Rebecca Badu

Oct 11, 2023

Proposal

- **What is the problem you are addressing? (problem)**

  The problem I'm addressing is lack of cybersecurity education for school age children because the majority of the younger generation using the internet remains oblivious to the online risks. It is true that many younger people who have grown up with ready access to the internet may not completely comprehend the dangers involved with online activity. This is due to a number of factors: Younger generations are frequently referred to as "digital natives," meaning they grew up with technology and are presumed to comprehend it intuitively. But this presumption might be false. Although they could be skilled with technology, that doesn't necessarily mean they are aware of the nuances of internet security. Limited Education: Comprehensive digital literacy and cybersecurity are still not taught in many educational systems. Although advanced subjects like identifying phishing attempts, creating strong passwords, and protecting personal information may not be effectively covered, basic internet safety is taught.

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

  The assumption "The majority of the younger generation using the internet remains oblivious to the online risks in the cybersecurity world" is based on widely observed patterns and trends in online activity. It's crucial to emphasize that this assertion is not supported by a particular empirical study or statistic, but rather reflects a common worry among professionals and educators in the field of cybersecurity. The cybersecurity knowledge gap among school-age children has been extensively studied in a number of studies, surveys, and observations. Here are some indicators that this is a problem: Numerous academic studies have been carried out to evaluate students' knowledge of cybersecurity and digital literacy. Surveys, interviews, and assessments are frequently used in these researches to gauge participants' online knowledge and behavior. Educational Initiatives: The significance of digital literacy and cybersecurity education has been acknowledged by numerous educational institutions and organizations all over the world. To close this knowledge gap and improve pupils' comprehension of online risks, programs have been put in place. Reporting of occurrences: Numerous reports have been made of instances of cyberbullying, online harassment, and other occurrences

involving school-aged children. These occurrences show a lack of understanding about safe internet behavior. Parental Concerns: Parents and other adults frequently express worries about the safety of their kids online and about the dangers they may not be aware of. Increased efforts are being made to inform parents and kids about cybersecurity as a result of this worry.

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

  Myself and the team will develop a public education strategy aimed at imparting essential knowledge to elementary students and beyond. It takes a multidimensional plan that encompasses schools, parents, and the community to develop a public education strategy for teaching fundamental cybersecurity skills to elementary students and beyond. Here is a thorough plan of action: Education Integration - Integrate age-appropriate cybersecurity modules into current disciplines like computer science, science, and digital literacy. This is known as integrating cybersecurity into the curriculum. Make learning about cybersecurity engaging and enjoyable by using interactive tools, games, and simulations. Implement a progressive curriculum that builds upon fundamental ideas as students advance through the grades. Resources and Training for Teachers: Conduct training sessions and workshops for teachers to give them the tools and knowledge they need to properly teach cybersecurity. Give teachers access to a collection of age-appropriate cybersecurity resources, activities, and lesson plans. Parental Participation: Organize parent workshops and seminars to inform parents on the value of cybersecurity and how they can help their kids establish safe internet habits. Collaboration between parents and teachers will help to establish a consistent approach to teaching cybersecurity. Useful Application: Implement practical activities and projects that let students apply cybersecurity principles to actual situations. Create simulated cyber incidents to instruct students on how to react and reduce potential dangers. By implementing this strategy, schools, parents, and the community can work together to equip students with the knowledge and skills needed to navigate the digital world safely and responsibly.

- What barriers do you expect to confront? (barriers)

  There could be a number of obstacles in the way of creating a public education strategy for cybersecurity education in elementary schools and beyond. These might consist of fewer resources: Budgetary Limitations: It can be extremely difficult to find financing for teacher training, curriculum development, and resource acquisition. Lack of Access to Technology: Not all schools or students may have access to the equipment required for a cybersecurity education to be successful. Training and experience of teachers: Lack of

Cybersecurity experience: It can be challenging to locate skilled educators who are knowledgeable in cybersecurity, especially in areas where such experience is limited. Time Restrictions: Teachers could already be working a lot, so finding time for additional training may be difficult. Design of a Curriculum for Each Age: Complexity balancing: Creating a curriculum that is thorough and age-appropriate can be a tricky balancing act. Parental Participation: Diverging Levels of Parental Involvement: Different parents may be more involved in and supportive of cybersecurity education than others, which could result in discrepancies in at-home reinforcement. Collaboration between educational institutions, governments, cybersecurity professionals, parents, and communities will be necessary to overcome these obstacles. Overcoming these obstacles will need flexibility, adaptability, and a long-term commitment to cybersecurity education.

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

A combination of qualitative and quantitative metrics is needed to assess the performance of a public education strategy for cybersecurity education in elementary schools and beyond. Here are a few success indicators: Student Competency: Assessment Results: Ongoing evaluations should reveal a progression in students' comprehension and application of cybersecurity concepts. Teacher Competency: Evaluations and Recommendations Teachers should receive regular feedback from students as well as ratings depending on how successfully they teach cybersecurity. Parental Involvement: Workshop Participation: increased involvement and attendance at cybersecurity workshops for parents. Accusation Reports: Fewer reports of online events involving students, such as cyberbullying or falling for online frauds, have been made. Technical competence: Improved general digital literacy and safe online habits among pupils. Increased tech literacy. Comments from interested parties: Surveys and Focus Groups: To get feedback on how well the program is working, surveys and focus groups will be held with students, instructors, parents, and community members. Success stories and case studies: Stories of students effectively using their cybersecurity skills to protect themselves online provide as anecdotal evidence.