victimization in the elderly (Judges, et al., 2017). For future research, they recommend following a behavioral based line of research for investigating the root causes of fraud victimization (Judges, et al., 2017).

Cassandra Cross, a School of Justice senior lecturer at Queensland’s School of Technology, explores how strong negative stereotypes of fraud victims and victim blaming create barriers to support for elderly fraud victims (2016). Older individuals are less likely to become a victim of crime in all categories except for fraud (Cross, 2016). Cross states fraud disproportionately impacts the elderly (2016). Fraud takes many forms and approaches: popular types of fraud include advance fee fraud and romance scams (Cross, 2016). Advance fee fraud occurs when a fraudster asks for a small amount of money in return for a larger, later payoff (Cross, 2016). The payoff, of course, never occurs. Types of advance fee fraud include the promise of lottery winning, fake inheritance notifications, the promise of a business investment, or a potential employment opportunity (Cross, 2016). Criminological literature asserts that the elderly are more likely to be targeted for fraud because of their physical, financial, and social vulnerabilities (Cross, 2016). Senior citizens commonly have a variety of assets along with good credit history and long lines of credit (Cross, 2016). This makes them particularly lucrative targets for scammers (Cross, 2016).

Cross conducted a study of volunteers who provide support to elderly fraud victims (2016). Of the observations noted, loneliness stands out as a major factor in crime victimization of the elderly (Cross, 2016). Internet and e-mail communication provide a way for the elderly to connect with others and stave off loneliness, but it also provides a proverbial hunting ground for fraudsters (Cross, 2016). Several victims fell victim to romance scams after the death of a spouse (Cross, 2016). Loneliness takes a toll on the overall mental health of the elderly (Cross, 2016). This well of loneliness is compounded by the physical inability to leave the house, lack of vehicular access, and lack of nearby family members (Cross, 2016). In their desperation, elderly individuals fall victim to online fraudsters (Cross, 2016).

Victimological literature paints a picture of fraud victims as greedy and gullible individuals who are undeserving of sympathy (Cross, 2016). Victim precipitation theory blames the victim or has them share blame for the outcome of an incident (Cross, 2016). Ideal victims in society are ones who have not contributed to their own victimization (Cross, 2016). Fraud requires that the victim actively participate in their victimization (Cross, 2016). Therefore, fraud victims are commonly portrayed in a negative light and can lead to the victim being blamed for their own defrauding (Cross, 2016). This can serve as a barrier to elderly fraud victims receiving the help they need from agencies and society (Cross, 2016). While greed and gullibility do play a role in fraud victimization, Cross states that loneliness and desperation for human connection play a much larger part (2016). Cross points out that fraudsters are commonly highly trained people with a lot of experience in social engineering (2016).

Stigma commonly serves as a barrier to fraud disclosure (Cross, 2016). This leads to an isolation feedback loop. Victims do not want to access recovery support and are afraid of what might happen if they tell their families (Cross, 2016). Cross’ interviews with elderly fraud support volunteers reveal that elderly fraud victims are afraid to tell their children because they’re afraid of being put in a nursing home, having their banking privileges taken away, or having outside communication cut off (2016). Cutting off outside communication creates a negative feedback look which leads to poorer mental health and a greater amount of loneliness and desperation (Cross, 2016). Concealing fraud victimization from family can also lead to isolation and depression, which can increase repeat victimization (Cross, 2016).

In 2018, AARP conducted a study on perceptions of digital identity. The guiding questions looked at online banking, unique password usage, and understanding of credit freezes because that is what security experts recommend as the three main ways to protect one's digital identity (Pak, Shadel, & Williams, 2018). The study found that of older adults age 65 and over, 33% have access to all of their online bank accounts (Pak, et al., 2018). This is compared to 50% for adult ages 18-49. 68% of those age 65 and over and 50% of those 18-49 who did not have online banking set up responded that they avoided setting it up because they thought that it would contribute to their personal information being stolen (Pak, et al., 2018). The authors state that while setting up online accounts for banking may feel like an increase in risk, it actually decreases the risk of identity theft and fraud victimization (Pak, et al., 2018). Younger adults are more likely to reuse passwords than older adults (Pak, et al.., 2018). 55% of respondents ages 18-49 admitted to reusing passwords while only 30% of those aged 65 + did (Pak, et al., 2018). Younger adults are also more likely to use Facebook to sign into other accounts (Pak, et al., 2018). 43% of those ages 18-49 had used Facebook to sign into other accounts while on 29% of those ages 65+ had done so (Pak, et al., 2018). Very few adults overall (14%) knew how to conduct a credit freeze (Pak, et al., 2018).

A 2018 report from the Federal Trade Commission (FTC) highlights fraud types and enforcement activities. Looking at median individual monetary loss per fraud incident, persons ages 50-59 lost an average of $500 per incident while those ages 80 and over lost an average of $1,100 per incident (FTC, 2018). In terms of overall fraud type, tech support scams received the greatest number of reports including a financial loss in individuals over the age of 60 (FTC, 2018). This is followed by fake businesses, prizes/sweepstakes/lottery scams, romance scams, government imposters, fake friends or family scams, and foreign money offers not prize related (FTC, 2018). For individuals over the age of 60, the most common form of payment for scams was credit card, accounting for 32% of incidents (FTC, 2018). The most lucrative form of payment was wire transfer, with a total of $104 million dollars paid to scammers over the course of 2017 (FTC, 2018). In 2017, the FTC took enforcement actions against phony grants, fake sweepstakes, tech support scams, fraudulent business education scams, fake apartment listings that preyed on section 8 housing voucher recipients, anti-aging product claims, and more (FTC, 2018).

The Federal Bureau of Investigation’s (FBI) Internet Crime Complaint Center (IC3) produced the *2019 Internet Crime Report.* In 2019, IC3 reports that there were 60,013 total victims over the age of 60 (IC3, 2019). The total monetary loss for those over the age of 60 was $835,164,766 (IC3, 2019). California saw both the largest number of overall victims and the largest monetary loss (IC3, 2019). The largest crime types by victim count were phishing/vishing/smishing/pharming, non-payment/non-delivery, extorsion, personal data breach, spoofing, business e-mail compromise, romance fraud, identity theft, harassment, and overpayment (IC3, 2019). When organized by victim loss, the top ten crime types are business e-mail compromise, romance fraud, spoofing, investment, real-estate, non-payment/non-delivery, identity theft, government impersonation, personal data breach, and credit card fraud (IC3, 2019). As part of the Elder Abuse Prevention and Prosecution Act of 2017, the FBI and the Department of Justice created the Elder Justice Initiative, which they have used to conduct community outreach and public service announcements (IC3, 2019).

