Joel A. Addo

CPD494

Akeyla Porcher

Old Dominion UniversityEntrepreneurship Research Paper

Innovation Proposal:

Introduction:

The extensive usage of the internet in recent years has given many benefits to society, including enhanced connectedness, access to information, and online services. However, as the digital era has progressed, there has been an upsurge in cybercrime. Seniors are a susceptible demographic when it comes to online security threats. Seniors are frequently targeted by cybercriminals who exploit their vulnerabilities for financial gain due to their lack of experience with online security (Mendel, 2019). This entrepreneurship research paper aims to demonstrate an understanding of entrepreneurial thought by investigating a problem that necessitates an inventive solution. The issue addressed in this study is the increased susceptibility of seniors to hackers due to their lack of expertise in online security. Cybercriminals frequently target seniors, taking advantage of their trusting nature and lack of technological skills. As a result, elders may lose personal information, money, and even their identities.

The report suggests implementing a program that educates seniors about online security to solve this issue. The program aims to provide seniors with the skills and knowledge to identify and avoid cyber-attacks. The article will look at many facets of this program, such as its goals, target audience, curriculum, and implementation tactics. The study will be broken into many sections, beginning with an introduction emphasizing the significance of addressing the issue of senior susceptibility to cybercrime. The paper will then conduct a literature assessment of pertinent cybersecurity research, highlighting current trends, difficulties, and best practices in the sector. The following sections will examine the proposed program, its design, and its possible impact.

Description of the Problem and the Innovation:

Cybercrime has become an increasing global problem recently, particularly among seniors. Because of their lack of familiarity with the issue, seniors increasingly become victims of cyber-attacks as technology advances. Cybercriminals take advantage of this flaw by employing various methods to access personal information such as bank records, login credentials, and other sensitive data. This can result in significant financial losses, identity theft, and other types of cybercrime. To solve this issue, an innovation is presented that involves the creation of a program focused on educating elders about internet security.

A study of the scholarly literature on cybercrime and the need for educational programs to address this problem emphasizes the need to design successful educational programs for seniors. According to research, seniors are prone to a wide range of cyber dangers, such as phishing scams, identity theft, and other types of fraud (Kemp & Erades Pérez, 2023). Additionally, research shows that educational programs can reduce seniors' vulnerability to cyber-attacks while enhancing their confidence and familiarity with computers (Albladi & Weir, 2020). Nonetheless, the literature emphasizes the importance of such initiatives.

Cybercrime and Seniors:

Cybercrime targets people of all ages, but seniors are at a higher risk as the population ages. People aged 60 and up reported over 62,000 fraud complaints in 2018 as reported by the FBI's Internet Crime Complaint Center, (HG.org Legal Resources, 2022). These scams cost over $650 million in losses. The elderly are especially vulnerable because they may be unfamiliar with new technology and are less likely to be aware of prevalent frauds (HG.org Legal Resources, 2022). As a result, it is critical to educate older persons about cybercrime prevention.

It is critical to address the issue of government and commercial impersonators as part of senior cyber security awareness training. In order to collect monetary payments or personal information for identity theft, these scammers sometimes act as government officials or representatives from well-known corporations or charities. They may threaten targets with the loss of government benefits or the imposition of tax responsibility, among other things. According to the FTC, the Social Security Administration was the most prevalent target of official impersonation fraud between 2017 and 2021, with over 308,000 recorded complaints (The Federal Bureau of Investigation, 2019). As, a result, seniors must be aware of the dangers of these sorts of scams and take precautions to safeguard their personal information and financial assets.

To prevent fraudulent activities, seniors should also maintain track of their finances, regularly monitoring bank statements and credit card bills for any strange behavior. They should also be careful of signing anything without first having it reviewed by a trustworthy professional, such as a lawyer. Third, elders should be on the lookout for fraud involving lottery or sweepstakes awards. These offers may appear too good to be accurate and frequently aim to deceive the victim into disclosing personal information. We can assist in minimizing the occurrence of cybercrime against seniors by teaching older persons about these dangers and protective actions.

