Equitable Access to Cybersecurity Education: A Case Study of Underserved Middle School Students

Madison Thomas
mthoma27@ncsu.edu
North Carolina State University
Raleigh, NC, USA

Erynn Elmore
eelmore2@ncsu.edu
North Carolina State University
Raleigh, NC, USA

Brenda Chavez
bcchavez@ncsu.edu
North Carolina State University
Raleigh, NC, USA

Ronaisha Ruth
rruth@umd.edu
University of Maryland, College Park
College Park, MD, USA

Charlotte Avery
cjavery@umd.edu
University of Maryland, College Park
College Park, MD, USA

Michel Cukier
mcukier@umd.edu
University of Maryland, College Park
College Park, MD, USA

Veronica Cateté
vmcatete@ncsu.edu
North Carolina State University
Raleigh, NC, USA

ABSTRACT

Existing research has primarily delved into the realm of computer science outreach aimed at K-12 students, with a focus on both informal and non-formal approaches. However, a noticeable research gap exists when it comes to cybersecurity outreach tailored specifically for underserved secondary school students. This article addresses this void by presenting an iterative pilot of a cybersecurity curriculum. This innovative curriculum integrates a one-week summer camp and a series of 1.5-hour workshops designed to provide students with a comprehensive understanding of cybersecurity.

The overarching goal of this approach is to foster wider participation in the field of computing, particularly in the realm of cybersecurity. This research aims to spark interest among students who may currently face limited access to computing resources. The cybersecurity lessons featured in this curriculum adhere to the standards set by Cyber.org, an organization supported by the Cybersecurity and Infrastructure Agency (CISA). Key topics covered include networking, the confidentiality, integrity, and availability (CIA) triad, and operating system security.

This paper not only outlines the process of creating and implementing these cybersecurity lessons but also emphasizes the iterative refinement process they underwent. The discussion primarily revolves around the valuable insights gained from implementing this curriculum at two prominent public universities in the eastern United States. By bridging the research gap and focusing on practical applications, this initiative contributes significantly to the broader discourse on cybersecurity education for underserved secondary school students.

ITiCSE 2024, July 8–10, 2024, Milan, Italy

ACM ISBN 979-8-4007-0600-4/24/07
https://doi.org/10.1145/3649217.3653581

CCS CONCEPTS

• **Social and professional topics** → **Computing education**; **Informal education**; **K-12 education**.

KEYWORDS

summer camp, secondary students, cybersecurity education, outreach

ACM Reference Format:
Madison Thomas, Erynn Elmore, Brenda Chavez, Ronaisha Ruth, Charlotte Avery, Michel Cukier, and Veronica Cateté. 2024. Equitable Access to Cybersecurity Education: A Case Study of Underserved Middle School Students. In *Proceedings of the 2024 Innovation and Technology in Computer Science Education V. 1 (ITiCSE 2024), July 8–10, 2024, Milan, Italy.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3649217.3653581

1 INTRODUCTION

Computer science (CS) education has seen a large increase in practitioners and students who are eager to incorporate computer science into the curriculum as a full course or integrated curriculum [17] [16] [18] [7], however, less of a push for incorporating cybersecurity into schools than there is for computer science, or even artificial intelligence [2]. Recent research investigated incorporating computer science or ICT topics at either the primary [34] [29] or upper secondary level [19], but few at the lower secondary school level pertaining to cybersecurity [13, 25].

With a projected 32% growth in cybersecurity jobs, there is a need for cybersecurity education at the K-12 level. As well, 2/3 of the world's population ages 15-24 used the internet in 2017 and most children use more than one device when connected to the internet [1]. Unfortunately, cybersecurity has yet to be mandated as a computer science topic in primary and secondary education not only in the United States [8], but also globally [21]. A 2019 report found that only 57% of surveyed instructors intended to implement a cybersecurity section in their K-12 curriculum [12].