**Senior Citizen Cybersecurity Education Frameworks and Programs**

CyberGenerations is a cybersecurity curriculum for senior citizens, developed as a partnership between AT&T and the Air Force Association’s CyberPatriot program (AFA, 2020). The curriculum introduces to seniors the topics of cybersecurity, password management, common Internet threats, Internet scams and fraud, and social media safety (AFA, 2020). The CyberGenerations curriculum is usually presented as a workshop, but there is also a self-paced guide available that contains all the information from the workshop (AFA, 2020). The workshop resources contain editable interest flyers, a facilitator guide, a workshop PowerPoint presentation, supplemental activities including an interactive Jeopardy-style PowerPoint presentation, and a copy of the self-paced guide (AFA, 2020). The self-paced guide starts off with a pre-program survey and a Cyber-Aware Quiz (AFA, 2020). At the end of the course there is another survey for program feedback (AFA, 2020).

The *Introduction to Cybersecruity* section starts by defining cybersecurity and establishing cybercrime as a threat (AFA, 2020). This is followed by a myth and truth section, which covers common misconceptions that senior citizens may have about information on the Internet (AFA, 2020). The subsection covers personally identifiable information (PII) including a list of information considered PII, how PII can be exploited on the darknet, and physical threats to PII (AFA, 2020). Following that is a subsection on securing mobile devices (AFA, 2020). The curriculum defines mobile devices and shares a list of tips on how to keep data safe on mobile devices (AFA, 2020). The list recommends logging out of social media apps once a person is done using them and disabling Wi-Fi and Bluetooth when not in use (AFA, 2020). The mobile devices subsection also covers how to activate and maintain location tracking for both Android and Apple in case of a lost device (AFA, 2020). In the subsection on web browser safety, the guide recommends using Microsoft Edge, Google Chrome, Mozilla Firefox, Opera, or Safari for safe web browsing (AFA, 2020). It mentions that Opera has a built-in VPN (AFA, 2020). As for web browser safety tips, the guide recommends using a pop-up blocker, checking for an https connection as opposed to an http connection, turning on automatic updates, and avoiding the use of autofill and built-in password management features (AFA, 2020).

The next section of the self-paced guide is on password management (AFA, 2020). It opens with a theoretical scenario where poor password management leads to a person losing money (AFA, 2020). This is followed by a subsection on creating strong passwords (AFA, 2020). Bad and/or weak password ideas such as using birthdays, names, or dictionary words are listed, follow by two or three examples of each poor password idea (AFA, 2020). The guide states that password length should be 10 characters or more and use a combination of upper and lowercase letters, numbers, and symbols (AFA, 2020). For strong passwords, the guide recommends creating a base password or passphrase followed by an acronym for the website it applies to (AFA, 2020). To keep track of passwords, the guide recommends using a passwords manager such as LastPass, dashlane, or 1Password (AFA, 2020). It also recommends changing one’s passwords every 6-12 months (AFA, 2020). The guide is strongly against autofill and automatically saved passwords (AFA, 2020). The case for autofill passwords will be discussed in the analysis section. The guide recommends opting-in to two-factor authentication when and where it is available (AFA, 2020). There is also a small section of what to do if an account is compromised, including changing one’s password, reporting the breach, and checking other accounts (AFA, 2020).

The following of section of CyberGenerations covers common Internet threats. Like the last section, it opens with a theoretical scenario (AFA, 2020). In this case, the scenario is about a man who falls victim to a phishing e-mail and his computer becomes infected with malware (AFA, 2020). Then the guide defines malware, symptoms of malware, and types of malware (AFA, 2020). The types of malware listed and defined are viruses, worms, trojan horses, adware, spyware, ransomware, rogue security software, browser hijackers, and zombies (AFA, 2020). It then lists how malware spreads, listing the Internet, media downloads, free software, removable media, and e-mail attachments (AFA, 2020). The guide defines social engineering and the methods social engineers use to defraud people (AFA, 2020). This includes phishing, spear phishing, vishing, and smishing (AFA, 2020). The subsection on phishing goes in depth on how to identify and avoid phishing and includes a picture of a phishing e-mail with all the red flags circled and explained (AFA, 2020). It also points out that 91% of cyberattacks begin with a phishing email and that 30 % of phishing e-mails are opened with 12% of the targets clicking infected links contained in the phishing e-mails (AFA, 2020). With vishing, the guide states that people should be suspicious of unknown callers and that they should not trust caller ID (AFA, 2020). This is counter to the recommendations of Munanga’s article, which lists caller ID as a fraud victimization reduction mechanism (2019). An important concept CyberGenerations conveys is that individuals should not attempt to outwit a social engineer (AFA, 2020). Instead, the best practice is to disengage with the potential scammer (AFA, 2020). Smishing is a form of phishing that occurs through text messages (AFA, 2020). The guide recommends ignoring smishing texts (AFA, 2020). If a person wants to act on a smishing text, the guide lists official reporting mechanisms (AFA, 2020). For preventing and mitigating common Internet threats, the guide recommends antivirus software such as AVG Free, Bitdefender Free, Avast, Symantec, McAfee, and AVG (AFA, 2020). It also covers how to check for anti-virus software on Mac OSX and Windows operating systems (AFA, 2020). CyberGenerations recommends periodically running security updates and using a VPN when in public (AFA, 2020). It does not, however, go over the steps to set up a VPN outside of the Opera browser’s built-in VPN (AFA, 2020). It covers public, unsecured Internet, the risks, and risk mitigations (AFA, 2020).

Section four of CyberGenerations covers scams and fraud (AFA, 2020). Similar to previous sections, it starts off with a couple of sample scenarios, which then leads into a subsection on scam awareness (AFA, 2020). The subsection discusses agencies and companies which may be impersonated by scammers, such as the IRS, the FBI, and banking/retirement investment companies (AFA, 2020). False claims through insurance companies are also a way scammers make money (AFA, 2020). It also warns against fake donation organizations, dating websites, and online/phone surveys that promise a prize if one follows a link in an e-mail or gives out their personal information over the phone (AFA, 2020). The guide provides longer summaries of common scams such as the IRS/Tax scam, the send-money or wire-transfer scam, the foreign lottery scam, the survey scam, the money-making scam, the computer security or tech support scam, the dating scam, and the charity or door-to-door scam (AFA, 2020). The tax scam is carried out when scammers pose as the IRS and threaten to send the victim’s (false) debt to collections if they do not immediately send money (AFA, 2020). Sometimes, the scammers will ask for gift cards or prepaid debit cards (AFA, 2020). Often the first contact the scammers make is through e-mail whereas the real IRS will usually contact a person via postal service first (AFA, 2020). The send-money or wire-transfer scam is where a person posing as a friend of family calls or e-mails stating that they are in trouble in a foreign country and are stranded (AFA, 2020). The guide recommends using official authorities such as the consulate in order to help the stranded friend or family member and contacting the friends and family up the supposedly stranded traveler for official contact information (AFA, 2020). The guide states that a person should not respond to the e-mail that was used for the official correspondence, rather the one that the person has on file (AFA, 2020). The foreign lottery scam occurs when a scammer calls or e-mails a victim stating that they have won a foreign lottery or other large prize (AFA, 2020). In order to claim the winnings, the scammer states that the victim needs to prepay taxes and fees (AFA, 2020). The victim pays the scammer and then the scammer is nowhere to be found (AFA, 2020). Survey scams occur when a person receives phishing e-mail or sees a social media post with a link to complete a survey (AFA, 2020). The survey may promise a grand prize for completion, when in reality the survey is used to install malware or steal personal information (AFA, 2020). The money-making scam is where a person may be asked to invest an amount of money for a trial or start-up kit with the promise of a big payoff for minimum effort (AFA, 2020). The money-making scam is commonly marketed as a work from home “job” (AFA, 2020). The tech support scam occurs when a person either clicks on a pop-up, responds to an e-mail, responds to a targeted advertisement, or answers a call from a fake tech support operation (AFA, 2020). Oftentimes, the links in pop-ups, e-mails, and targeted ads automatically install malware on the victim’s computer, and then displays a number that leads to the fake tech support operation (AFA, 2020). The guide points out that tech support will only contact a person if they have been contacted first (AFA, 2020). Dating scams prey on the elderly because they are seen as gullible (AFA, 2020). Sometimes scammers will find their victims on legitimate online dating websites, create a connection with the victim, and then ask for money for made-up reasons (AFA, 2020). Charity scam fraudsters take pictures from unsuspecting families on the Internet and pose them as their own, creating a tragic backstory in order to solicit donations (AFA, 2020). The guide then goes on to discuss identity theft (AFA, 2020). It recommends following the steps of deter, detect, review, and defend in order to prevent identity theft (AFA, 2020). For online shopping, the guide recommends using reputable retailers and websites, not shopping on unprotected Wi-Fi, and being wary of fake reviews (AFA, 2020).

