Cybersecurity Awareness Course for the Elderly

Shacara Pitre

CYSE 494: Entrepreneurship in Professional Studies

Professor Akeyla Porcher

April 18, 2023

The world is constantly evolving and the younger generations are adapting naturally with the times. However, the elderly are having a harder time adjusting as they are still not used to this digital age world. With practically everything being moved from paper to digital, the elderly are having to work twice as hard to keep up with our growing society. The baby boomers and some generation x are having to learn and rely on their grandchildren for anything involving technology. This makes them vulnerable and a perfect target for cyber-attacks, specifically when it comes to vishing schemes. Vishing involves a person using fabricated scenarios over the phone in order to gain personal information.

The elderly are a prime target for cybercriminals as they are inclined to give out their personal information over the phone since many of them have not been educated on cybersecurity. Therefore, the problem is the elderly not having the knowledge of internet safety. For instance, the elderly are vulnerable to scams such as those offering low cost insurance and discount drugs. Some of the reasons why the elderly are vulnerable to online scams are that they lack computer skills and are too trusting. When it comes to their lack of computer skills, this refers to them not having security on their computers such as firewalls, secure passwords, automatic updates for software, etc. Next, the elderly are too trusting when it comes to material that looks official since they do not know the signs of an online scam.

There are many sites in which the elderly can be vulnerable to such as on social media (i.e. Facebook) and online dating apps. In order to solve this problem, my group and I came up with the idea of creating a cybersecurity awareness course for the elderly because they fall victim to different cyber-attacks such as phishing and identity theft. We are going to offer this course through a website in which the elderly can learn about various cybersecurity risks. One of the main objectives within this course is to provide the elderly with a positive and comfortable

online learning environment where they feel motivated and encouraged to protect themselves on the internet.

The course will be $9 per video lecture and it is a one-time purchase for the elderly. For this project, we will be building a website so all the courses are in one place. For the courses, they are going to be video lectures that will engage the elderly and each lecture will discuss a different topic. At the end of each lecture, there will be a review quiz or questionnaire at the end that reiterates what they have learned in that specific course. There are going to be 5 basic lectures that are broken up into units, so that the content builds with each unit.

The courses are as follows: Introduction to Cybersecurity, Passwords and Management, Social Engineering, Antivirus, and Recap. In the Introduction to Cybersecurity course, its purpose is to discuss the basics of cybersecurity and introduce the relevance of it to the elderly. In other words, it will give them reasons why they are prime targets within cyber-attacks along with internet safety tips. Then, as the elderly progress within the course, they will move on to learn about how they can detect phishing scams among other things. Overall, we want to ease the elderly into this content as it can be overwhelming for them if they were to receive this information all at once.

The goal of this paper is to showcase in detail the problem which is the elderly and their lack of knowledge with cybersecurity. As a result, I will explain how our cybersecurity awareness course will be the perfect innovation. I will explain the details including what is involved within each lecture. There are some barriers that my group and I will face with the creation of this course. Some challenges that my group and I will take into consideration and address within this paper are whether or not the elderly have access to a computer, the internet, financial issues, and the ability to access a website to even get started.

Technology is forever evolving and that requires us as a society to adapt. As we turn on the news, we find many stories that report on various cybercrimes that are happening around the world. I want to start this literature review off by starting with defining cybersecurity. There are many definitions of cybersecurity. However, in my words, cybersecurity involves detecting malicious attacks on computer systems and protecting networks and computer systems from information that is not authorized from getting out.