Despite the lack of K-12 cybersecurity requirements across the globe, a growing population of students have an interest in cybersecurity, with those needs not being met in formal education settings. In informal educational settings, limited research on cybersecurity education that teaches a wide range of topics for students to determine if they have an interest in pursuing additional cybersecurity and computer science courses at the secondary level [31] [6] [5]. Both informal and formal education settings lack of accessible cybersecurity education for middle school students that is an all encompassing, full curriculum. In attempts to address this gap, we developed a two phase cybersecurity outreach program, named SecureIT, for early age, secondary school students. Phase 1 encompasses a one week summer camp developed from previous curriculum and Phase 2 includes a multi-session weekend outreach event expanding on curriculum supported by Cyber.org standards [9].

The contributions of this research are:

- Develop reuseable curriculum that can be used at multiple research sites to teach students introductory cybersecurity concepts
- Understand how the participants interaction with the curriculum contributes to their perceived learning, interest, and confidence in cybersecurity
- Determine what, if any, correlation exists between participants' level of enjoyment in cybersecurity activities correlate with their intent to pursue further studies or a career in cybersecurity
- Observe participants change in attitudes towards the program, SecureIT, before and after the program
- Discover what, if any, significant difference in participants' attitudes towards the program, SecureIT, before, during, and after engaging with the curriculum?
  - If a significant difference exists, determine what factors contribute to the difference

We follow this introduction with background on previous work investigating cybersecurity education and design based research. We then share the phases of our work creating and refining the curriculum in sections 3.1 and 3.3. Finally, we share lessons learned and implications for practice of cybersecurity education.

2 BACKGROUND

Previous research has investigated children's understanding of the internet [15] [11], networking [27], computer viruses [31], social networking [6], and informatics [5], but not additional cybersecurity topics like operating systems, the CIA Triad, and hacking [9]. This is critical gap as there is a 32% increase in cybersecurity jobs and students need to begin building a strong cybersecurity education foundation.

Prior work examined children's understanding of cyber-safety, particularly online safety, with a focus on primary school aged (K-5) students [10]. While online safety is important, the goal of this research is to focus on a broad cybersecurity education that includes the prior topics discussed as singular lessons. Research by Riel and Romeike found that students did not have a clear understanding of computer networks and how communication happens on those networks [27]. This was another motivating factor to increase students' understanding of networking and cybersecurity.

Students' understanding of computer viruses was the focus of the study by Tsarva et al in 2020. The research found that the topic of computer viruses and how they work can be taught to children as young as 3rd and 4th grade [31]. Folk models of malware have also been investigated by Wash [33] and found that users erroneously think that certain operating systems or devices are immune to viruses. While the respondents in Wash's work are older than this work's population, students in secondary schools still have the ability to develop folk models, so it is important to keep this in mind that students may come into learning about cybersecurity and other topics with erroneous preconceptions.

When conducting this research, it was imperative that the topics taught were relatable to the students and built off of their existing knowledge around computing, while also being scalable for students who had completed prior computing or cybersecurity courses offered in the community [32]. When piloting the curricular programs, it was critical that the research was implemented with an iterative design process and improved and tailored as the project continued. Thus, this research follows a Design-Based Research (DBR) approach [4]. The DBR approach allows a team to conduct research in authentic educational settings, focusing on the design of the intervention, using mixed methods research in an iterative fashion while focusing on multiple stakeholders and a persistent problem. This is an appropriate research model since University of Maryland, College Park and North Carolina State University are in two different geographic areas with a similar research agenda of improving access to and engagement with cybersecurity education. The persistent problem we encountered was the lack of cybersecurity education and a cohesive curriculum for early secondary school students.

3 IMPLEMENTATION CONTEXT AND CURRICULUM DESIGN

Our project is broken down into two preliminary phases; Phase 1, the first summer camp pilot, and Phase 2, weekend workshops taking place during the academic year. The goal of these two phases is to determine what is more impactful when teaching cybersecurity; summer camps or weekend workshops. Both summer camps and workshops took place at two large public universities in the eastern United States.

University of Maryland, College Park (UMCP) is a leading public institution in a suburban area with a majority African American population. UMCP offers 8 STEM-related summer programs and 12 computer science after school programs for secondary-aged students. Of the 8 middle-grade summer programs, the camp implemented in Phase 1 was the only camp that geared towards cybersecurity. There was also one residential cybersecurity camp designed for upper-secondary aged students.

