Name: Joel Addo
Course: CPD494
Date: 03/03/22

Innovation Proposal

My team and l propose introducing a program that will teach seniors about online security, as they are a common target of cybercriminals because of their lack of familiarity with the subject. There is mounting evidence that cyber assaults against the elderly are becoming more common as more seniors engage in internet activities. Our solution is to produce videos teaching senior citizens about cybersecurity. These classes will be dynamic and entertaining, covering subjects including secure surfing, password management, and internet privacy. Our program's effectiveness will be determined by several factors, such as the number of people who complete the training, the quality of the participant reviews, and the frequency with which cyberattacks on the elderly are reported to decrease. For seniors, we will provide a one-time payment option, while businesses can pay on a subscription basis.

According to Zwilling et al. (2020), the elderly are especially susceptible to cyberattacks owing to their lack of education and awareness regarding internet safety. Because of this lack of information, they are vulnerable to various internet scams and frauds, resulting in monetary losses, identity theft, and other types of harm. According to a National Cybersecurity Alliance (2022) survey, just 26% of seniors think they are extremely competent in defending themselves online, and only 17% utilize two-factor authentication to safeguard their accounts. Additionally, many older people may be unaware of numerous cybersecurity concerns, such as phishing schemes, malware, and ransomware assaults.

This lack of understanding and information among the elderly is a critical issue that must be addressed. Cybercrime may have catastrophic repercussions for anybody, but it is typically more severe for the elderly, who may lack the finances or support networks to recover from the damage inflicted by such assaults (Karagiannopoulos et al., 2021). My team and l hope to solve this issue and safeguard this vulnerable demographic from the dangers of cybercrime by offering a complete internet safety education course designed exclusively for seniors.

Cyber-attacks are growing more common and sophisticated in today's increasingly digital environment, and the elderly are typically the most vulnerable. Americans over 60 are the most common victims of scams and fraud, with losses totaling billions yearly (National Cybersecurity Alliance, 2022). Many older adults are unaware of internet safety and the most recent cybersecurity dangers and recommended practices. They may also be more trusting, making them more vulnerable to fraud and phishing efforts. The COVID-19 epidemic has forced more individuals to work, shop, and socialize online, increasing the likelihood of cybercrime activity

(Eian et al., 2020). This lack of internet safety knowledge among the elderly is a big issue that must be addressed. My hope to empower older people with the information and skills they need to defend themselves from cyber risks and fraud by giving an online safety education course geared exclusively to them. Online identity protection, password management, secure online buying, detecting and avoiding fraud and phishing efforts, and best practices for accessing social media will all be covered in our course. By offering this training, we will help older adults use the internet securely and confidently, reducing their exposure to cybercrime.

Solution

We recommend making videos teaching senior citizens about cybersecurity to combat the growing threat online criminals pose. The course material will focus on providing seniors with actionable information and skills that can be immediately used when navigating the internet to mitigate the most prevalent cybersecurity risks they may encounter. We will go over how to recognize and avoid phishing scams, how to make and use strong and unique passwords, how to use two-factor authentication to secure accounts, how to keep personal information safe on the internet, how to recognize and avoid malware and ransomware attacks, and how to use social media and online dating sites securely. The course will be presented in an approachable manner, with engaging, interactive modules and relevant real-world case studies.

Delivery Method

Participants can study quickly and from any location since the complete course will be available online utilizing a cutting-edge learning management system. The platform will be easily navigable, providing users with learning-oriented multimedia content and interactive exercises. To ensure participants have all they need to participate effectively in the course, our staff will offer them technical help and coaching.

Marketing and Promotion

To reach the demographic of senior citizens, our stuff plan to employ several different promotional and advertising tactics. Partnerships with senior centers and retirement homes, as well as social media advertising and email marketing, will all be part of this strategy. My team will also market the course to applicable businesses and organizations by drawing on their current network of connections in the cybersecurity field.

Barriers

The reluctance to change is one of the key obstacles we expect to face. Because of their possible discomfort with new technologies, many seniors may be reluctant to enroll in an online course (Bianchi, 2021). On top of that, participants will have varied levels of technical knowledge; thus, the course material may need to be modified accordingly. Furthermore, extra challenges may be associated with distributing and supporting the course.

Assessment

Our program's effectiveness will be assessed based on different factors, such as the number of people who complete the training, the quality of the participant reviews, and the frequency with which cyberattacks on the elderly are reported to decrease. The number of businesses that sign up to take a course is another metric we will watch closely to gauge interest and product viability. We will utilize these measurements to fine-tune the show for our intended audience.

Pricing

Our price structure will include a one-time payment option for seniors and a business subscription plan. As we have not finished developing and testing the prototype to ensure it fulfills our intended market's demands, we have not set a price for it yet. We will check the

market to see what price will get us the best results while yet being reasonable. However, until further review, the following is how the price structure is shaping out to look.
Individuals:

- One-time purchase option for access to the entire course: $49.99

Companies:

- Subscription model based on the number of participants:
    - 1 to 50 participants: $249/month
    - 51-100 participants: $399/month
    - 101-250 participants: $699/month
    - 251+ participants: custom pricing

We consider these prices fair and market competitive while allowing us to meet our expenses and make a profit. However, we reserve the right to adjust the price depending on data collected from our target market.

My team wants to introduce a program to teach seniors how to be safe online in response to the rising number of hacks aimed at this demographic. The course material will provide students with foundational cybersecurity knowledge and skills that can be immediately used in their day-to-day online lives, including recognizing, and avoiding phishing scams, developing and using strong and unique passwords, and safeguarding sensitive data. Participants can study quickly and from any location because an intuitive learning management system will present the full course online. The business owners plan to promote and advertise their product to the elderly using many channels, including social media advertising, email campaigns, and collaborations with senior centers and retirement homes.

The course's success will be gauged by the reactions of the students and the results of the tests they take, as well as through collaborations with providers of cybersecurity software and other educational establishments. My team will update the course depending on student input and developments in the cybersecurity industry. They hope to provide other courses and certificates in cybersecurity and related industries and expand the course to new locations and populations. We want our participants to be able to use the internet securely and confidently by equipping them with the information and skills necessary to defend themselves against cyberattacks.

References

Bianchi, C. (2021). Exploring how internet services can enhance elderly well-being. *Journal of Services Marketing*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/jsm-05-2020-0177

Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Z, F. (2020). Cyber Attacks in the Era of COVID-19 and Possible Solution Domains. *Www.preprints.org*. https://doi.org/10.20944/preprints202009.0630.v1

Karagiannopoulos, Dr. V., Kirby, Dr. A., Oftadeh-Moghadam, S., & Sugiura, Dr. L. (2021). Cybercrime awareness and victimization in individuals over 60 years: A Portsmouth case study. *Computer Law & Security Review*, *43*, 105615. https://doi.org/10.1016/j.clsr.2021.105615

National Cybersecurity Alliance. (2022, July 5). *Multi-Factor Authentication*. National Cybersecurity Alliance; National Cybersecurity Alliance. https://staysafeonline.org/resources/multi-factor-authentication/

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 1–16. https://doi.org/10.1080/08874417.2020.1712269