The last section of the self-paced guide covers social media awareness and safety (AFA, 2020). The example scenario at the beginning of the section covers fake social media accounts and then points out that senior citizens are more likely to use Facebook than any other social media platform (AFA, 2020). The guide describes Facebook, Twitter, Instagram, YouTube, Pinterest, and LinkedIn, describing each platform’s purpose and general capabilities (AFA, 2020). When interacting with social media, CyberGenerations recommends users be picky with who they accept as friends, warns against over-sharing, and locking down security settings (AFA, 2020). There is a short section of online dating safety and then the guide discusses social media scams (AFA, 2020). Topics covered include dummy profiles, clickbait, sick baby hoaxes, and social media charity scams (AFA, 2020). Dummy profiles are fake social media profiles that threat actor use to spread malware, and steal personal and financial information (AFA, 2020). Clickbait contains interesting headlines or photos that are designed to generate a click (AFA, 2020). This leads to a malicious website that downloads malware onto the victim’s device (AFA, 2020). The sick-baby hoax uses images of sick infants in order to solicit donations for treatment (AFA, 2020). The images do not belong to the scammer and the money does not go to helping a sick child (AFA, 2020). Charity scams will sometimes ask victims to purchase cell phones in bulk and send them to (non-existent) less fortunate people who need them (AFA, 2020). The final subsection is on social media etiquette (AFA, 2020). The etiquette rules include avoid oversharing, such as announcing vacation details or financial information, commenting and posting with care, such as avoiding arguments, all caps, and flooding others’ feeds, researching and obtaining consent prior to positing or sharing photos and videos, and analyzing friend-requests prior to accepting them (AFA, 2020). Following the course content, there are links and contact information for resources and agencies and state-specific aging agencies (AFA, 2020). The very last part of the course is the post-course survey which asks for feedback and recommendations on the course (AFA, 2020).

David Kane of Utica college developed a security awareness training framework for the elderly as part of his master’s capstone in 2015. Kane’s framework is designed assuming a low level of cyber schema in the target audience (2015). The framework focuses on establishing a baseline including vocabulary and information security concepts and reinforcing the concepts through multiple sessions (Kane, 2015). Kane recommends that the training include step-by-step instructions for configuring security settings and a hands-on portion of the class where students can follow along with the teaching using a computer (2015). His training framework adopts a community support viewpoint, providing resources for both the elderly and their families (Kane, 2015). Kane states that resources must be effective, inexpensive, trusted, and knowledgeable and recommends providing bookmarks with reliable information (2015). The framework establishes need by listing the factors that make senior citizens targets and illustrating the potential impact of poor information security practices (Kane, 2015). The framework then looks at the means, methods, and behaviors used by threat actors in order to defraud and exploit senior citizens (Kane, 2015). Kane advises showing specific examples with each method threat actors use in order to increase comprehension (2015). The framework then looks at methods of detection and prevention and patterns of behavior that serve as prevention and mitigation methods (Kane, 2015). Finally, Kane suggests that workshop developers partner with tech companies or universities in order to obtain sponsorship (Kane, 2015).

Jose Magdiel Rivera Gonzalez of Utica College discusses themes of information security awareness in older adults in his 2019 capstone project. The first theme is the negative effects of aging include cognitive decline, a lack of skills, and the underreporting of scam susceptibility (Gonzalez, 2019). Older adults notoriously underreport cybercrime and fraud, possibly because of feelings of shame and weakness (Gonzalez, 2019). Older adults lack confidence and ability in basic computer skills such as running updates, using complex passwords, and setting up firewalls (Gonzalez, 2019). The capabilities gap creates an opportunity for threat actors to strike (Gonzalez, 2019). There are also several misconceptions about older adults which hinder the ability to assist senior citizens with information security (Gonzalez, 2019). There is a misconception that older adults are unable to learn the computer and information security skills needed to stay safe online (Gonzalez, 2019). Older adults are in fact capable of learning such skills, and when taught computer skills and safety habits, they apply them (Gonzalez, 2019). The second theme that Gonzalez uncovered is the need is the need for more cybersecurity awareness and training (2019). Older adults need trainings with formal structure that tailors to their needs (Gonzalez, 2019). Data on common scams that target the elderly are widely available from the FBI, the FTC, and the FCC (Gonzalez, 2019). This data needs to be shaped into tailored trainings to protect the elderly (Gonzalez, 2019). The thirds theme analyzes the composition of awareness and training (Gonzalez, 2019). Gonzalez states that awareness programs should use specific and detailed information in order to effectively convey topics (2019). Programs should be built using a strong framework that can be adapted to specific needs and maintain relevance (Gonzalez, 2019). Gonzalez recommends integrating the Behavior Change Wheel framework into the design process (2019). Trainings should also consider assistive technologies and the physical and metal degenerative effects of aging (Gonzalez, 2019). Gonzalez advocates for further research into what older adults know and do not know about information security, so that effective trainings can be developed (2019).