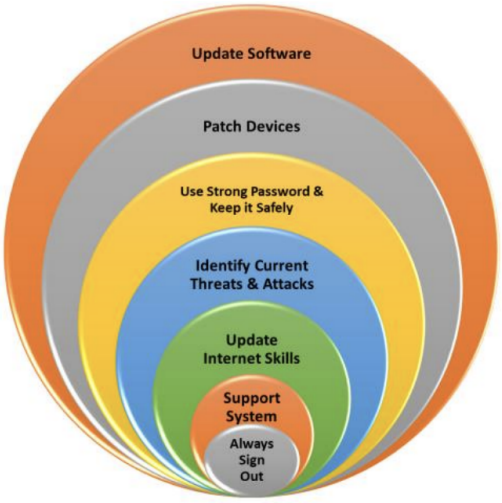
The elderly are one of the groups that we don't think use the internet as much. However, there were over 50% of them using the internet in 2012. The elderly are using the internet to get involved with community groups, plan travel, manage their finances, shop, and to keep in touch with their friends and families (CISA, 2012). When it comes to the elderly, cybersecurity concerns have been overlooked and there is limited research. Researchers tend to focus on how cybersecurity affects the younger generations and adults. Among the groups of internet users, the elderly make up around 50% and the numbers are gradually increasing (Zulkipli et al., 2021). The elderly are naturally not as tech savvy as the youth and lack the interest to learn because of health issues or physical conditions since they would need assistance to use a new device.

To focus on devices, elderly people do not properly store them. They are not aware of the importance of installing security software, such as antivirus software or anti-spam software on their devices. Furthermore, they do not update their device regularly making them vulnerable to cyber-attacks. Ensuring that your device is up to date will ensure that you have the latest security to protect yourself against these kinds of threats. Unfortunately, if they become the victim of a cybercrime, it typically goes unreported to authorities because of two factors. One is that the elderly are not sure where they should report these cases. Second, they don't know how to handle

this issue since many of them are not used to crimes that can happen through technology (Zulkipli et al., 2021).

As I stated earlier, the elderly are more trusting when it comes to strangers and are inclined to disclose confidential information about themselves through social engineering tactics performed by cyber criminals. The elderly are more familiar with judging a person when they meet in person. However, the intention of those online is not as noticeable as should make them more skeptical. For clarity, the "elderly are typically more trusting and respectful of official looking material than younger generations, so are more apt to fall for scams" (Arfi & Agarwal, 2013). Passwords and password management are one of the main problems when it comes to the elderly and security. Instead of using complex passwords, they use basic ones that are easy for them to remember. They even go as far as to repeat passwords for different applications.

Phishing, behavioral attack, consumer attack, and identity theft were the four most common cyber-attacks used on the elderly in 2020 (Zulkipli et al., 2021). In the article titled "Synthesizing Cybersecurity Issues and Challenges For The Elderly", the authors proposed a framework to encourage cybersecurity awareness among the elderly. The factors included ensuring the awareness level among the elderly at the optimal level. Below is a depiction of their solution: it showcases what information the elderly should be aware of when it comes to staying safe on the internet.



Phishing is the act of using fraudulent emails to steal a user's sensitive information, such as credit cards, phone numbers, and addresses. Research studies have shown that there has been an increase in fraud scams among the elderly, specifically financial scams which are being labeled as "the crime of the 21st century". For instance, in 2019, the ICS received 68,013 complaints from victims who were over the age of 60 regarding personal losses of around $835 million (Alwanain, 2020). As a result, the elderly were the group placed at the top of the fraud list. Furthermore, in the following year, the FBI's Internet Crime Complaint Center reported that there were 791,790 complaints involving cyber-attacks including phishing, spoofing, extortion, and different types of web-based fraud.

One type of phishing scam that targets the elderly frequently is telemarketing scams. Anyone with a phone can receive these spam calls, but the elderly are more inclined to give them attention. Majority of people have been aware of these kinds of calls and block them or simply do not answer them. For instance, on iPhones, a call that may be considered spam usually comes up as "spam likely" underneath the number. In a telemarketing call, criminals may offer the elderly free prizes, inexpensive vacations, health care products, and low cost vitamins. These scams typically target women 60 years of age and older (Arfi & Agarwal, 2013).

From this amount, 28% of those complaints came from victims over the age of 60, which resulted in $1 billion in losses for senior citizens (Eimiller, 2021). However, many of the cases involving elderly fraud go unreported. Failure to report the problem means that law enforcement cannot stop or do anything about it. Also, it makes it hard to come up with problem-oriented efforts to proceed because there is a lack of information on the targets, perpetrators, and their methods (Arfi & Agarwal, 2013). Finally, it allows for these types of attacks to keep happening and for more people to fall victim to them.