North Carolina State University (NCSU) is a large public university adjacent to a bustling downtown city center. NCSU offers general engineering and computer science-themed day camps across the K-12 grade band in addition to residential camps for 11th and 12th-grade students. NCSU had not hosted a cybersecurity-specific computer science camp prior to Phase 1. However, exploratory middle-grade computer science camps have been hosted for over a decade with varying themes of games and block-based coding.

The camps were instructed by local university students majoring in computing related field. Instructors taught in teams of 3-4 during the camp, rotating roles between lead instructor and teaching assistant for each activity. The program coordinator was also present and hands-on for both camps. The goal of the camp was for students interested in the growing field of cybersecurity to learn to think like cybersecurity engineers and employ design thinking to protect the devices they interact with daily (smart technologies, wearables, internet sites). Each day included a warm-up activity, an introductory tutorial, plugged and unplugged cybersecurity activities, and then a challenge activity in the afternoon for students to extend upon the lessons learned earlier in the day or week.

3.1 Phase 1

3.1.1 Recruitment. To assist in recruitment, UMCP used its strategic partnership with the Center for Inclusion and Diversity (Center), located on their campus. The Center has a history of implementing summer programs and school-year outreach for students from historically underrepresented groups in computing. In addition to building relationships with families, the Center has established partnerships with local schools, campus departments, neighboring universities, and organizations such as Girl Scouts of the USA, the National Center for Women and Information Technology, and Computer Science Teachers Association, and has leveraged these relationships to support recruitment efforts. The Center also manages a website, newsletter, and several social media platforms to communicate upcoming events and programs.

At NCSU, a partnership was formed with the outreach branch of the college of engineering that has provided over 20 years of infrastructure such as recruiting, meals, and logistics for K-12 summer programs. The partners use a camp management software to maintain a mailing list for advertisements and potential participants. They also utilize national connections and local area school networks to communicate messages to parents and teachers. Similar to UMCP, a program website and newsletter was also used to share upcoming programs and events.

A breakdown of Phase 1 participant demographics is provided in Tables 1 and 2. The mean age of students at both campuses was 12, with a breakdown by location provided in figure 1. Overall, each camp hosted a diverse participant group including at least 33% girls, and 33% Black, Hispanic, or Native American students.

Table 1: Demographic Characteristics of UMCP Phase 1 Participants

Total	Gender			Race/Ethnicity				
	Female	Male	Other	Black	Asian	Hispanic	White	Unknown
N=21	8	12	1	7	6	3	2	2

Table 2: Demographic Characteristics of NCSU Phase 1 Participants

Total	Gender		Race/Ethnicity					
	Female	Male	Black	Asian	Hispanic	Native American	White	Unknown
N=24	8	16	3	4	3	2	8	4

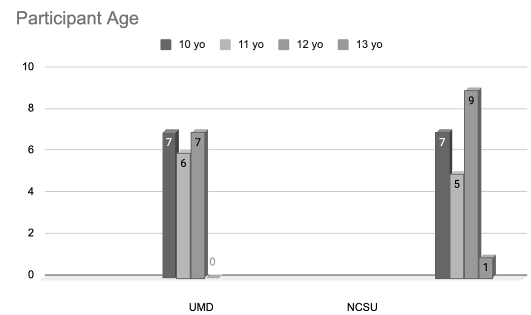

Figure 1: Ages of campers at UMCP and NCSU

3.1.2 Phase 1 Content. Content originated from UMCP's Center's cybersecurity camp curriculum designed for high school juniors and seniors. Lecture materials and lesson activities were modified to be accessible to a middle school audience by providing more scaffolding within the content. Scaffolding helps students make connections between any prior knowledge they may have. Scaffolding is also important in instruction as it has been found to help broaden participation in computing through more accessible learning ramps and increased engagement [29]. Additionally, we modified the materials, following a similar topical reduction strategy to that of Kaur et al. in their 2023 work [19]. Kaur et al found that secondary school students learned and applied the concepts taught after applying a reduction approach to the amount of content and concepts being taught.