Kara Pernice, Janelle Estes, and Jakob Nielson of the Nielsen Norman Group developed general principles for designing websites and computer-based information for the elderly using data on how the elderly prefer text, search function, content, navigation, graphics, forms, and general principles of design (Pernice, et al., 2013). For general principles, the researchers recommend avoiding jargon or complex language, provide printed, easy to understand reference materials, and provide closed-captioning and a transcript for any videos used (2013). Text should be at a minimum 12-point font, in sans serif, using medium or bold typeface (Pernice, et al., 2013). Italics and all caps can be difficult to read and should be avoided (Pernice, et al., 2013). Search features should provide suggestions, display an open, visible field with space for at least 18 characters, and allow for typos that lead to relevant search results (Pernice, et al., 2013). Content should be presented factually and be arranged by topic (Pernice, et al., 2013). Avoid stereotypes and generalization about seniors (Pernice, et al., 2013). Unfamiliar terms should be defined and avoided unless absolutely necessary (Pernice, et al., 2013). When organization information, key information should be presented first (Pernice, et al., 2013). Information should be chunked into easy-to-scan sections with clear headings (Pernice, et al., 2013). Language should use an 8th grade level or below (Pernice, et al., 2013). Information presented should be written in active voice, use positive language, and be summarized at the end (Pernice, et al., 2013,). When developing a computer-based training, use a consistent layout throughout with clear paths to content. The user’s current location should be clearly displayed, and subcategories should be exposed when hovering (Pernice, et al., 2013). Navigation should use the fewest clicks possible and avoid changes (Pernice, et al., 2013). Pop-up windows should be avoided (Pernice et al., 2013). Graphics and videos should enhance and supplement text, not replace it, words should be used instead of abstract symbols, and should be short and to the point (Pernice, et al., 2013). Buttons should be large, obviously clickable, and not require precise movement (Pernice, et al., 2013). Patterned backgrounds and the use of yellow, blue, or green close together should be avoided (Pernice, et al., 2013). Forms should only require or ask for necessary information, be forgiving of errors, and provide clear explanations (Pernice, et al., 2013). Pernice, Estes, and Nielson point out that websites are 43% more difficult for senior citizens to use than for their younger counterparts, so integrating senior citizen web design concepts makes the Internet more accessible to the elderly (2013).

**Summary**

Older adults have a lower level of confidence in the computer skills than their younger counterparts but are willing and able to learn safe practices. When presenting information, the elderly prefer to follow written lists of instructions. Information should be presented clearly and concisely and avoid the use of jargon. Any tech-related vocabulary should be defined, preferable at the beginning of the presentation. Repeating material may help with increasing comprehension and long-term memory of the content. Cognitive decline in older adults is strongly linked to their susceptibility to fraud. They may also overestimate their ability to safely manage their finances even when they recognize their cognitive decline. The part of the brain that deteriorates first as part of cognitive decline is also responsible for emotional regulation and safe decision making. Because of this, elderly individuals experiencing cognitive decline tend to focus on the positives of information presented as opposed to the negatives or potential consequences.

The elderly are commonly targeted by fraudsters because of the stereotypes of older generations being more trusting and gullible. The fast-evolving nature of tech makes developing specific workshop content difficult. Instead, strong frameworks that are adaptable to new information should be developed. Preventing fraud victimization is a community effort that requires the partnership of experts, government agencies, community outreach groups, tech companies, and families.

**Methodology**

This project draws from the literature review in order to create a research-backed cybersecurity curriculum for seniors. The goal of this project is to arm seniors with the tools and knowledge they need to stay safe online. A large part of the cybercrimes that senior citizens encounter are scams, so there is a heavy focus on general scam avoidance and financial safeguards. The following research questions are presented, given in null hypothesis format:

H1. There are no generational barriers to effective communication with senior citizens.

H2. Senior citizens see no benefit from the integration of technology into their lives.

H3. There are no psychological factors that increase fraud victimization in the elderly.

H4. Senior citizens to not engage in risky cybersecurity practices.

H5. Senior citizens do not regularly encounter financially detrimental cybercrimes.

H6. Senior citizens cannot mitigate cybersecurity issues by themselves.

H7. Senior citizens do not encounter barriers when asking for help with cybersecurity issues.

In the analysis section, the null hypotheses will be analyzed in the context of the literature review. The analysis will then be applied and integrated into the project’s curriculum. The goal of this research is to determine the sociological, psychological, and financial factors that contribute to the cybercrime victimization of the elderly.

**Variables**

This project analyzes the relationship between senior citizens and cybersecurity for the purpose of developing an effective community education curriculum. Thus, variables from cyberspace and senior citizens must be considered.

**Independent variables.** Independent variables in the context of this study include the social support and social systems of senior citizens, cognitive decline, and cybercrime and cyberscam types. Communication methods also fall under independent variables, since this paper examines the media and communication preferences of senior citizens for the purpose of developing effective communication within the curriculum.

**Dependent variables.** Dependent variables include the frequency and severity of cybercrime victimization of the elderly. Frequency looks at how often senior citizens are victimized by cybercrime. Severity looks at both the emotional and financial fallout of cybercrime victimization. Cybercrime victimization creates a negative feedback cycle that turns psychological wellbeing into a dependent variable.

**Case Studies**

The case studies presented in the literature review focus on how senior citizens perceive cyberspace, cybersecurity, and personal information. The case studies are presented in the form of interviews with senior citizens and people who work with senior citizens. Anecdotes are also presented from communication experts and medical personnel.

**Data Collection and Sources**

Data is collected from articles in peer-reviewed journals, U.S. government reports and publications, and the master’s and PhD projects of previous students. Case studies present the viewpoints and opinions of senior citizens as it relates to cybersecurity and identity protection. The case studies also look at the sociological and psychological components behind cybercrime victimization in the elderly. U.S. government reports provide historical data on cybercrime and scam victimization of the elderly and other age groups. The reports also include the types and frequency of cybercrimes and scams, which is useful in developing an effective curriculum. Government publications and the projects of previous students provide frameworks and class ideas which can be integrated into the curriculum packet.

**Analysis Procedures**

The literature review was analyzed in the context of the seven null hypotheses. The analysis section discusses how the literature review’s findings can be integrated into the curriculum packet. Quantitative and qualitative data is presented to contrast between U.S. senior citizens and other age or geographic groups.

**Limitations and Bias**

The studies presented from peer-reviewed journals distinctly lacked viewpoints from black, indigenous, and people of color. For the majority of study participants, especially in Cassandra Cross’ articles, recruitment came from senior centers, which indicates that these seniors already had access to senior specific resources.

As for the curriculum packet, user testing is inadvisable at the time of writing due to the current COVID-19 pandemic. The specific information contained in the curriculum packet may need updated by the time the pandemic has subsided. For this reason, the packet will include a general framework where instructors can easily update relevant information.

**Analysis**

The analysis section will be separated into seven subsections, focusing on hypotheses one through seven. Each subsection will draw from the literature review in order to disprove the hypothesis in question. Furthermore, the information obtained from the literature review will be analyzed for its relevant integration into the curriculum packet.