The Need for an Educational Program:

Academic literature emphasizes the necessity for a program to teach elders about online security. According to research, implementing educational programs to provide seniors with the essential information and abilities to defend themselves from cyber risks is recommended

(Nicholson et al., 2019). Seniors can benefit from educational programs that teach them to recognize and prevent possible scams and fraud and secure their sensitive information from cyber-attacks. Such initiatives can help boost elders' trust and familiarity with technology, allowing them to reap the numerous benefits of the digital era.

Using teaching materials and hands-on exercises, seniors can be trained to respond to and recover from cybersecurity incidents. Seniors can be educated about the necessity of having a strategy in place and what measures to follow regarding a cybersecurity issue. This may be accomplished through the use of films, webinars, and tutorials that guide users through the process of creating a response plan. Seniors might also be given situations to work through to practice recognizing and minimizing cyber dangers. One way to help seniors prepare for a cyberattack is to teach them about the need for a plan to restore lost data, programs, or services. They can be instructed on the tools and resources available for system restoration, such as backup and restore methods and system restore points. Again, instructional tools like movies and tutorials may be utilized to educate elders about the rehabilitation process.

Existing Educational Programs for Seniors:

Several established educational initiatives are aimed at educating the elderly about online security. Some of these programs are given by government entities, such as the FTC's Pass It On the program, which seeks to educate older people about fraud prevention. The campaign includes resources such as factsheets, bookmarks, films, and presentations that explain how scams work and what to do if they are targeted. The Pass It On initiative has grown in response to community partners' demands and changes in fraud tendencies.

The FTC works with various groups nationwide to deliver consumer education messages and inform the public about their activities. During the most recent reporting period, FTC personnel in Washington, DC, and eight regional offices engaged in over 210 outreach activities to safeguard people of various communities from fraud. One-third of these programs focused on older individuals and their caregivers, while others addressed financial resilience and recovery from the COVID-19 epidemic.

The FTC is committed to protecting older persons via legal enforcement, education, and outreach. In the subsequent years, the Commission's efforts to innovate and safeguard older individuals will be guided by research, experience, and stakeholder feedback. There are other services, such as the AARP's "Fraud Watch Network," are supplied by non-profit groups and private enterprises. The AARP Fraud Watch Network is a program that aims to educate and empower people, particularly seniors, to protect themselves from fraud and scams. The program provides various services, such as fraud alerts, instructional materials, and a helpline where people can report fraud and obtain help. To acquire and disseminate information about scams and fraud, the initiative collaborates with law enforcement agencies, government organizations, and other non-profits. They utilize this information to develop instructional materials and services to assist people in recognizing and avoiding fraud.

The AARP Fraud Monitoring Network provides various advantages to elderly individuals. First, it provides knowledge and tools to assist elders in recognizing and avoiding fraud. This is especially essential since fraudsters frequently target elders because of perceived access to financial resources. The AARP Fraud Watch Network protects seniors from financial abuse by arming them with knowledge. Second, the service includes a hotline to report fraud and obtain aid. This allows seniors to seek assistance and support if they have been victims of fraud.

In addition, the hotline can give information on reporting fraud to law enforcement or other authorities, which can assist in avoiding future victimization. Lastly, the AARP Fraud Watch Network provides a forum for seniors to share their stories and connect with others who have been scammed. This can help decrease the sense of isolation and guilt that many seniors may have after being defrauded, as well as create a supportive group that can assist them in recovering from the emotional and financial consequences of scams.

The Proposed Innovation:

The proposed innovation expands on current initiatives focused on teaching seniors about internet security, such as the AARP Fraud Watch Network and the Federal Trade Commission's "Pass it On." While these initiatives have successfully delivered education and training to elders, their funding and accessibility are limited. The proposed curriculum seeks to solve these constraints by providing a comprehensive and user-friendly approach to online security education accessible to seniors of all technical proficiency levels. This program will enable seniors to traverse the digital world confidently and securely by providing the information and skills to defend themselves from cyber-attacks. This initiative aims to improve seniors' well-being and quality of life by lowering their exposure to internet scams and fraud.

