Cybersecurity Awareness Program for Everyone (C.A.P.E)

Non-Profit Entrepreneurship Academic Paper

Khaliyd Fuller

Old Dominion University

CPD 494: Entrepreneurship in Professional Studies

Professor Porcher

March 20, 2023

Introduction

The Problem with Cybersecurity Awareness

In our group, we have decided to address the problem of cyber awareness for our cybersecurity entrepreneurship innovation project. Since we live in a digital age where nearly everyone is carrying a computing device of some kind, whether it be a laptop, tablet, or smartphone at all times – cybersecurity awareness is becoming increasingly important. Nowadays even very young children are playing with computer tablets, which means that we are beginning to develop our digital footprints at a very young age. Each of the variety of different interconnected devices that we use exposes us to a different attack vector for cybercriminals to target to exploit. This is why it is important for individuals to learn about cybersecurity awareness and for businesses to invest into strengthening their cybersecurity departments to protect their sensitive information from being exposed to unauthorized third parties.

Due to the variety of different cyber attacks that exist today, poor cybersecurity awareness becomes a major threat for both individuals and businesses. *Authorized computer users are the biggest threat to information security, but are also the biggest defense – if they have a good sense of cybersecurity awareness.* Young adults and seniors in particular may have trouble understanding the importance of protecting their data and the danger of sharing personal information online. While young adults who spend much of their time online using social media may be at risk of cyber-related issues such as cyberbullying, online harassment, and identity theft from sharing too much personal information online, seniors may be more susceptible to falling victim to cybercrimes such as scams, phishing, and malware due to unfamiliarity with deceptive online practices. Both demographics can benefit from specific targeted cybersecurity awareness training in order to keep their personal information safe when they are browsing online. This is exactly what our non-profit organization seeks to do with our cybersecurity awareness training program.

The Solution is Cybersecurity Awareness Training

In order to address the problems surrounding cybersecurity awareness, we have decided to create a non-profit cybersecurity awareness training program in order to spread awareness for individuals as well as businesses. Our cybersecurity training will seek to provide targeted training for specific demographics whether they be young adults, seniors, business employees, or students. We expect that many cybersecurity insurance companies will seek to adopt our training program as a co-requisite that their business customers must enroll into in order for them to receive coverage. The website will feature a variety of content including, but not limited to:

1. A feed of relevant articles and blog posts written by cybersecurity professionals relating to current cybersecurity issues.
2. The learning program itself will include "games" that are intended to make the learning experience more interactive in order to increase the retention of information. The site will host a leaderboard, so that learners can compare their scores and compete to have the highest "cybersecurity awareness score."
3. The program will include short-form videos to make learning more digestible, rather than having learners read long articles. This is also intended to improve learning retention.

Our non-profit organization will seek to raise funds in order to provide computing devices to underprivileged communities that enroll in our cybersecurity awareness training program, as well as offering scholarships to learners who maintain a high "cybersecurity awareness score" and are seeking to pursue higher education or immediate employment into a cyber-related field. We will also seek to connect learners with cyber-related opportunities to gain experience and build their resumes. This can include both opportunities to work with non-profit organizations to create innovative cyber-related projects, as well as paid employment with companies that utilize our cybersecurity awareness program. By engaging with the communities in the Hampton Roads area, we hope to improve the level of cybersecurity awareness and encourage the next generation to adopt good cybersecurity practices. We believe that these efforts will lead to increased interest in the field of cybersecurity and result in more qualified cybersecurity professionals.

Barriers to Entry

Barriers that we expect to challenge include gaining credibility and funding for our mission. Some individuals and businesses may not understand the immediate importance of investing into cybersecurity training, but we seek to address this by providing credible information from experienced, certified cybersecurity professionals and reputable sources. By building off of the work laid out by HRCyber, we intend to strengthen the understanding of cybersecurity in the Hampton Roads area. HRCyber was established after Old Dominion University was awarded a grant of ~$250,000 by the U.S. Department of Commerce to stimulate cybersecurity education and workforce development under the National Initiative for Cybersecurity Education (NICE) objectives from October 2016 to April 2018. As a program that also seeks to be closely associated with ODU, we hope to integrate various events that are sponsored by the university in order to connect learners with community outreach opportunities, such as ODU's GenCyber Summer Camp program to learn about various cybersecurity topics and to get hands-on experience with cybersecurity technologies. By building a close relationship with the university, we hope to gain credibility within the community that we serve.