**H1. There are no generational barriers to effective communication with senior citizens.**

Sivricova and Moiseeva point out that generational stereotypes are shaped by a shared history (2018). This shared history is culturally and geographically defined (Sivricova & Moiseeva, 2018). The shared history that serves as a basis for generational knowledge and understanding varies so widely across the United States. For example, Black, Native American and Alaska Native, and Hispanic senior citizens would expect to have a different shared history than that of upper middle-class Caucasian Americans. Geographically, the United States spans from Alaska, Hawaii, Florida, Maine, Mississippi, and California. Each state and community has a distinctly different shared history that must be considered when trying to communicate with the elderly population. Such stereotypes can be a barrier to trust and respect between generations (Bridge, 2018). Since technology shapes generational identity (Cantoni & Danowski, 2015), it is important to be patient and understanding with senior citizens’ frustrations with technology (Handelsman, 2016). Younger generations prefer to learn by trial and error, while older generations prefer to learn through lectures (Cantoni & Danowski, 2015). The curriculum design and framework developed in this project will account for the preferred learning styles of the elderly along with cultural and geographic influences of the shared history of senior citizens.

**H2. Senior citizens see no benefit from the integration of technology into their lives.**

The Internet provides senior citizens with hobbies, banking services, entertainment and social connection (Zheng, et al., 2015). Senior citizens primarily use the Internet for social connection, financial information, and health information (Zheng, et al., 2015). According to a study from the University of Utah, seniors who actively engage in online activities are less stressed than those who do not (Zheng, et al., 2015). Additionally, the researchers point out that ability to seek out information and engage socially though the Internet contributes to overall life satisfaction in the elderly (Zheng, et al., 2015). Handelsman and Bridge caution that technology should be used when it serves as the most appropriate platform, but that digital technology should not be used for the sake of looking futuristic (2016, 2017). Bridge states that technology can enhance cross-generational communication, especially within the workplace (2017). Cybersecurity education must take into account that the Internet is used for legitimate communication and business reasons (Cross, 2016). The elderly use the Internet and e-mail to ward off loneliness (Cross, 2016). Thus, cybersecurity education should be focused on how to safely navigate and interact online (Cross, 2016).

The curriculum will integrate technology where appropriate, such as using a slide show presentation. Nonetheless, the class will use paper handouts and quizzes since paper is the easiest and most appropriate platform in this situation. Since senior citizens primarily use the Internet for social connection, financial information, and health information (Zheng, et al, 2015), the curriculum will focus on avoiding scams in these sectors. Additionally, the curriculum will not advocate for an abstinence only approach to cybersecurity for senior citizens, since the senior citizens who do engage online see an increase in their quality of life and psychological wellbeing.

**H3. There are no psychological factors that increase fraud victimization in the elderly.**

Senior citizens are particularly vulnerable to fraud because of isolation (Cross, 2016). Senior citizens are particularly vulnerable to fraud, especially romance scams, after the death of a spouse (Cross, 2016). The elderly also may have a physical inability to leave the house, with no car or ability to drive a car and a lack of nearby family, furthering their social isolation (Cross, 2016). Isolation and loneliness decrease a person’s overall mental health and leaves them vulnerable to fraud (Cross, 2016). Cognitive decline is the largest indicator single of fraud victimization (Judges, et al., 2017). A victim’s lack of conscientiousness, lack of honesty, and lack of humility are also associated with fraud victimization, but the correlation is not nearly as strong as that of cognitive decline (Judges, et al., 2017). Adults who are experiencing overall cognitive decline are less likely to report decreased confidence in their ability to manage their finance, even if they report decreased confidence in overall activities (Judges, et al., 2017). Cognitive decline is linked to poor financial literacy and poor financial decision making (Judges, et al., 2017). From a biological standpoint, vmPFC activity in the brain declines as people age, and is one of the first parts of the brain to indicate age-related decline (Koester, et al., 2016). VmPFC decline creates a halo effect around information and causes people to focus on positive information presented (Koester, et al., 2016). VmPFC decline is hypothesized as one of the reasons the elderly are more likely to trust misleading advertisements (Koester, et al., 2016).

Loneliness and cognitive decline are major risk factors for cyberfraud victimization. Loneliness can be addressed through community groups such as senior centers or faith-based groups. Cognitive decline, however, is a more difficult topic to address. Cognitive decline requires direct intervention. For this reason, senior citizens are hesitant talk with their families if they are a victim of fraud (Cross, 2016). Some seniors worry that they will lose freedoms when they admit to being a victim of fraud (Cross, 2016). Seniors who hide fraud victimization often fall into a loop of isolation, loneliness, shame, and repeat victimization (Cross, 2016). Cross recommends having community resources available where senior citizens can talk about their fraud victimization without judgment or blame in order to prevent repeat victimization (Cross, 2016). Similar programs can be implemented in communities where the curriculum is deployed in order to increase the psychological wellbeing of senior citizens. These programs should be easily accessible and free to use.

**H4. Senior citizens do not engage in risky cybersecurity practices.**

Seniors engage in risky cybersecurity practices, some by revealing exploitable personal information through social media and online quizzes (Morgan, 2015). Genealogy websites are also quite popular with senior citizens and encourage users to reveal personal information about themselves and their families (Cross, 2016). This information is exploitable by threat actors, but in at least one case, a senior citizen thought that revealing this information wasn’t a risk because the website requires a login (Cross, 2016). Some seniors respond to phishing e-mails with personal information either out of curiosity or out of hope that a scam will be true (Cross, 2016). Phishing e-mails sometimes do not raise red flags for seniors until the scammer asks for money (Cross, 2016). One senior interviewed by Cross rationalized that even if they gave a scammer their banking details, the scammer would not find any money in the account (Cross, 2016). They were unaware that scammers can use banking details to open new accounts or lines of credit (Cross, 2016). Senior citizens lack an understanding of the capabilities of threat actors and therefore have generally poor cybersecurity risk management practices.

**H5. Senior citizens do not regularly encounter financially detrimental cybercrimes.**

Cybercriminals exploited $835,164,766 from victims over the age of 60 in 2019(IC3, 2019), just from reports to the FBI alone. Cyberfraud often goes unreported because of feeling of shame and guilt (Cross, 2016). Senior citizens are targeted by cyberscammers because of their generally favorable credit history and their trusting and helpful nature (Munanga, 2019). According to the FTC, the median amount lost per fraud incident from victims over the age of 80 was $1,100 (2018). In 2018, the greatest number of reports of fraud reporting a financial loss for people over the age of 60 were from tech support scams (FTC, 2018).

**H6. Senior citizens cannot mitigate cybersecurity issues by themselves.**

Older adults are able to learn the skills necessary to stay safe online (Gonzalez, 2019). Senior citizens apply cybersecurity skills when they are taught, but need trainings with detailed and specific information (Gonzalez, 2019). Increased conscientiousness is associated with lower fraud victimization (Judges, et al., 2017). This is because people who are conscientious tend to take time to consider their financial actions and pay closer attention to details (Judges, et al., 2017). Harvard Medical School reports that conscientiousness can be raised in a person by training them to focus on the specifics, making daily plans, using reminders, and staying social (Harvard, 2012). Judges, et al. brings up the possibility of cognitive training techniques as a method of preventing fraud victimization in the elderly as a future area of study (2017).