Consequently, content topics such as networking, cryptography, hacking, and cybersecurity attacks were selected for inclusion in Phase 1. Previous research found that students needed more networking knowledge to understand cybersecurity concepts [27]. This was addressed in Phase 1 by ensuring students had the foundational knowledge of networking prior to learning about cybersecurity, therefore the first day of camp in Phase 1 was spent learning about networking. Students gained hands-on experience with networking by using NetsBlox, a block-based programming language [22, 30] to implement message passing. Students also visited websites that host ethical hacking puzzles to engage in simple warm-ups.

3.1.3 Phase 1 Implementation. Local students majoring in a computing related field served as instructors for both camps. The lead instructor at NCSU had 3 years of teaching experience at the collegiate level and disseminated the lessons learned to other NCSU staff. The program director at UMCP had 6 years of K-12 teaching experience and also lead a training for the UMCP instructors. Demographic details of the instructors are available in Table 3. To cover the expenses of instructor salaries, transportation, and materials UMCP charged each camper $400 and NCSU charged $450, with NCSU providing meals. Additionally, both universities provided funding for students who expressed financial hardship or need and were awarded scholarships to offset the cost of attending camp. To develop the flow of each camp day in Phase 1, the curriculum followed an active learning approach. A copy of the camp schedule is shown in Figure 2. The warm up activities included playing online game-based learning games, like Kahoot and Blooket, related to the topic students would be learning that day or a review from the previous day. Additionally, the population of students were from different secondary schools, so these activities helped promote engagement among the student groups during the beginning of the session; and as learning aids throughout the lesson. Each day, the instructor lectured on the daily topic, which included computer networks, encryption and decryption, or types of computer hacking. Students then completed unplugged and plugged-in cybersecurity activities like being a human firewall. The goal of the afternoon challenge activity is for students to extend upon the lessons learned earlier in the day or week.

The camp also followed a project based learning approach [26], with students creating projects through block-based programming that encompassed what they learned throughout the week. Students had creative freedom to complete a project that they were interested in with any topic they learned throughout the week, as it has been shown that students value having a choice [21] [29] [23]. Students were able to iteratively work on the project throughout the week, getting assistance from the camp instructors as well. Each participant completed a pre-survey on the first day of camp and a post-survey on the last day of camp. The surveys utilized questions from the Computer Science Attitudes Survey [20] and the Cybersecurity Engagement and Self-Efficacy Scale, Version 2.0 [3, 24] and were modified to meet the needs of this intervention and age group. The survey questions explored key themes such as a student's attitude, belonging, confidence, exposure, future plans, interest, and self-efficacy as it relates to computing and cybersecurity. Questions consisted of multiple choice, open-ended, and Likert scale responses with scales between 1-3, 1-4, and 1-7. At both universities, students engaged with cybersecurity outside of the classroom via cybersecurity company and museum tours to make connections to their classroom experiences. Regarding their favorite part of the camps, both groups ranked working on projects as number one followed by visiting the labs/field trips. When investigating the open-ended responses for what was the most exciting concept or skill learned at camp, six different concepts emerged from the data (frequency of appearance): coding (13), cryptography/ciphers (9), hacking (6), networking (5), binary numbers (3) and protection/security (3). In regards to the open response question on what they may want to learn in the Phase 1 camp the following summer, 25% of students reported that they would like to learn more coding or more advanced coding. Another 17% wanted to learn more practical hacking and 10% of students were interested in learning about more ways to protect information. These requests were split evenly across camp locations. Given the differing dynamics of the two camp populations, the overall survey feedback on activities was positive, with students saying they enjoyed the time spent coding and working on projects. Campers further self-reported increases in interest in studying computer science/cybersecurity in college as well as 95% reporting increased skills and knowledge with technology after attending the camp. There was one significant difference in results between campus A and B, where campers at NCSU reported more changes in attitude toward computer science/cybersecurity, 86.4% vs 55%, p=.025.

