Sarah Noble
CYSE 494
Professor Porcher

Project Proposal

What is the problem you are addressing? (problem)

With the creation of new technologies and the internet, younger generations are the first to have been completely surrounded and dependent on the internet and electronic devices since birth. Younger people are becoming increasingly reliant on technology as their technological devices are integrated into their everyday lives. Too often, young users are not fully aware of the risks that are associated with using these devices and the harm they are capable of causing. Moreover, cyber hacking techniques are becoming more complex and sophisticated over time. Internet use is not limited to adults and children should receive the proper education about cybersecurity practices as well. Consequently, it is imperative that users are taught good cyber-hygiene practices at a young age to better equip them with the knowledge and skills necessary to avoid becoming a victim to these cyber attacks.

From educational purposes to entertainment, children spend a significant amount of time on the internet. Given their age and lack of knowledge of cybersecurity, it is not surprising that children and young people are often exposed to and targeted by these attacks. Additionally, parents are not always aware of what their child is doing online and whether or not they are engaging in risky internet behaviors. Raising cybersecurity awareness by implementing educational programs can help prevent the spread of cyber attacks while also informing users about the risks they are constantly being exposed to. As a result, internet users' understanding and knowledge of cybersecurity will be strengthened and hopefully, more users will be able to utilize these learned cyber practices in order to properly protect themselves from potential cyber threats.

How do you know it's a problem? (context)

In this day and age, children themselves are frequent users of the internet and may even have their own personal devices; however, they are not given the proper education to fully gain an understanding of the possible dangers. They are becoming increasingly targeted by cyber criminals due to their minimal knowledge about cybersecurity. Although cybersecurity may seem like a complex topic to younger people, they are basic lessons that can be taught to children to ensure their safety over the internet. Examples of this include learning how to keep their personal information private and avoiding speaking to strangers over the internet. Simple lessons such as these should be integrated in the classrooms and home of children in order to familiarize themselves with safe cybersecurity practices.

Just as sex education, driver's education, and D.A.R.E. programs are included in school's curriculums, cybersecurity educational programs should also be developed and taught. As of now, cybersecurity is not taught in schools. Certain topics pertaining to cybersecurity may be integrated into broader curriculums; however, it is not taught as its own course. Furthermore, topics such as encryption or phishing attacks are not touched on at all. For these reasons, cybersecurity education is rarely included in elementary, middle, or even high school's curriculums. Another issue is that many educators feel themselves are not equipped or

knowledgeable enough to teach such topics to their students. This raises other concerns as the best method of preventing these attacks is through education.

What are you going to do about the problem? (solution)

A possible solution for the lack of cybersecurity education in schools is creating an educational program for students attending middle and high schools. Starting small, my group and I decided to focus on schools located in the Hampton Roads area. Although we are only covering grades 6-12, a simpler version of this can also be created to accommodate children grades k-5. While we are still putting our ideas into place, some things that we believe can be included in this program include modules covering different topics, review quizzes, participation activities, simulations, etc. In addition to this, if enough students begin to take an interest in this program, we could also consider creating AP courses for students in high school regarding cybersecurity. This could further assist them in planning for their future as they are applying to colleges and considering what to major in.

While creating and developing our program, our group could also reach out to some schools in the Hampton Roads area. In doing so, we will be able to see what schools in our area are doing to educate students on safe cybersecurity practices right now. If they currently are not touching on any cybersecurity topics, we could figure out what is preventing them from doing so and if they would be willing to incorporate a program in their school.

What barriers do you expect to confront? (barriers)

With the development of any kind of product, it is expected that barriers will be encountered. The biggest barrier this product will face is the resistance of integrating our curriculum into schools. As stated previously, many schools may be hesitant to implement cybersecurity programs because educators may not feel equipped or knowledgeable enough to do so. While we do not have the power or resources to do so, basic concepts could also be introduced to teachers as a first step. Training more high-quality teachers may also be essential to make a direct impact on students' learning. In addition to this, schools may not want to add on to the existing curriculum or student's current workload. They may want to continue incorporating certain cybersecurity topics into an already existing and broader curriculum; however, these topics do not go in depth enough to facilitate learning. Lastly, access to cybersecurity education may also be inconsistent across communities and different educational settings; moreover, schools may not have the proper resources to implement a cybersecurity curriculum in their school.

How will you know if you are successful? (assessment)

While implementing the entirety of our curriculum is ideal, we will know we are successful even if schools in the Hampton Roads area are at least willing to consider making our program available to its students. We realize that implementing a new educational program into schools may be time consuming and difficult. However, if schools do not want to implement our entire program, we will feel successful just knowing that topics are being introduced to kids under broader curriculums. By educating and making users aware of the potential risks they encounter everyday, we can teach them safe cyber practices that will encourage them to be more cautious of what they do on the internet. As long as users are being introduced to such topics at an earlier age, this can make a huge difference in the overall rate of cyber attacks targeting children and young people.

We will also know if we are successful if more students are able to learn about and take an interest in cybersecurity as a profession. In my personal experience, I did not hear of cybersecurity until I reached sophomore year of university. The field of cyber security is one of the fastest growing careers and younger generations are already tech-savvy. If we could get more students interested in cybersecurity throughout their school years, we will feel more confident in knowing that students will be better equipped to properly protect themselves from cyber threats and may even contribute to the cyber workforce.