We will realistically gain buy-in by showcasing testimonials that were provided by early adopters of our training program. We intend to receive funding for our innovation by pitching our idea to investors and earn revenue by offering our cybersecurity awareness training program to individuals, businesses, government agencies, and schools. This revenue will be used to maintain and expand our operations, provide computing equipment to underprivileged communities, and sponsor learners who are seeking higher education or immediate employment into a cyber-related field.

Literature Review

Defining Cybersecurity Awareness

In order to adequately discuss the pervasive issue of cybersecurity awareness, it is essential to first define what cybersecurity awareness is. According to AbdRahim, Hamid, Kiah, Shamshirband, and Furnell (2015), cybersecurity awareness has been defined as “a methodology to educate internet users to be sensitive to the various cyber threats and the vulnerability of computers and data to these threats,” with Shaw, Chen, Harris, and Huang (2009) similarly defining cybersecurity as “the degree of users’ understanding about the importance of information security and their responsibilities to exercise sufficient levels of information control to protect the organization’s data and networks” (as cited in Quayyum, Cruzes, Jaccheri, 2021, p. 2) Using these definitions, we can understand that the objective of cybersecurity awareness is to educate computer users about the threats that they face online in order to better protect sensitive data from preventable cyber attacks where the cause was lack of cybersecurity awareness. Computer users should be knowledgeable about various cybersecurity topics in order to make informed decisions when ensuring the security of their devices including firewall configuration, antivirus software, security patches and updates, email phishing and spam filters, and malware. Businesses and individuals should follow cybersecurity best practices and stay informed about new and emerging threats in order to be proactive in implementing security measures to prevent or mitigate damages that can be caused by potential cyberattacks.

Failures of Previous Cybersecurity Awareness Campaigns

In order to create an effective cybersecurity awareness program, it is essential to research previous cyber awareness campaigns to learn more about not only what they did right, but where they went wrong. By learning from the failures of prior awareness efforts, we will be able to more effectively address the needs of the communities we are seeking to serve. The most important aspect of discussion will not be how to effectively communicate the importance of securing our devices, but to demonstrate how devices can be secured in a way that is easy for the average person to understand. The awareness program will not be effective if the learner is not motivated to apply what they learn in their everyday lives, so it is important to find real-world examples of why it is important to follow cybersecurity best practices.

One of the most common failures of cybersecurity awareness campaigns is the lack of engagement with the target audience, which results in low conversion rates and little impact. Cybersecurity awareness campaigns that utilize passive learning methods such as listening to lectures or reading textbooks are often ineffective when compared to more active learning methods such as hands-on exercises that require real-time participation from the learner. It is best to provide a variety of learning methods to the learner (readings, videos, exercises, quizzes, etc.) in order to diversify offerings for a diverse demographic of learners.

Another failure is the over-reliance on the fear factor. Cybersecurity awareness is not just a problem that requires technical solutions, it also requires an understanding of human behavior. The best way to mitigate or prevent cyberattacks is to avoid cognitive biases and social engineering, that cause computer users to act against their own self-interest and compromise their computer systems as a result. While fear and anxiety can be powerful psychological motivators for behavioral change, focusing on fear too heavily can be counterproductive and leave the audience feeling overwhelmed and helpless. According to Ahluwalia (2000), “fear invocations have often proven insufficient to change behavior,” and Write (1994) suggests that "invoking fear is not an effective tactic, since it could scare people who cannot afford to take risks" (as cited in Maria Bada, Angela M. Sasse, Jason R.C. Nurse, 2015, p. 7-9)

The lack of personalization towards a diverse target audience is also a major point of failure for cybersecurity awareness campaigns. When trying to educate the public and address real-world problems, you will often find that one size does not fit all. Cybersecurity awareness campaigns that fail to take into account the unique needs and concerns of their demographically diverse target audiences are often ineffective. For example, cybersecurity awareness campaigns that are focused on children may require a different approach and focus, as opposed to a campaign that is focused on seniors. In order to promote behavioral change amongst diverse target audiences it is important to effectively communicate and tailor messaging in a way that is easy to understand. Cybersecurity training programs should tailor the experience towards the learner's specific needs and allow for personalization of the experience for their ideal method of learning. By empowering the learner with a personalized learning experience and the ability to track their progress, this will allow them to modify the experience in order to fit their needs. Modern cybersecurity awareness programs should seek to integrate emerging technologies, such as artificial intelligence, in order to enhance the effectiveness of the learning experience. Tools powered by artificial intelligence will allow learners to more easily tune the learning experience to meet their needs and receive easy to understand feedback to their questions.