Table 3: Demographic information of Phase 1 instructors

Total	Gender		Classification			Multiracial, Black or Hispanic
	Female	Male	Undergrad	Graduate	Staff	
Uni A N=4	3	0	3	0	1	3
Uni B N=4	3	1	2	1	1	2

3.2 Iterative Refinement Process

After Phase 1, the curriculum and survey instruments were modified based on feedback and student interactions. Since the curriculum came from a prior cybersecurity high school camp, the research team determined it would be more impactful if campers learned from the secondary school standards set forth by Cyber.org [9]. Additionally, even though the team scaffolded the curriculum in Phase 1, additional scaffolding was needed, so the material was accessible to all learners. The results from Phase 1 were limited as an oversight led to a missing correlation between the pre and post survey questions for some constructs. Prior to starting the implementation of Phase 2, the surveys were modified to ensure all constructs were assessed in both the pre and post surveys. The Phase 1 and Phase 2 implementations utilized similar curriculum but were not a continuation of one another. As well, the projects students created did not incorporate the topics discussed and were shallow demonstrations such as games that mentioned the topic superficially. For Phase 2, it was imperative that more guidance was provided on what is expected in final projects [14].

3.3 Phase 2

3.3.1 Recruitment. Recruitment at UMCP was the same protocol as conducted in Phase 1. To help provide infrastructure for workshops during the academic year, NCSU changed partnerships to a Science Technology Engineering and Math (STEM) enrichment, pre-college program put on through one of the university's extension programs. Within the pre-college program rising 6th-8th grade students were recruited from school districts within close proximity to the university. Recruitment placed a special emphasis on enrolling students from underserved groups, including students in underrepresented minorities (African-American, Hispanic, Pacific Islander, Native American), first-generation college student, or come from a low-income background. As part of the pre-college program, each student is required to have at least a "C" (2.0/4.0) average in his/her core classes (Math, Science, Language Arts/English, Social Studies). Given this new recruitment partnership, it is assumed that students at NCSU did not have any computer science or cybersecurity experience.

A breakdown of Phase 2 participant demographics is provided in Tables 4 and 5. The most common age of students at both campuses was 12, with a breakdown by location provided in figure 1. UMCP had 0 non-responses and NCSU had 2 non-responses. Overall, each camp hosted a diverse participant group including at least 33% girls, and 33% Black, Hispanic, or Native American students.

3.3.2 Phase 2 Content. The Phase 2 curriculum was developed by utilizing the Cyber.org standards [9]. After completing the first iteration of the curriculum, it was imperative that the learning outcomes aligned with established principles. Cyber.org provides three major themes in their standards: Computing Systems (CS),

	Monday	Tuesday	Wednesday	Thursday	Friday
8:45-9:00	Drop Off *(Location)*	Drop Off *(Location)*	Drop Off *(Location)*	Drop Off *(Location)*	Drop Off *(Location)*
9:00-9:15	Intro to Camp and Cyber security	Intro to Cyrptography	Intro to Ethical Hacking	Introduced Security Project Base Activity, 3 Part Project on ELMS	Security Project Base Activity
9:15-9:30		Unplugged Activity			
9:30-9:45	Ice Breaker				
9:45-10:00		Intro to Cyrptography	7-Steps of Hacking group Activity		
10:00-10:15	Unplugged Activity			Field Trip	
10:15-10:30	Break	Break	Break		Break
10:30-10:45	Intro to Cyber	Intro to Cyrptography	Intro to Ethical Hacking		Security Project
10:45-11:00					
11:00-11:15		Student Cyber Attack Presentations			Capture the Flag Activity
11:15-11:30	Social Activity		OSINT Report on Tony Stark Activtiy on ELMS		
11:30-11:45					
11:45-12:00			Intro to Ethical Hacking		
12:00-12:15	Walk to Lunch Location	Walk to Lunch Location	Walk to Lunch Location		Walk to Lunch Location
12:15-12:30	Lunch *(Location)*	Lunch *(Location)*	Lunch *(Location)*		Lunch *(Location)*
12:30-12:45					
12:45-1:00	Walk Back	Walk Back	Walk Back		Walk Back
1:00-1:15	Intro to Networks	Binary Flippy Do Lecture Activity + Binary Challenge	Unplugged Activity - DDoS		Prepare for Presentations/ Clean Code
1:15-1:30			Phisihing Myself Activity + Presenting Phishing Emails	Security Project	
1:30-1:45		Running Dog Activity			
1:45-2:00					
2:00-2:15	Break	Break	Break	Break	
2:15-2:30	Netsblox Setup	Chatroom Activity	Chatroom Activity + Security Project Base Activity	Security Project	
2:30-2:45	Running Dog Activity				Post Survey
2:45-3:00					Student Security Gallery Walk Presentations
3:00-3:15			Social Activity	Social Activity	
3:15-3:30	Clean Up	Clean Up	Clean Up	Clean Up	Clean Up
3:30-3:45	Pick Up *(Location)*	Pick Up *(Location)*	Pick Up *(Location)*	Pick Up *(Location)*	Pick Up *(Location)*