**H7. Senior citizens do not encounter barriers when asking for help with cybersecurity issues.**

Senior citizens encounter the misconception that they are unable to learn the computer and information security skills necessary to stay safe (Gonzalez, 2019). Older adults need formal, structured educational resources with specific and detailed information that accounts for their needs as senior citizens (Gonzalez, 2019). The definition of personal information is quite broad, which makes rationalizing what should and should not be shared difficult (Cross, 2016). Risk management for information security can be difficult for seniors, especially when they do not understand the abilities of threat actors (Cross, 2016). This project bridges the barrier by providing a structured curriculum tailored to the needs of seniors.

**Curriculum Packet**

The curriculum packet includes a sample lesson plan, a cybercrime handout for students to keep for future reference, an assisted notes handout, a quiz, a quiz answer sheet with justifications, and an adaptable framework for future curriculum development. There is also a “How to...” handout that provides detailed step-by-step instructions on how to run updates, set-up online banking, set-up a credit freeze and credit fraud alert, and report fraud and cybercrime. The “How to…” document’s step-by-step instructions are consistent with Gonzalez’s recommendation that awareness programs should use specific and detailed information (2019). A separate slide show presentation will be attached to go along with the curriculum. The quiz uses large-print sans-serif font, as recommended by Pernice, Estes, and Nielson. The handouts and slide show presentation avoid the use of all-caps and italics since they are difficult for senior citizens to read and uses 12-point or above sans-serif font (Pernice, et al., 2013). The assisted notes handout can be extracted from the PowerPoint presentation using the notes page under the view tab. The support and reporting slide of the presentation should be updated to reflect local resources prior to the class. The framework covers the communication needs and considerations along with how to build course content using up-to-date resources. The curriculum packet is intended for use with a class of around 5-20 students and encourages discussion and critical thinking in addition to providing senior citizens with step-by-step instructions on how to stay safe online. The smaller the class, the more individualized attention can be given to students who struggle with specific issues. The curriculum can be used in senior centers and senior living facilities, community schools' programs, Osher Lifelong Learning programs, and more.

**Sample Lesson Plan**

**Target Audience:**

Senior citizens age 65 and over

Content is also relevant to caregivers and family members of senior citizens

**Learning Objectives:**

Students will understand current cybercrime trends and how it relates to them as senior citizens.

Students will know how to access resources to prevent, mitigate, and report cybercrime.

Students will gain skills and techniques with which to avoid cybercrime.

**Materials/Supplies/Handouts Needed:**

Pens/pencils

Cybercrime handout

Assisted notes handout

**Technology Requirements:**

Projector and screen **or** large TV for displaying slide show presentation

Slide show viewer software

**Preparation:**

Advertise class in relevant areas

Obtain a sufficient space for the class

Partner with applicable local agencies or tech companies

Print off handouts and quiz

Sharpen pencils if necessary

Obtain snacks for class to increase attendance

**Activities:**

Quiz

Discussion

|  |  |  |
| --- | --- | --- |
| Time (minutes) | Activity | Purpose |
| 10 | Introduction | -Develops a rapport with students |
| 10 | Quiz | -Develops an understanding of the baseline cybersecurity knowledge of class |
| 10 | Quiz Review | -Starts students thinking about their role in cybersecurity |
| 5 | Handouts | -Assists students with vision or hearing difficulties during PowerPoint presentation  -Provides reference and note-taking materials |
| 20-30 | Slide Show Presentation | -Delivers core of cybersecurity information |
| 10-20 | Questions/Discussion | -Address student questions and revisit unclear terms  -Discuss cybercrimes and cybercrimes that students have encountered if they feel comfortable sharing  -Analyze actions the student took and how those actions would change after being presented with class information |
| 10 | Wrap-up | -Provide short overview of topics covered in class  -Direct students to further research and resources available in their community |
| 10-30 | Cookies/Coffee | -Food and drink are a way to increase attendance |

**Cybercrime Handout**

**Cybercrime Types**

* Ransomware
* Phishing
* Tech Support Scams
* Romance Scams
* Clickbait

**Avoiding Cybercrime**

Don’t interact with scammers

* Don’t respond to phishing e-mails
* Don’t open attachments
* Don’t click on links in e-mails

Set-up online banking

* Monitor regularly

Monitor current scams and cybercrime trends

* AARP Fraud Watch
* FTC Scam Alerts
* IC3 Consumer Alerts

**Mitigating Cybercrime**

Run updates regularly

* Operating system (OS) updates
* Application updates like Microsoft Word
* Anti-virus updates

Backup essential files

* Photos
* Important documents
* Use a disconnected external hard drive for backups

**If You are a Victim of a Cybercrime**

File a police report

* Obtain a copy

File IC3 and FTC reports

Initiate fraud alert on credit

Close accounts that the criminal has access to and change pins/passwords

* Bank accounts
* Online accounts

Update computer and anti-virus software

**How to…**

**Update your computer**

* Apple
  + Click on the Apple icon in the top left corner
  + Select “About This Mac”
  + A window should pop up with a button that says “Software update…”
  + Click the “Software update…” button to run updates
* Windows
  + Click on the “Start” button in the lower left corner
  + Type in “Update”
  + Select “Check for updates”
  + If updates are available, click “Install updates”
* Chromebook
  + Click on the clock in the lower right corner
  + Select the settings icon in the pop-up menu
  + Select “About Chrome OS” below the menu bar on the left side of the screen
  + Click “Check for updates” on the right side of the screen
  + Click “Restart” once updates have finished installing

**Update your anti-virus**

**Note:** Use trusted anti-virus software. Some malware can look like anti-virus software.

**Trusted anti-virus software examples:** Windows Defender, Norton, Avast, Bitdefender, Kaspersky, McAfee, Trend Micro, F-Secure, Intego, AVG Technologies, Webroot, ESET, Malwarebytes

* Windows Defender
  + - Click on the “Start” button in the lower left corner
    - Type in “Defender”
    - Select “Windows Defender Security Center”
    - Click “Virus & threat protection”
    - Click “Protection updates”
    - Click “Check for updates”
    - Install updates if available
* Malwarebytes for Windows
  + Click on the “Start” button in the lower left corner
  + Type in “Malwarebytes”
  + Select “Malwarebytes”
  + In the lower right corner of the dashboard, look for the word “Updates”
  + Click on the blue word next to the word “Updates” to check for updates
  + Install updates if available

**Set-up online banking**

* Navigate to your bank’s website
* On the home page under the sign-in, there should be a button labeled “Enroll in Online Banking” that leads to a form
* Fill out the form
* Choose a password at least 12 characters long
* Check your accounts regularly to detect unauthorized purchases and stop fraud early

**Set-up a credit freeze**

**Note:** Setting up a credit freeze does not affect your credit score. You have to set up a credit freeze individually with each of the three credit bureaus. Placing and lifting a credit freeze is free.