Determining Demographic Vulnerability

With the increasing availability of and reliance upon internet connected devices, it is imperative that we focus our efforts on providing digestible information to those who are the most vulnerable to cyber threats online. For demographics such as young children who lack the life experience to adequately assess online threats, as well as seniors who are generally unfamiliar with emerging technologies and can more easily be manipulated— cybersecurity awareness can be of major importance to ensuring their privacy and security are maintained while browsing online. With respect to children who use the internet on a daily basis, Tsurtsus, Tsapatsoulis, Stamatelatos, Papadamou, and Sirivianos (2016) "conducted a literature review and identified several risks that children are exposed to which they classified into five categories of content risks, contact risks, children targeted as consumers, economic risks, and online privacy risks. They also noted that children faced risks associated with illegal and harmful content online such as sexual exploitation, inappropriate content such as pornography, and harmful advice regarding alcohol and drugs, suicide, and psychological and nutritional disorders" (as cited in Quayyum, Cruzes, Jaccheri, 2021, p. 3). This suggests that malleable children are particularly susceptible to manipulation and being negatively influenced by harmful, age-inappropriate content online such as drugs, sex, gambling, and targeted advertisements that can lead to serious problems such as addiction later in life. According to Blackwood-Brown, C. (2018), there has been a rapid increase of internet usage amongst senior citizens, one of the most vulnerable demographics, who are prone to finance-related cyberattacks due to their limited cybersecurity awareness and limited technological skills. While senior citizens have much more life experience when compared to children and are less likely to be negatively influenced by information found online— their unfamiliarity with technology and tactics used by cybercriminals can leave them vulnerable to manipulation and exploitation for financial gain. In order to develop an effective cybersecurity awareness program, it will be necessary to tailor the content to the specific needs of each demographic and the cyber threats they are particularly susceptible to.

Benefits of Gamification in Cybersecurity Education

According to research studies like Alotaibi et al. (2016), gamification has proven to be effective in many research areas and can help create cybersecurity awareness. Gamification is defined as the process of using game mechanics in the process of education in order to better engage learners in the subject matter and increase retention of the information learned. The increased level of engagement can provide a fun learning experience by incorporating game elements such as challenges, rewards, and competition. These elements can motivate learners to be active participants and focus on learning objectives and active learning has been proven to be much more effective when compared to passive learning methods. According to Patten (2015), “common cybersecurity awareness training programs utilize methods such as e-learnings or regular presentations which can be considered intimidating, time-consuming, and non-inviting,” whereas Kassicieh et al., (2015), notes that “gamification is often related to promising results regarding attention, feedback, and motivation” (as cited in Rieff, 2018, p. 4) . Through the use of game-based activities, learners can apply what they have learned in practical and interactive ways, which can allow them to retain the information better. Gamification can also increase retention rates by creating a memorable and fun learning experience that stimulates multiple of the learner’s senses and emotions. An additional benefit of gamification in education is the encouragement of tracking learning progress and completing achievements. According to Blohm (2013), “the continuous documentation of one’s own behavior visualizes progress, facilitates the derivation of achievable personal goals, and offers immediate feedback so that users perceive feelings of high individual performance” (as cited in Junibel Cruz, Sanchari Das, 2020, p. 2). Gamification also normalizes the idea of failing, learning from mistakes, and trying again to be successful. Receiving instant feedback on success and failures, as well as rewarding learners who are successful will encourage them to continue learning and improving.

Interdisciplinary Problem-Solving

The problem we are seeking to address is interdisciplinary in nature and can be related to coursework assigned outside of the major's requirements. While naturally the field of cybersecurity will include topics such as technology, business, and law, there is also the need to address topics such as education and psychology. Understanding human behavior as it relates to psychology will be a major factor in aiding learners' ability to integrate cybersecurity best practices into their everyday lives in order to mitigate the potential for cyber-related incidents to occur, as well as understanding the behaviors of cybercriminals and the tactics that they employ.