There are a couple of reasons why the elderly are not quick to report that they were a victim of fraud. One is that they could feel embarrassed, guilty, or ashamed due to the scam. Second, the elderly could feel fearful that their families will lose trust in their ability to continue to manage their own finances (Aliperti, 2021). The FBI recommends taking appropriate measures to protect yourself against cyber-attacks. For instance, the one that I find to be the most important and relevant to the issue discussed in this paper is to be able to recognize scam attempts. I discussed this before and will continue to discuss the importance of it in this paper.

When it comes to the cost of healthcare expenses and investigative and legal costs for these crimes, it is estimated to be about a million dollars annually. Healthcare or health insurance fraud has been the number one if not close to it crime committed against the elderly. Some equipment manufacturers offer bogus products that are seen as “free” to people. Insurance companies are then charged for the products that were either not delivered or not needed by the elderly.

There are certain organizations that are frequently targeted by phishing attacks, which include: Microsoft, Netflix, PayPal, and Facebook. There have not been any concrete solutions for this issue, but there are things that organizations can do to protect their users by looking at

end user awareness. Anti-phishing training for end users should be included in any technical solution proposed, specifically with elderly users (Alwanain, 2020). Online services such as online banking and shopping are the biggest targets for phishing scams in older adults. This is because they lack security awareness.

To avoid fraud online while shopping, it is important to look at the website address and make sure it starts with “https” in which s stands for secure. Also, looking for the padlock icon on the search bar of the website ensures that the site uses encryption (CISA, 2012). On the other hand, when looking at medical advice it is important to look for sites ending in .edu or .gov to make sure that you are getting accurate up to date information. Even though there are technical approaches that can be taken to mitigate phishing attacks, they don’t solve the problem. It is more effective to improve the level of security awareness because that is what will help users be able to spot signs of phishing.

Furthermore, Aliperti included some tips in his article on what to do if you are targeted by a scammer. First tip is if at any point you feel as though you are being scammed, don’t share any personal information. Also, don’t allow anyone permission to access your accounts. Second, monitor your accounts and credit and credit for unusual activities, such as large deposits or loans you did not apply for. Third, contact law enforcement to file a report and notify any financial institution that is applicable to you.

Identity and money are two of the biggest reasons why the elderly are targeted by cyber criminals. Identity theft is one of the most popular cybercrimes out there and it is targeting the elderly more frequently. The difference between the elderly and other groups is that they can be targeted by people they know or professional criminals (Patriot Federal Credit Union, 2023). There are many ways that criminals try to gain the identity of the elderly. One is medical identity

theft that occurs when a person steals a victim's personally identifiable information (PII), such as their social security number. With this information in mind, they use it to bill either Medicaid or an insurance company for services the victim never received (Patriot Federal Credit Union, 2023). This could result in unpaid medical bills that mess up the victim's credit score and are at risk of receiving improper health care if the victim's medical records are mixed up with the perpetrator.

Next, is tax fraud which involves criminals trying to file a falsified tax return in the elderly's name to claim a tax refund. This complicates the senior citizen's taxes and delays any kind of refund that might have been owed. To protect seniors from becoming victims to identity theft, the Patriot Federal Credit Union recommends that they monitor their financial accounts, utilize strong complex passwords, file taxes early, monitor credit reports, watch out for strange communications, protect documents, and watch out for impersonator scams. To dive deeper into credit reports, there is a service called IdentityIQ that delivers credit reports to members directly to help ensure that a person's information is accurate. It notifies seniors via real time credit alerts of major changes on their credit report and any other suspicious activity. IdentityIQ flags signs of identity theft as soon as they pop up (Patriot Federal Credit Union, 2021).