Figure 2: Phase 1 Schedule

Table 4: Demographic Characteristics of UMCP Phase 2 Participants

Total	Gender			Race/Ethnicity				
	Female	Male	Other	Black	Asian	White	Multi-racial	Unknown
N=16	5	8	3	5	3	3	2	3

Table 5: Demographic Characteristics of NCSU Phase 2 Participants

Total	Gender			Race/Ethnicity			
	Female	Male	Other	Black	Hispanic	Multi-racial	Unknown
N=30	15	13	2	18	3	18	1

Digital Citizenship (DC), and Security (SEC) and three categories under each theme. The research team selected topics that seemed appealing to novice learners while providing the most hands-on experience. The selected topics include: Computer Networks, CIA Triad, Software and Operating Systems, Authentication, Data Security, and Adversarial Thinking. Furthermore, activities were curated to help with learning the material and promote active learning. For each lesson, student guides were created to break the activities into smaller tasks to help improve scaffolding. Research has found that unplugged activities have positive effects on girls' attitudes and performance, thus this was used as a guiding idea for some of the activities such as creating a Jeopardy game for Day 3 and roleplaying as a computer operating system for Day 2 [29]. Students engaged with physical hardware in Phase 2, such as Raspberry Pi's. At the end of each session, students completed exit tickets related to the lesson.

3.3.3 Phase 2 Implementation. During the development of the Phase 2 curriculum, students were considered to be at a novice level related to cybersecurity. In the development process, the research team discussed how each session would be conducted to maintain site reliability. We opted for a setup that had minimal lecturing and implemented interactive participation in the classroom, as students in Phase 1 mentioned the lectures were too lengthy. Phase 2 curriculum was designed so the lecture and discussion would include technology and applications that are popular among secondary-school students. For each session, students were greeted with a warm-up brain teaser, to encourage collaboration. Then, the instructors lectured about the respective topics for the day. Afterward, students were put into groups by the instructors to complete an activity that was submitted online before the end of the session. Finally, students completed their exit tickets. Due to a difference in IRB approval and workshop timings, students were given a pre-survey at the beginning of Session 1 at NCSU and Session 2 at UMCP. Survey questions consisted of multiple choice, open-ended, and Likert scale questions where the scales for most questions were 1-5. The question: *How likely are the following people to encourage you to participate in Computer Science or Technology classes, clubs, or camps?* used a 1-7 scale of strongly agree to strongly disagree (as prescribed by the original question authors) for a pre-selected list of responses. Sessions during Phase 2 were held on the weekends, 2 hours at UMCP and 1.5 hours at NCSU. UMCP and NCSU both had 3 sessions each. These sessions occurred during the Fall 2023 semester at both universities. The program coordinator was also present and hands-on for workshops at UMCP. Local university students majoring in computing served as instructors for both workshops, operating in teams of 3-4 and rotating roles between lead instructor and teaching assistants. As Phase 2 is still ongoing, post-test data has not been collected, and will be presented in future work.