Cybercriminals often use social engineering, a form of psychological manipulation, to deceive computer users into revealing sensitive information or performing actions that put their systems at risk. By understanding the psychology behind cyber attacks such as phishing, our program will be able to aid learners in identifying and reporting these cyber attacks. The study of psychology can also be useful for addressing cognitive biases that can lead users into making poor decisions with regard to the security of their computer systems. These biases are systematic errors in a user's thinking that can cause them to act against their own self-interest. Two examples of this would be the illusion of control, where a user may overestimate their ability to prevent cyber-related incidents, and optimism bias, where a user may underestimate the likelihood of themselves being the target of a cyberattack. By increasing learners' awareness of these cognitive biases, we can aid them in making more rational decisions when they are dealing with various online communications that may potentially compromise their system's security.

Naturally, fear and anxiety can often be powerful motivators for behavioral change and by emphasizing the risks and consequences of falling victim to cyber attacks can be an effective method of motivating both individuals as well as organizations to take steps to protect their data.

By providing real anecdotal experiences from individuals and organizations who have taken massive losses by falling victim to cyberattacks, we hope to encourage learners to become motivated to protect themselves for their own self-interest. Ultimately, fear and anxiety alone cannot ensure that learners will consistently take the necessary precautions to protect themselves from cyber threats, but it is an effective tool in ensuring that they *want* to learn how to protect themselves all on their own, for their own sakes. In order to encourage learners to practice these cybersecurity best practice behaviors consistently, it is important that learners make these practices become habitual and routine. Habits and routines are powerful psychological factors that can influence behavior without an individual needing to be consciously aware of potential risks. Our program will seek to encourage learners to integrate cybersecurity best practices into their daily routines such as checking for software updates to patch exploits and vulnerabilities, as well as using a unique, strong password for each online account. Ultimately, the purpose of our cybersecurity awareness program is to educate learners about mitigating risks, so the program should be designed with learning and training in mind. We seek to aid learners by providing access to real-world examples and accurate information regarding the importance of cybersecurity, using interactive and engaging training methods, and encouraging practicing best practices on a frequent basis to help develop the skills necessary to protect themselves against cyber threats.

Determining Success

There are several methods that we intended to employ in order to determine whether or not our cybersecurity awareness program has been successful. For example, by utilizing metrics and key performance indicators (KPIs), such as our website traffic, conversion rates, retention rates, and social media engagement, we can track the effectiveness of our cybersecurity awareness program. We can also measure the success of our cybersecurity awareness training program through surveys and feedback by gauging the learners' understanding of various cyber-related topics when they start the learning program and providing various assessments throughout the program in order to collect data on how effective the program is at improving the cybersecurity awareness of learners. This will allow us to evaluate the effectiveness of the training program and make any necessary adjustments for improvement. Another measure of success we intend to use is the number and severity of cyber-related incident reports amongst the adopters of our training program where the cause of the cyber incident was lack of adequate cybersecurity awareness (phishing, weak password, no two-factor authentication, out-of-date software, etc.) If the number of incidents or the severity of incidents decreases, it may indicate that our cybersecurity program has been effective. Other ways to determine if our venture has been successful are successful partnerships and collaborations with other organizations in the cybersecurity community and having a positive return on investment (ROI), such that the benefits of our cybersecurity awareness program outweigh the costs of running the program.

Goals and Requirements

Funding

In order to make our innovation a reality, it is necessary to plan carefully in order to fulfill the requirements necessary to operate successfully. Our group will require funding in order to successfully kickstart our non-profit organization to begin development of training programs and educational initiatives. We will need to develop a fundraising plan alongside reasonable short-term and long-term goals. We intend to seek funding by applying for government grants and investments from local businesses in the Hampton Roads area. If we can reach our funding goals, we'll seek to establish our non-profit organization as a legal entity. As a non-profit we will need to obtain the necessary licenses and permits to operate our program. Once we ensure that we are compliant with all laws and regulations, then we will seek to assemble a team of employees and volunteers to help develop and maintain our cybersecurity awareness program.