Along with credit cards, it can let you know when your social security number, SSN, is used on an application for credit that is submitted in your name. Seniors are eligible to be compensated for up to $1 million in out of pocket expenses and losses if they experience identity theft, written by AIG. Seniors also get caught up in investment scams. Many of them live on a fixed income, so they may want to increase the value of their home and ensure they have sufficient funds to meet their basic needs. This is where investment scams come into play.

Cybercriminals convince the elderly to invest in things such as real estate, stocks, and bonds by promising unrealistically high rates in return. These investments consist of uninhabitable properties or fake shares in a nonexistent or unprofitable business (Arfi & Agarwal, 2013). The lack of computer and internet skills makes the elderly a prime target for various scams. Many of their computers are not secured including automatic updates, firewalls, secure passwords, etc. In addition, many of them are not tech savvy with navigating the internet and are not familiar with tricks scammers and some less reputable companies use (Arfi & Agarwal, 2013).

Romance scams are another big issue when it comes to the elderly. Nowadays, everyone is looking for a partner online instead of in person. In this situation, criminals pose as an interested romantic partner on a dating website which targets women or recently widowed (Aliperti, 2021). They initiate the relationship with the victim online and start to build their trust. As a result, cyber criminals convince the victim in providing personal or financial information about themselves. This is done in order to launder money unknowingly and to give money or buy expensive gifts (Zulkipli et al., 2021). Senior citizens are more inclined to be lonely and less knowledgeable making them one of the groups most vulnerable to this scam.

Many of the journal articles that have been discussed here have offered solutions to this problem which is the elderly's lack of cybersecurity awareness. They have offered solutions such as strong passwords, updating software, recognizing signs of scams, etc. It is important to be aware of the different types of cybercrime that are out there. Cybercrime is any crime that is committed using a computer. The types of cybercrime are child pornography, cyber laundering, cyber stalking, cyber terrorism, cyber theft, and spam. We talked about a few of these in previous sections, but I want to dive deeper into defining what they are.

Child pornography is the use of a computer to exploit underage children into creating material and then distributing it for profit. Cyber laundering is illegally transferring money electronically with the goal of concealing its source and destination. Cyber stalking is using any form of technology to create fear in a person by expressing threats or intimidating them. Cyber terrorism is the act of premeditated violence committed against civilians through the use of technology. It usually has a political agenda behind it. Cyber theft is the act of stealing information or committing criminal acts on the computer. Lastly, spam is unsolicited messages through email used to trick people into giving out sensitive information about themselves.

Outside of my major which is cybersecurity, the lack of awareness that the elderly have on cybersecurity risks relates to criminal justice. I have taken a couple of classes that tied cybersecurity with criminal justice. One of them being CRJS 310 which is Cyber Criminology Foundations. It discusses computer related crimes and how law enforcement officials investigate them. In this course, we discussed the motive behind a crime as well as how the criminal goes about it. Also, we talked about the different laws that are out there to govern cybercrime. One being the California Consumer Privacy Act which protects the privacy of the residents in the state of California.

Prior to working on getting my bachelor's degree at ODU, I received my Associate's degree in Health Science. With this in mind, I have studied the effects of age and what happens as people get older. The elderly can have a variety of different health problems that could make them unaware of the dangers of cybercrime. For instance, older people with dementia are going to have a hard time trying to remember complex passwords versus someone who doesn't (Zulkipli et al., 2021). As a result, they prefer using passwords that are easy and will come to mind quickly.

Also, older people usually use the same password on various applications so that they don't get confused on what password goes with which application. Many people, elderly included, will write their passwords down which is at risk of getting misplaced or put in the wrong hands. Elder abuse was a big topic not just in some of the health classes for my associate's degree, but also in today's world. Many people try to take advantage of the elderly. This could be physically, verbally, mentally or emotionally. One type that ties in with the problem discussed in this paper, is when family members specifically try to get their hands on their elderly family member's money.

Banks are able to spot this type of abuse especially if the family member is trying to speak for the elderly person and they are not giving any kind of consent to do so. Elderly people still have rights of their own and it will be looked at as suspicious if family members are trying to speak for them when they want money wired to another account. Unless they are incompetent and have signed legal documents saying they have given permission to so and so to speak on their behalf, the elderly person still has the final say so.