Integration with Classes Outside of Major:

The issue of internet security for seniors, and the innovative approach of developing a curriculum to teach them about it, is not restricted to any one major or field of study. It is a problem that affects all internet users, regardless of their background or industry (Mannheim et al., 2019). As a result, including this issue and innovation in classes outside of the major is critical in ensuring everyone knows internet security's importance. Seniors can gain insight into the psychological strategies employed by cybercriminals to deceive vulnerable populations, such as the elderly, and how to defend against them through raising public awareness and understanding of the issue in psychology courses. They can also learn about the financial effect of cybercrime and how to develop preventative steps to protect elders' assets. They can learn about the technical elements of online security and how to design safe systems in technology programs.

Seniors can realize the interdisciplinary nature of the issue and the significance of teamwork in tackling it by combining this challenge and innovation with classes outside of their major. Topics such as network security, virus prevention, and phishing scams are frequently taught in cybersecurity classes for IT students. These are areas of worry for seniors who may lack the technical skills to defend themselves from these hazards. Seniors, for example, may need to be made aware of the need to keep their software up to date to avoid vulnerabilities that fraudsters might exploit (Blackwood-Brown et al., 2019). They may also be unfamiliar with frequent phishing schemes and the significance of caution when clicking links or downloading documents. IT students may help build a curriculum that tackles these specific areas of concern for seniors and gives them the tools to defend themselves online using the information and skills obtained in a cybersecurity class.

The cybersecurity topics taught in IT programs are easily transferable to senior education. One idea taught in cybersecurity training, for example, is the significance of secure passwords. This is important for seniors since they may have never heard of this notion before and may be using weak or readily guessable passwords that are easily compromised (Blackwood-Brown et al., 2019). Another cybersecurity notion is two-factor authentication, which adds an extra layer of protection beyond a password. This is especially important for elders, who may be unfamiliar with this strategy and would benefit from knowing more about it.

Regarding the suggested innovation, a program to teach seniors about internet security and integration with classes outside of the major may entail collaborating with local senior centers or retirement homes to give cybersecurity instruction. IT students might visit the facilities and teach elders about password security, two-factor authentication, and other pertinent issues. The lessons would include interactive components such as seminars or hands-on activities which reinforces principles learned and ensures seniors are more prepared to defend themselves online.

Effectiveness of the Innovation:

Many measures will be used to judge whether the suggested innovation of a program to teach seniors about internet security is adequate. The number of seniors attending and finishing the program might be a metric. This will show the program's reach and efficacy in educating elders about internet security. Second, pre- and post-program questionnaires may be used to measure seniors' awareness of internet security before and after participating in the program. This will assist in establishing whether the training increased their understanding of internet security and whether it effectively met its objectives. Also, the number of reported internet security incidents involving seniors may be recorded before and after the program's adoption. A decrease in the number of reported instances would imply that the program was successful in lowering seniors' exposure to cybercrime. Finally, feedback from seniors who participated in the program may be gathered to establish their impression of the program's efficacy in enhancing their understanding of online security and if they feel more confident and secure when using the internet.

Implementation Plan:

The suggested innovation's implementation plan comprises numerous phases to ensure its success. The following actions are required to make the innovation a reality:

Introduction to cybersecurity:

The basic cybersecurity training will introduce seniors to typical online threats such as phishing schemes, malware, and ransomware, as well as practical methods to minimize these risks. This course will assist seniors in getting a fundamental understanding of cybersecurity, ensuring that they are aware of possible online threats.

Developing the Curriculum:

Experts in the industry will create a curriculum for the cybersecurity program. The curriculum will be structured to address all of the essential subjects about internet security that seniors should be aware of.

Creating Video Courses:

For the program, five video courses will be created. Each video lesson will cost $9, affordable for seniors on a fixed income. The innovation team realizes that cost is a crucial barrier to program participation for seniors on fixed or low income. To address this, my team intends to investigate alternative funding possibilities to give the program to seniors at a reduced or no cost. One strategy may be to seek grants or contributions from groups that support projects to improve senior digital literacy.