* Equifax
  + Visit <https://www.equifax.com/personal/credit-report-services/>
  + Select “Place A Freeze”
  + Fill out the form
  + Store your password in a secure place
    - You’ll need your password in order to unfreeze your account
  + Or call: 800-685-1111
* Experian
  + Visit <https://www.experian.com/help/>
  + Select “Security Freeze”
  + Select “Add a Security Freeze”
  + Select “Freeze my own credit file”
  + Fill out the form
  + Store your pin in a secure place
    - You’ll need your pin in order to unfreeze your account
  + Or call: 888-397-3742
* TransUnion
  + Visit <https://www.transunion.com/credit-help>
  + Select “Freeze Credit”
  + Select the “Add Freeze” button under “Freeze My Credit” heading
  + Fill out the form
  + Store your password in a secure place
    - You’ll need your password in order to unfreeze your account
  + Or call: 888-909-8872

**Set-up a fraud alert on your credit**

* General Information:
  + Setting up a fraud alert on your credit is free of charge
  + You should set up a fraud alert if your personal information has been stolen, lost, or involved in a breech
  + When you set up a fraud alert with one credit bureau, it issues a fraud alert to the other credit bureaus
* Equifax
  + Visit <https://www.equifax.com/personal/credit-report-services/>
  + Click on “Place an Alert” under the “Add a fraud or active duty alert” heading
  + Fill out the form
  + Store your password in a secure place
  + Renew fraud alert yearly
* Experian
  + Visit <https://www.experian.com/help/>
  + Click on “Fraud Alert”
  + Click on “Add a Fraud Alert”
  + Click on “Temporary fraud alert”
  + Scroll down to “Add a fraud alert using your personal information”
  + Fill out the form
  + Renew fraud alert yearly
* TransUnion
  + Visit <https://www.transunion.com/credit-help>
  + Click on “Fraud Alerts”
  + Click on “Add Fraud Alert” under the “Initial Fraud Alert – 1 Year” heading
  + Click on “Register” under the “Create an account” heading
  + Fill out the form
  + Renew fraud alert yearly
  + Or call: 800-680-7289

**Report a scam or identity theft to the FTC**

* FTC Complaint Assistant to report **fraud or scams**:
  + FTCComplaintAssistant.gov **or** ftc.gov/complaint
* For FTC complaints regarding **identity theft** visit:
  + IdentityTheft.gov
* Or call:
  + 1-877-FTC-HELP (1-877-382-4357)

**Report a cybercrime to the FBI**

* The FBI’s Internet Crime Complaints Center (IC3) handles cybercrimes
  + Visit ic3.gov
  + Click “File a Complaint”
  + Click “IC3.gov”
  + Click “I accept” after reading the FAQs (Frequently Asked Questions)
  + Fill out the form

**Report a scam to AARP**

* Visit AARP’s website to report a scam or search existing scams
  + Type AARP.org/money/scams-fraud/tracking-map in your search bar
  + Fill out the “Report a Scam” form
  + AARP scam reports are public, so don’t include personally identifiable information
* Or call AARP’s Fraud Watch Network Helpline:
  + 1-877-908-3360
  + Hours: Monday – Friday 7 am to 10 pm Eastern Time

Quiz

Answer with “True” or “False”

1. Setting up online banking increases your chances of cybercrime victimization.
2. Shaming scammers is an effective way to make them stop.
3. You should update your computer and your anti-virus software regularly.
4. Short passwords are better because they are easier to remember.
5. If you don’t use a computer, your personal information cannot be exploited by cybercriminals.
6. A person’s full name, social security number, driver’s license number, passport number, and e-mail address can be purchased for around $4 on the dark web.
7. Senior citizens are commonly targeted by scammers because of their good credit scores.
8. You should not click links in unsolicited or suspicious e-mails.
9. Wire transfers can be reversed.
10. If a person you meet online asks for your bank account information saying that they will give you money, they are most likely a scammer.

**Quiz Answer Key**

1. Setting up online banking increases your chances of cybercrime victimization.
   1. **False**. Online banking decreases the risk of identity theft and fraud victimization (Pak, et al., 2018).
2. Shaming scammers is an effective way to make them stop.
   1. **False**. Scammers are often highly trained individuals with lots of experience in social engineering (Cross, 2016).
3. You should update your computer and your anti-virus software regularly.
   1. **True.** Computers and anti-virus software require regular updates to stay current and protected against the latest threats (Christensson, 2010).
4. Short passwords are better because they are easier to remember.
   1. **False.** Long, unique passwords are recommended because they are harder for hackers to crack. NIST recommends a minimum password length of eight characters (Grassi, Fenton, Newton, Perlner, Regensheid, Burr, & Richer, 2017).
5. If you don’t use a computer, your personal information cannot be exploited by cybercriminals.
   1. **False**. Even if you don’t use a computer, your personal information is most likely available online through public records, genealogy websites, and donation recognitions in newsletters, and more (Cross, 2016).
6. A person’s full name, social security number, driver’s license number, passport number, and e-mail address can be purchased for around $4 on the dark web.
   1. **True**. The exact purchase amount varies based on a victim’s credit score and other factors, but a packet of information with person’s full name, SSN, driver’s license number, passport number and e-mail sells for around $4 on the dark web as of 2020 (Damiani, 2020).
7. Senior citizens are commonly targeted by scammers because of their good credit scores.
   1. **True**. The stereotype of senior citizens having good credit scores and the ability to create long lines of credit makes them a target for scammers (Cross, 2016).
8. You should not click links in unsolicited or suspicious e-mails.
   1. **True.** These links can lead a user to malware, or a website designed to steal their personal information (AFA, 2020).
9. Wire transfers can be reversed.
   1. **False.** Wire transfers cannot be reversed once the recipient’s bank has accepted the payment order (Baylor, 2019). There is no exception for fraud victims.
10. If a person you meet online asks for your bank account information saying that they will give you money, they are most likely a scammer.
    1. **True.** The FBI reports that if someone offers to deposit money in your bank account in exchange for your banking details, it is most likely a scammer trying to carry out fraud or theft (FBI, n.d.). This is a common tactic used in romance scams (FBI, n.d.)

**Framework**

**Communication**

* Provide written information to supplement orally presented information
* Adapt for cultural and geographic communication differences
  + Rate of speech, length of class, resources available
* Be mindful of communication difficulties such as hearing or vision loss
  + Large-print font, microphones, handouts

**Class topics**

* Password/Authentication management
  + Retrieved latest recommendations from NIST
* Top cybercrime and fraud trends
  + Retrieve top 5 or top 10 cybercrime trends by frequency and by financial impact from IC3 yearly report
  + Retrieve fraud data from FTC yearly report
* Skills and tools
  + Social engineering prevention
  + How to run and/or automate operating system and application updates
  + Analyze top cybercrime trends
  + Social media literacy

**Trusted Sources**

* AARP
* IC3/FBI
* FTC
* NIST

References

Air Force Association. (2020). CyberGenerations. *CyberPatriot.* Retrieved from <https://cyber-education.s3.amazonaws.com/CyberGenerations/CyberGenerations+Self-Paced+Guide_Final.pdf>

Anderson, K. (2013). Consumer Fraud in the United States, 2011. *Federal Trade Commission*. Retrieved from <https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf>

Baylor, C. (2019). What Is the Time Frame for Reversing a Wire Transfer? *The Nest.* Retrieved from <https://budgeting.thenest.com/time-frame-reversing-wire-transfer-33881.html>