We will know that we are successful with our cybersecurity awareness course when we read the reviews from the elderly that leave testimonials about how our course changed their life and helped them to be more knowledgeable of their security on the internet. There will be an option once they complete the course for them to fill out a survey based on the overall structure of the lecture. This will help us learn and improve the course for those in the future. Also, we will know we are successful when we start seeing the progress of our course grow financially. Furthermore, the elderly who do decide to take our cybersecurity awareness course, will hopefully find the information in the lectures they choose to take are fundamental and will encourage their senior friends and family to take it as well.

Having a cybersecurity awareness program can help reduce human error. “According to MasterCard-+, 95% of data breaches are due to human error. However, many of these errors could be fixed simply by having a cybersecurity awareness mindset” (Fortra’s Terranova Security). The first step is to gather data on the elderly regarding statistics, vulnerabilities, typical target attacks, etc. This will be used to build the course and determine what information is included in each lecture. Once the course is up and running, my team and I will monitor the activity and how many people sign up. Then, we will come together to report any insights we as a team find. We will work on improving the course and update lectures as new information comes out.

To turn our cybersecurity awareness course into reality. We start by building a website to have a place to lay out the information. On the website, each topic is broken up into lectures. The lectures can be purchased individually for $9 each. That way the elderly can decide which courses they feel they need. Some may know more about cybersecurity than others, so giving them the option to choose which lectures they want to sign up for will help benefit those that need it.

There are 5 lectures offered on the website with topics including, introduction to cybersecurity, passwords and management, social engineering, antivirus, and a recap. In the introduction to cybersecurity lecture, the course will be aimed for the elderly looking to learn the basics of cybersecurity and introduces them to the relevance of cybersecurity for them. Some of the key takeaways from this lecture include defining cybersecurity, explaining why it is important, how it affects daily life, and where to start. The passwords and management lecture will help those who want to learn about the essentials of writing passwords and where to store

them. Some key points are what makes passwords weak, how to create strong passwords, and where to store them.

The social engineering lecture aims to discuss how scams work and indicators used to detect these attacks. It starts with defining social engineering. Then, it discusses the signs of social engineering attacks. Furthermore, it talks about how to deal with social engineering attacks. The antivirus lecture will give the elderly the option to learn about the purpose of using software to protect themselves from viruses and identify common options on the market. The course will discuss what an antivirus is, why it is a good tool for preventing viruses and malware, and what common applications provide antivirus solutions. Lastly, the recap lecture will summarize lessons learned in the previous classes about basic cybersecurity practices. It will provide some answers for the elderly who are still not sure about cybersecurity and if they are keeping themselves safe on the internet.

Now that we have the website up and running, we need to get the word out to the elderly. This can be done through advertisements. We can look to see how much it would cost to advertise our course on television. Also, we could look into getting a spot on the local news to see if they would promote it. We can go down to our local news station's headquarters and pitch our idea to them. Some older people are on social media, such as Facebook, so we could advertise it on there.

It is important that we use language that they can understand. Nowadays, young people have come up with terms that older people may not understand. When speaking about cybersecurity, we will use terms that they understand and won't be too complex. We will make sure that the course is fully explained including all that is encompassed in it and how it could benefit them. When advertising the course, it is important to make it personal. The advertisement

should speak directly to them. In this case, the goal is to get the elderly to participate and sign up for these lectures in the cybersecurity awareness course.

It is even helpful to earn their loyalty. Since it is a one-time fee, it makes the elderly see that we are a no string attached business. We just want the best for them while still making a reasonable profit for ourselves. Considering the cost that other companies could force the elderly to pay, I would say our lectures are reasonable. Furthermore, in the message we want to convey confidence to the elderly. We want them to feel like they are capable of learning, digesting, and then utilizing the material that they learn within this course. Our goal is not to point out them being old, but that they are capable of learning technology as well. Lastly, we want to implement a call to action that will convince them that they should consider taking our course.