Moreover, my team may consider collaborating with local community organizations or government agencies to seek funds or other resources to make the program more accessible to seniors. My team is dedicated to ensuring that cost does not impede participation for the seniors most in need of this program. The following subjects will be covered in the courses:

Password management”

The password management course will teach seniors how to efficiently generate and maintain secure passwords. This is essential to internet security since weak passwords are readily hacked and exploited, resulting in unwanted access and data breaches.

Social engineering:

The social engineering training is designed to assist seniors in identifying and avoiding typical social engineering strategies employed by cybercriminals (Syed, 2021). Such approaches sometimes entail duping people into disclosing personal or sensitive information. This course will give seniors the knowledge and skills to detect and prevent such risks.

Anti-virus:

The anti-virus training will teach seniors the value of installing an anti-virus application on their devices and how to utilize it successfully. This course will teach seniors to safeguard their gadgets from malware and other internet risks, ensuring their devices are secure and safe.

Recap:

The review course will consolidate the essential themes addressed in the introductory courses and offer seniors a complete understanding of recommended practices for internet security. This course will help seniors put all they have learned into context and ensure they have a solid foundation for keeping safe online.

Turning Innovation into a Reality:

A complete implementation plan covering the program would be required to guarantee that the proposed innovation is thriving in teaching seniors about internet security. This covers the curriculum and video courses and embraces a diverse strategy to reach a larger audience and more effectively meet its objectives. As a result, the following tactics will be put in place:

The first step is to undertake comprehensive research and analysis of existing cybersecurity education programs for seniors. The unique program will be built with clear and simple instructions and guidelines that will allow seniors to successfully learn and execute internet security best practices. Additionally, the study should demonstrate that many seniors need to know the most recent cybersecurity risks and how to defend themselves (Blackwood-Brown et al., 2019). As a result, the novel curriculum may also address the most recent cybersecurity dangers and offer seniors up-to-date knowledge and skills for online safety. Therefore, a substantial study is essential in developing an effective and unique cybersecurity education program for seniors.

The success of the proposed invention depends on the design and development of a comprehensive and user-friendly cybersecurity education program for seniors. Seniors have distinct needs and concerns regarding internet security, and the program should be designed to suit them (Blackwood-Brown et al., 2019). Phishing and other social engineering assaults, for example, are frequent strategies used to target elders. These assaults are particularly effective because they exploit elders' trust and lack of expertise with contemporary technologies (Syed, 2021). As a result, the software should provide detailed instructions and guidance for identifying and avoiding such assaults and other online security dangers. It should also be user-friendly and straightforward, keeping in mind that some seniors may need more experience with technology or be less tech-savvy than younger generations. As a result, establishing and implementing a cybersecurity education program tailored to elders' unique requirements is crucial to guaranteeing its efficacy in assisting seniors in protecting themselves from cyber-attacks. It necessitates careful consideration of their specific circumstances, intending to make the application as accessible and user-friendly as possible.

Before starting the program, it is critical to do a pilot test to evaluate its efficacy and make any required changes. A pilot test is an important stage in ensuring the efficacy and viability of the senior cybersecurity education program. Before introducing the program to a broader audience, the creators may receive valuable input and discover areas for improvement by testing it with a small sample of seniors. The pilot test input will help the developers to tweak and enhance the application better to fit the needs and preferences of the target population. This will boost the program's chances of success, eventually assisting seniors in protecting themselves from cyber risks. Furthermore, the pilot test might assist in uncovering any technological flaws or challenges that must be solved before the program is made available to a broader audience.

After completing the program, it should be released and marketed through various channels, including social media, virtual communities, senior centers, and other relevant institutions. The cybersecurity education curriculum's effectiveness for seniors depends on its launch and promotion. The program may only reach its target audience if it is properly promoted. Increasing the program's visibility and accessibility through numerous channels will make it simpler for seniors to access the program and learn about internet security. Social media channels may be leveraged to reach a larger audience, and senior centers and related organizations can assist in promoting the program to seniors who may need access to internet resources. To guarantee optimum impact, the program's promotion plan should be adapted to the requirements and tastes of the target audience.

