Cybersecurity Awareness Training Program

Innovation

Problem	The problem we have decided to address is cybersecurity awareness. In the digital age that we live in, people begin to create a digital footprint at increasingly earlier ages. These days nearly everyone is carrying either a laptop or smartphone around, and even children are playing with tablet computers. We each have a variety of interconnected devices (IoT) which expose us to a variety of different attack vectors for cybercriminals to target. This is why it is important to invest into proper cybersecurity awareness training for not only businesses, but for individuals as well.
Context	Poor cybersecurity awareness is a major problem for both individuals and businesses today due to the variety of different cyber attacks that exist today. Young adults and the elderly in particular may have trouble understanding the importance of protecting their data and the dangers of sharing personal information online. Where young adults who spend much of their time online using social media may be at risk of cyberbullying, online harassment, and identity theft from oversharing personal information, the elderly may be more susceptible to falling victim to scams, phishing, and malware. Both demographics can benefit from specific cybersecurity awareness training in order to keep their personal information safe when they are browsing online.
Solution	In order to address the problems surrounding cyber awareness we have decided to **create a non-profit cybersecurity awareness program** to spread awareness of cyber-related issues and good cybersecurity practices for both individuals as well as business employees. Cyber insurance companies will be able to use our cybersecurity awareness training program as a co-requisite in order for business customers to receive coverage.
Features 1. Articles 2. Games 3. Videos	1. The website will serve learners a feed of relevant **articles** relating to cyber issues and will feature blog posts written by cybersecurity professionals. 2. The learning program will include "**games**" to make learning more interactive to increase retention and include a scoreboard, so learners can compete to have the highest cyber awareness score. 3. The program will include short-form **videos** to make learning more digestible, rather than having learners read long articles in order to increase retention.

Community 1. Providing 2. Connecting	Our non-profit will seek to raise funds in order to **provide** computing devices to underprivileged communities that enroll in our cyber awareness training program, as well as scholarships for learners who have a high cyber awareness score and are seeking 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 a resume. 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.
Barriers 1. Credibility 2. Funding	Some barriers that we expect to challenge include **credibility** and **funding**. Some individuals and businesses may not understand the importance of investing into cybersecurity training, but we seek to address this by providing credible information from experienced, certified cybersecurity experts and reputable sources. We will realistically gain buy-in by showcasing testimonials from early adopters. We intend to receive funding for our innovation by pitching our idea to investors and to earn revenue by offering our cybersecurity awareness training program to individuals, businesses, governments, 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.
Assessment	We can measure the success of our cybersecurity training education program by gauging the learners' understanding of various cyber-related topics when they start the learning program and providing assessments throughout the program to collect data on how effective the program is at improving the cyber awareness of learners. We can also measure success in a reduction of cyber-related incidents among adopters of our cybersecurity awareness training program where the cause of the cyber incident was lack of adequate cybersecurity awareness (phishing, weak password, no 2FA, out-of-date software, etc.)