Throughout the whole process of writing this paper, I have learned how to manage my time wisely. I have never written a paper this long before, so I was a little overwhelmed. However, I appreciate it being broken down into sections to make it easier on how much information to include. Also, I learned how to shift my mind into thinking like an entrepreneur and learning that even entrepreneurs need to work as a team. Throughout our time together working on this project, we have collaborated on ideas and have made compromises to meet each one of our goals.

Entrepreneurship is never something that I thought about pursuing, so this course definitely took me out of my comfort zone. This project helped me think about those who are victims of cyber-attacks and how they can be prevented. That is where the idea of focusing on a specific group came into play. We as a group decided to focus on how the elderly are at risk of cyber-attacks and what would be a good innovation to help with this problem. What I would

have done differently is sell our course to companies, so that their employees could become aware of these issues too.

It was easier to focus on one group, but if we had more time, it would have been interesting to see how we would promote our course to companies. We would definitely make it a subscription based service instead of letting them choose one lecture like the elderly. Companies would be able to use our course to educate their employees on the dangers of cyber-attacks and how to protect themselves and the company. I am not sure how much we would charge them for the subscription, but it would be on a monthly basis since we would be updating it as new information arises. The next step is to get this course out to the public so that as many of the elderly population can take advantage of this opportunity.

Overall, cybercrime is going to continue to be an issue as technology evolves. The best we can do is to provide resources to people so that they know the signs and dangers that go along with being online. The elderly are free to recommend this course to anyone that they feel may benefit from it as well, including young people. Young people can be naive and careless on the internet, especially on social media. Many do not take into consideration what they post on social media and how cyber criminals are behind the screens watching their every move. As we can see from what was discussed in this paper, no one is invincible to being a victim of a cyber-attack. Cyber criminals know exactly how to target their victims based on age, social status, job, etc.

References

Arfi, N. & Agarwal, S. (2013, July). Knowledge of Cybercrime among Elderly. https://www.researchgate.net/profile/Nabat-Arfi/publication/344905326_Knowledge_of_Cybercrime_among_Elderly/links/5f9864bf458515b7cfa3f172/Knowledge-of-Cybercrime-among-Elderly.pdf

Aliperti, M. (2021, June). How to Protect Seniors Against Cybercrimes and Scams. https://www.doit.nh.gov/sites/g/files/ehbemt506/files/inline-documents/sonh/nl2021-06-protecting-seniors.pdf

Alwanain, M. (2020, September). Phishing Awareness and Elderly Users in Social Media. https://www.researchgate.net/profile/Mohammed-Alwanain/publication/344134421_Phishing_Awareness_and_Elderly_Users_in_Social_Media/links/5fc562ffa6fdcce95268ebef/Phishing-Awareness-and-Elderly-Users-in-Social-Media.pdf

CISA. (2012, June). Cybersecurity And Older Americans. Pew Research Internet Study. https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Older%2520Americans.pdf

Eimiller, L. (2021, June 15). FBI Warns of Cyber Scammers Using Various Methods to Deceive and Defraud Elderly Victims for Financial Gain. https://www.fbi.gov/contact-us/field-offices/losangeles/news/press-releases/fbi-warns-of-cyber-scammers-using-various-methods-to-deceive-and-defraud-elderly-victims-for-financial-gain

Fortra's Terranova Security (n.d.). How To Measure The Success Of Your Security Awareness Program. https://terranovasecurity.com/measure-success-security-awareness-program/

Patriot Federal Credit Union. (2023, January 24). Elderly Americans Are Vulnerable To Identity Theft. https://www.patriotfcu.org/blog/elderly-americans-are-vulnerable-to-identity-theft/#:~:text=There%20are%20several%20reasons%20that,to%20hacks%20and%20data%20breaches.

Zulkipli et al. (2021). Synthesizing Cybersecurity Issues And Challenges For The Elderly. Turkish Journal of Computer and Mathematics Education. Vol 12, No. 5. Research Article.