Mackenzie Coleman

Entrepreneurship Group Proposal

WCS 494 Entrepreneurship

Professor Porcher

September 30, 2022

There is no question that over the last several decades, the world has taken off in the new age of technology. The development of technology has led to a new world of understanding and learning about the world around us and set new possibilities for the world. However, with this new, amazing addition to life, there are complications that follow. We see technology being used by billions of people every single day; this raises one of our most pressing questions of this time. How do we protect our information on this technology? These concerns of information protection and technology security prompted the development of Cybersecurity.

In the 21st century, cybersecurity has become one of the most demanding jobs in the world. This is due to the high volume of technology use, and over-time, people have discovered ways to use technology for malicious intentions. Cyber-attacks are now one of the most common forms of crime today. From ransomware attacks to phishing emails, cyber-attacks happen all day, every day, and some people go on and have no idea their information is at risk. The problem that will be addressed in this proposal is regarding cybersecurity education and what has and is currently being done to promote cybersecurity education for kids and teenagers. We want to create an official Cybersecurity Curriculum for middle schools and high schools that will start teaching the importance of cybersecurity along with how to use technology safely. While creating this curriculum, we will also be researching what schools in the Hampton Roads area of Virginia are currently doing to spread cybersecurity education and awareness.

As the world has adapted to this new age, people all around the world, continue to expand the capabilities of technology. While this is amazing for so many known reasons, one of the biggest concerns brought up is kids with access to this technology. Recently, more noticeably over the last 10 years, kids have been raised with a piece of technology in their hands from the time they learned to walk. For example, you see parents using tablets or phones to occupy their children while at a busy public location, you see kids watching a screen while in the car or playing with their friends while watching YouTube videos. Technology and the Internet surround us. To give a good perspective, according to an article published by npr.org, 53 percent of children in the United States have their own smartphone by 11 years old (Kamenetz, 2019). As a society, we have experience problems with cybersecurity knowledge and awareness well before COVID-19. However, since COVID-19 cyberattacks have noticeably increased exponentially, primarily because of the increase and demand in internet access and technology while under quarantine. With the increase in device use, some people lacked the necessary knowledge of their device and how to keep their information safe. For this reason, more people became susceptible to cyber-attacks. COVID-19 also led to online leaning. This meant all students from all grades were moved to online classrooms. This is another way to show that technology is now more present than ever. Even though students are back in classrooms, the technology has not gone away. With the implementation of this cybersecurity curriculum, schools will have the information and tools to teach their students, as well as their faculty, the important information they need to know regarding the technology they use daily. Because of children and teens having, some even needing, constant access to technology, it is important to ensure they are educated on the proper way to use these devices and being as safe as possible.

Now that we have addressed the primary problem of the lack of cybersecurity knowledge around the world, what can we do about it? Our goal is to design a structured curriculum focused on cybersecurity education and safe device practices. This curriculum would focus on the basics of device protection, effective password creation techniques, different methods of cyber-attacks for example, phishing emails. In middle schools, the problems would be more simplified for the age group to understand at their level. At the end of the day, most people no matter the age

group, are using similar, if not the same, devices and applications. For instance, I am 22 years old and a middle schooler in my neighborhood, age 13, requested to follow me on Instagram. After declining it and thinking quickly to myself, "A 13-year-old doesn't need to follow me." I then thought deeper and realized, "Wow. A 13-year-old uses the same technology as me, including the social media platform, and most likely does not know half of the information I do," regarding how to keep herself and her information safe. However, I do not actually know if she had knowledge of cybersecurity, but reality is, she probably does not and neither do most kids.

The main objective for our cybersecurity curriculum is to give students the opportunity to learn vital information that will help them in their future. While creating this new cybersecurity curriculum, I feel that we will encounter a few barriers, however, no barrier that we cannot overcome. One of the main challenges I feel we will face is gaining interest from students and kids. The word itself, cybersecurity, could have the potential to steer the students away if they do not know what it means. As students get further into their education, starting in middle school. In the U.S. kids have their core classes or required classes, and they now have the options to choose their elective classes like art, music, humanities, and more. Our curriculum could have the potential to eventually expand into several classes focused on different technological fields for students before they continue into the real world where they will, more than likely, have to use a form of technology every day. However, I feel that we will have to deliver the information in a creative, interactive way to keep students engaged and interested, while also retaining the important information. One of the ways we thought to keep students engaged is to add summary questions at the end of each chapter for teachers to assess what information has been retained by students and what needs more attention. Another potential barrier we might encounter in this process is resistance to integration of the curriculum in schools. This resistance could come from school faculty, thinking students do not need this information yet. There also could be some resistance from parents who might not have knowledge of cybersecurity themselves and might not think it is important for their child to take the classes. This barrier is expected, not only because people might be hesitant about the information, but also because change can be difficult for some people. Some might see this additional curriculum as an unnecessary change to the education field, however, the research and findings will eventually show how this curriculum has the potential to benefit so many students and people in general.

In my opinion, I feel that we will know if this cybersecurity curriculum is successful through several ways. If we see schools, specifically in Hampton Roads, using this curriculum to educate their students on cybersecurity practices and safe device use, this would be one of the major successes of this innovation. If we see schools in our area implement a version of our curriculum to further the education of their students on the importance of cybersecurity, then we would be achieving one of our biggest goals of this new curriculum. Another way we will see success, that we would see happen over a much longer period, is eventually seeing the number of cyber-attack victims decrease in the Hampton Roads area and as well as around the country. Educating students, prior to leaving high school, on the importance of cybersecurity on the devices they are utilizing daily, should be a conversation in every school that has students using technology. Another form of success will be seeing students, and maybe some teachers, applying what they have learned during the course into their daily life. Knowing that the information is being used, while also benefitting the students and teachers that are learning it would be a huge form of success. One of the main reasons for cyber-attacks are because of human error. This is due to any different factors but most of the issues come down to the lack of knowledge on cybersecurity and device protection. This has the potential to change if we adjust the way we are

educating and preparing young adults for the real world by implementing cybersecurity curriculums.

Resource:

Kamenetz, A. (2019, October 31). *It's a smartphone life: More than half of U.S. children now have one*. NPR. Retrieved September 29, 2022, from https://www.npr.org/2019/10/31/774838891/its-a-smartphone-life-more-than-half-of-u-s-children-now-have-one