Cybersecurity Awareness Training Website Proposal

Khaliyd Fuller

Old Dominion University

CPD 494: Entrepreneurship in Professional Studies

Professor Porcher

February 28, 2023

In my 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 the elderly 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, the elderly 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.

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, the elderly, 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.

Some 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.

We can measure the success of our cybersecurity awareness training program 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. Another measure of success we intend to use is the reduction of cyber-related incidents 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.)