It is critical to continuously assess the program's efficacy and make required modifications based on input from users and stakeholders. It is critical to continuously assess the program's efficacy to verify that it is accomplishing its goals and objectives. Assessing the program allows you to see where you are falling short and where you might improve. This input can come from users and stakeholders such as community partners, educators, and subject matter experts. Based on the input collected, essential adjustments to the program may be made to ensure that it remains effective in assisting seniors in protecting themselves from cyber risks. The program may remain relevant and up to date with the current advancements in cybersecurity by making continual modifications.

To market the program and reach a larger audience, seeking partnerships and collaboration with relevant organizations such as the AARP Fraud Watch Network is critical. These collaborations will aid in raising awareness of the program and its advantages. Ultimately, securing funds for the program's implementation and sustainability through partnerships, grants, or other financial sources is vital. It will be challenging to sustain the program and continue to equip seniors with the essential information and resources to defend themselves from cyber-attacks without financing.

Summary of What was Learned From the Project:

The initiative sought to address the cyber dangers that elders suffer due to their lack of knowledge of internet security. The suggested invention was creating a program to teach elders about online security. The researchers analyzed academic literature and surveyed it to determine the knowledge gap among seniors. The implementation strategy called for creating a five-course video series covering various internet security topics, each costing $9. The experiment determined the effectiveness of educating elders about internet security to reduce cyber dangers. Difficulties in obtaining a representative sample of seniors and a lack of interest in some locations were faced. These obstacles were solved through collaborations with senior centers and providing incentives for involvement. More engagement and hands-on training might have helped to improve the project.

The project's plans include collaborating with other senior centers and expanding the service to reach a larger audience. Senior centers, cybersecurity specialists, and funding agencies should all be key stakeholders and collaborators. The program's performance may be measured in the future by measuring the number of participants, changes in behavior, and feedback. Expanding the program is possible by including more interaction and hands-on training and forming collaborations with more organizations. The suggested idea provides a realistic answer to the problem of cyber risks that the elderly encounter. It is impossible to overstate the significance of cybersecurity education for elders. The project's influence has been shown, and it has the potential to be successful in reducing cyber dangers among seniors in the future.

References:

Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1), 1-19. https://doi.org/10.1186/s42400-020-00047-5

Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2019). Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. *Journal of Computer Information Systems*, 1–12. https://doi.org/10.1080/08874417.2019.1579076

Kemp, S., & Erades Pérez, N. (2023). Consumer Fraud against Older Adults in Digital Society: Examining Victimization and Its Impact. *International Journal of Environmental Research and Public Health*, *20*(7), 5404. https://doi.org/10.3390/ijerph20075404

Mannheim, I., Schwartz, E., Xi, W., Buttigieg, S. C., McDonnell-Naughton, M., Wouters, E. J., & Van Zaalen, Y. (2019). Inclusion of older adults in the research and design of digital technology. *International journal of environmental research and public health*, *16*(19), 3718. https://doi.org/10.3390/ijerph16193718

Mendel, T. (2019, September). Social help: developing methods to support older adults in mobile privacy and security. In *Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers* (pp. 383-387). https://doi.org/10.1145/3341162.3349311

Nicholson, J., Coventry, L., & Briggs, P. (2019, May). " If It's Important It Will Be A Headline" Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-11). https://doi.org/10.1145/3290605.3300579

Syed, A. M. (2021). Social engineering: Concepts, Techniques and Security Countermeasures. *arXiv preprint arXiv:2107.14082*. https://doi.org/10.48550/arXiv.2107.14082

The Federal Bureau of Investigation . (2019). *FBI Releases the Internet Crime Complaint Center 2018 Internet Crime Report — FBI*. Www.fbi.gov. https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2018-internet-crime-report#:~:text=The%20FBI