Team Building

We would like to have our team consist primarily of university students who are majoring in cyber-related fields. This will allow us to employ and aid in the development of the next generation of cybersecurity professionals, as well as to save in employment costs. The team will need to consist of junior web and app developers, as well as consulting assistants who work with the community to educate about the importance of good cybersecurity practices in order to protect their data. The team will also require working facilities with technology infrastructure in order to develop, maintain, and host the cybersecurity awareness program for learners to access remotely. We will seek to work with technology partners and vendors to ensure the security and reliability of our technology infrastructure. We may seek to integrate our program closely within universities, in order to benefit from pre-existing infrastructure to reduce costs and become more integrated within the community. By establishing partnerships and collaborations with other organizations within the cybersecurity space we can increase the reach and impact of our training program. This will likely include working with schools, universities, non-profit organizations, local businesses, and government agencies.

Community Outreach and Impact

As part of our mission to educate the community about cybersecurity, we would like to host various community events that allow for the community to gain hands-on experience with various emerging technologies in order to encourage learning and promote growth in the field of cybersecurity. We will seek to work with schools, universities, businesses, and government agencies alongside other organizations in order to gauge the community's understanding of cybersecurity related topics in order to adapt our awareness training to the community's current needs. We will try to convert many community members into active users of our awareness training program, so that we can better track how effective the program is at building good cybersecurity habits. We would also like to provide incentives for learners who continue to advance through our cybersecurity awareness program by providing free technology to learners who achieve a high 'cyber awareness score.' The training program will allow learners to track their own learning progress and their own 'cyber awareness score' relative to other community members. This will allow the learner to take their education into their own hands and incentivize them to improve their understanding of cybersecurity related topics. We will need to develop the proper metrics and KPIs to track the progress of our program, and regularly evaluate and adjust our approach based on the results.

Reflecting on Cybersecurity Awareness & Non-Profits

Throughout the project we have learned a lot about the amount of time, effort, and funding that goes into kickstarting a non-profit organization and the research into prior attempts at improving cybersecurity awareness has changed my initial perspective. Our research into creating a non-profit organization to promote cybersecurity awareness has influenced my understanding of the challenges associated with starting and running a non-profit with respect to acquiring funding and maintaining operations while not being motivated by profit. I feel as though non-profit organizers must carefully manage the funding they acquire as they are not in the business of making money per say. It is important to set reasonable expectations about what opportunities the non-profit organization can afford and look for opportunities to save by cooperating with other organizations.

My initial perceptions of cybersecurity awareness before beginning my research suggested that seniors would be a primary beneficiary of cybersecurity awareness education due to lack of familiarity with emerging technologies, however, as my research continued, I came to the conclusion that this was not necessarily true. I believe that everyone can benefit greatly from cybersecurity awareness programming and that even those who are familiar with technology may be just as susceptible to falling victim to cybercrimes. I think the aspect of the psychological factors involved with victimization of cybercrimes is something that the general public should be more aware of. I believe that even the most technologically literate individuals can fall prey to psychological manipulation and inadvertently compromise their computer systems. I believe that cybercrimes will only continue to grow in number and hold much more severe consequences in terms of privacy and finances as technology advances, and I believe that we should all continue to educate ourselves in order to keep our data secure.

References

Farzana Quayyum, Daniela S. Cruzes, Letizia Jaccheri. “Cybersecurity awareness for children: A systematic literature review” *International Journal of Child-Computer Interaction, Volume 30, 2021*

https://www.sciencedirect.com/science/article/pii/S2212868921000581

Rieff, I. (2018) “Systematically Applying Gamification to Cyber Security Awareness Trainings” *A framework and case study approach*

https://repository.tudelft.nl/islandora/object/uuid:bf832ca0-91d9-4be1-9a25-fe284c23d115/datastream/OBJ1/

Maria Bada, Angela M. Sasse, Jason R.C. Nurse, “Cyber Security Awareness: Why do they fail to change behavior?” *International Conference on Cyber Security for Sustainable Society, 2015*

https://arxiv.org/abs/1901.02672

Blackwood-Brown, C. (2018). *An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills* (Order No. 10842968). Available from ProQuest Dissertations & Theses Global; SciTech Premium Collection. (2088133071).

http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/empirical-assessment-senior-citizens/docview/2088133071/se-2

Junibel Cruz, Sanchari Das, “SoK: A Proposal for Incorporating Accessible Gamified Cybersecurity Awareness Training Informed by a Systematic Literature Review” *In Proceedings of the Workshop on Usable Security and Privacy (USEC) 2022 in Conjunction with Network and Distributed Systems Security (NDSS) Symposium 2022.*

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4054885