Bridge, R. (2017). CROSS-GENERATIONAL COMMUNICATION. *Training Journal*, 24–26. Retrieved from <http://search.proquest.com/docview/2225756625/>

Canadian Centre for Cyber Security. (2018). Cyber Threat and Cyber Threat Actors. Government of Canada. Retrieved from <https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors>

Cantoni, L., & Danowski, J. A. (Eds.). (2015). *Communication and technology*. Retrieved from <https://ebookcentral.proquest.com>

Christensson, P. (2010). Antivirus Definition. *Tech Terms.*  Retrieved from <https://techterms.com/definition/antivirus>

Christensson, P. (2016). Operating System Definition. *Tech Terms.*  Retrieved from <https://techterms.com/definition/operating_system>

Cross, C. (2016). ‘They’re Very Lonely’: Understanding the Fraud Victimisation of Seniors. *International Journal for Crime, Justice and Social Democracy*, *5*(4), 60–75. <https://doi.org/10.5204/ijcjsd.v5i4.268>

Cross, C. (2016). “But I’ve never sent them any personal details apart from my driver’s licence number …”: Exploring seniors’ attitudes towards identity crime. *Security Journal*, *30*(1), 74–88. <https://doi.org/10.1057/sj.2015.23>

Damiani, J. (2020). Your Social Security Number Costs $4 On The Dark Web, New Report Finds. *Forbes.* Retrieved from <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/#19bf4b1013f1>

Dennis, M. (2019). Cybercrime. Encyclopedia Britannica. Retrieved from <https://www.britannica.com/topic/cybercrime>

FBI. (n.d.). Romance Scams. *Federal Bureau of Investigations.* Retrieved from <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams>

Fossati P. (2012). Neural correlates of emotion processing: from emotional to social brain. *European neuropsychopharmacology : the journal of the European College of Neuropsychopharmacology*, *22 Suppl 3*, S487–S491. https://doi.org/10.1016/j.euroneuro.2012.07.008

Fruhlinger, J. (2019). Social engineering explained: How criminals exploit human behavior. *CSO Online.* Retrieved from <https://www.csoonline.com/article/2124681/what-is-social-engineering.html>

Fruhlinger, J. (2020). Ransomware explained: How it works and how to remove it. *CSO Online.* Retrieved from <https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html>

FTC. (2018). Protecting Older Consumers. *Federal Trade Commission.* Retrieved from <https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2017-2018-report-congress-federal-trade-commission/protecting_older_consumers_-_ftc_report_10-18-18.pdf>

FTC. (2019). How to Recognize and Avoid Phishing Scams. *Federal Trade Commission.* Retrieved from <https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

Grassi, P., Fenton, J., Newton, E., Perlner, R., Regensheid, A., Burr, W., Richer, J. (2017). Digital Identity Guidelines. *NIST.* Retrieved from <https://pages.nist.gov/800-63-3/sp800-63b.html>

Handelsman, J. (2016). Enhancing Cross-Generational Communication. *ASHA Leader*, *21*(6), 6–7. <https://doi.org/10.1044/leader.FTP.21062016.6>

Harvard Medical School. (2012). Raising Your Conscientiousness. *Harvard Health Publishing.* Retrieved from <https://www.health.harvard.edu/staying-healthy/raising-your-conscientiousness>

IC3. (2020). 2019 Internet Crime Report. *Federal Bureau of Investigation.* Retrieved from <https://pdf.ic3.gov/2019_IC3Report.pdf>

Javed, Y., Davis, B., & Shehab, M. (2019). Seniors’ Media Preference for Receiving Internet Security Information: A Pilot Study. *arXiv.org*. Retrieved from <http://search.proquest.com/docview/2189132965/>

Judges, R., Gallant, S., Yang, L., &Lee, K. (2017). The Role of Cognition, Personality, and Trust in Fraud Victimization in Older Adults. *Frontiers in Psychology*, *8*, 588–588. <https://doi.org/10.3389/fpsyg.2017.00588>

Kane, D., Riddell, C., & Morales, I. (2015). *Security awareness training of the elderly: Means, methods, discovery, safety, and security* (ProQuest Dissertations Publishing). Retrieved from <http://search.proquest.com/docview/1754639702/>

Koestner, B. P., Hedgcock, W., Halfmann, K., & Denburg, N. L. (2016). The Role of the Ventromedial Prefrontal Cortex in Purchase Intent Among Older Adults. *Frontiers in aging neuroscience*, *8*, 189. https://doi.org/10.3389/fnagi.2016.00189

Leclerc, C. M., & Kensinger, E. A. (2008). Age-related differences in medial prefrontal activation in response to emotional images. *Cognitive, affective & behavioral neuroscience*, *8*(2), 153–164. https://doi.org/10.3758/cabn.8.2.153

Merriam-Webster. (n.d.). Clickbait. *Merriam-Webster.com dictionary*. Retrieved from https://www.merriam-webster.com/dictionary/clickbait

Morgan, J., Sharum, B., Dell’Osso, L., & Salmons, J. (2015). *Exploring senior citizen perceptions of their cyber data privacy and security* (ProQuest Dissertations Publishing). Retrieved from <http://search.proquest.com/docview/1752059359/>

Munanga, A. (2019). Cybercrime: A New and Growing Problem for Older Adults. *Journal of Gerontological Nursing*, *45*(2), 3–5. <https://doi.org/10.3928/00989134-20190111-01>

Pak, K., Shadel, D., & Williams, A. (2018). Up for Grabs: Taking Charge of Your Digital Identity: AARP National Survey of Internet Users Age 18+. *AARP Research.* Retrieved from <https://doi.org/10.26419/res.00228.000>

Penrice, K., Estes, J., Nielson, J. (2013). *Senior Citizens (Ages 65 and older) on the Web*. Nielson Norman Group: Fremont, CA.

Rivera González, J., DeCarlo, R., & Medina, K. (2019). *Building Information Security Awareness and Training for Older Adults* (ProQuest Dissertations Publishing). Retrieved from <http://search.proquest.com/docview/2305191208/>

Rogalsky, C., Vidal, C., Li, X., & Damasio, H. (2012). Risky decision-making in older adults without cognitive deficits: an fMRI study of VMPFC using the Iowa Gambling Task. *Social neuroscience*, *7*(2), 178–190. https://doi.org/10.1080/17470919.2011.588340

Sivricova, N. & Moiseeva, E.. (2018). Values of generations in the context of inter-generational communication. *SHS Web of Conferences*, *55*. <https://doi.org/10.1051/shsconf/20185502017>

Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of Persons by Fraud. *Crime & Delinquency*, *41*(1), 54–72. <https://doi.org/10.1177/0011128795041001004>

Zheng, R., Spears, J., Luptak, M., & Wilby, F. (2015). Understanding Older Adults’ Perceptions of Internet Use: An Exploratory Factor Analysis. *Educational Gerontology*, *41*(7), 504–518. <https://doi.org/10.1080/03601277.2014.1003495>