4 DISCUSSION

Student data was collected in the form of pre and post surveys for both Phases. IRB approval was given by UMCP that included a reliance agreement to cover researchers at NCSU. The IRB allowed collecting student demographic data survey responses related to the students experience and knowledge levels around cybersecurity and computer science. Over 70% of students in Phase 1 expressed enjoyment with the overall camp, excluding those with 'some agreement.' Students familiar with cybersecurity found the networking topic confusing and expressed disappointment in learning the same encryption and decryption methods that they learned in prior experiences. Those new to cybersecurity enjoyed both networking and cipher activities, with 30% listing those as their favorite activities. A majority of NCSU students preferred coding. Students at both UMCP and NCSU had varying degrees of experience, both in cybersecurity and computer science. At UMCP, 60% of the students participated in the Center's K-12 Outreach summer or UMCP's school year computing outreach program. At UMCP, only 10% of students self-reported having confidence in their knowledge of cybersecurity, whereas, 90% self-reported having little to no experience in cybersecurity outside of cyber safety. Students at NCSU had little to no computer science or cybersecurity experience. We also saw that students at UMCP had more programming experience than students at NCSU. With this, we noticed that UMCP students finished the activities quicker than anticipated. Future work should look at developing extension activities for students with more experience. Hosting both a cybersecurity-specific summer camp and a workshop has been a good experience for the students and the institutions' broadening participation in computing efforts. We have discovered there are differences in developing both program efforts. At UMCP, summer camp is a fee-based program that launched for the first time last year. Attendance was consistent, engagement fluctuated but overall an experience that students valued for a first of its kind. NCSU's summer camp is also a fee-based program. Although attendance was consistent, engagement was not as prevalent. The Phase 2 workshops were free of charge. With the curriculum adjustments that were made, we noticed students were more engaged with the new lessons and activities. During the Phase 2 workshops, attendance fluctuated, which was attributed to the program being free and on a weekend. Once data is collected from the post-surveys at each location, we hope to do further analysis on UMCP's quick to learn group versus the slower paced group at NCSU to help understand where extra scaffolds and extensions were placed.

4.1 Lessons Learned

To other practitioners who want to use this content, we would recommend the following:

- Curriculum development - The lessons in Phase 1 incorporated lectures that were too lengthy for lower secondary students. We saw that in Phase 2 students enjoyed learning more when the lecturing was kept to no more than 25 minutes at most.
- Content delivery - Certain topics, such as networking models and social engineering, required more hands-on lesson planning. Students required more physical engagement and hands-on activities to understand the topics.
- Student knowledge levels - UMCP and NCSU had students of varying computer science and cybersecurity knowledge. We found that students at UMCP would complete the activities faster than the students at NCSU. Future work should consider implementing open-ended lesson extensions so students can stay engaged if they finish their work early.
- Student reading comprehension - During Phase 2, we found that students had differing levels of reading comprehension skills. This coincides with the work done by Shehzad et al and Salac et al, where they found that language and literacy skills impact participation in computing [29] [28]. Some students had English as a second language, and would benefit from materials in another language or that relied more on figures and pictorial information.
- Cross site implementation - In order to succeed at a cross site implementation of the curriculum, research and outreach staff should meet biweekly to discuss how each program is going. It was critical that both universities were aware of the ongoing situation at the other location to help prepare materials and set evaluation goals.

4.2 Limitations

One limitation in this research was participation biases. Both universities relied on outside organizations to recruit participants for their programs and were unable to control for prior experience or parental coercion. We recognize the potential influence of parental enrollment in various camps and programs. To address this limitation, collaborative efforts with the respective universities will be undertaken to ensure a thorough and varied selection of available camps. Furthermore, NCSU plans to recruit for summer camp participants independently. Another limitation related to recruitment was the cost of the camp. While scholarships were provided, they were limited. Future work should look into ways to implement cost effective cybersecurity summer camp. A second limitation is the discontinuity in NCSU's program. A large break was taken between sessions due to building closures used by their partner organization. We believe using the program coordinator to organize more of the logistics may help the implementation be more agile in response.

5 CONCLUSION AND FUTURE WORK

This work focused on implementing a two phase outreach program to teach early secondary aged students about cybersecurity. Phase 1 included a one week long summer camp at two universities. Phase 2 included weekend sessions taking approximately two hours each. In both phases, students learned cybersecurity topics. Improvements around scaffolding and standards alignment took place between sessions. Future work will look at focus groups in different types of Phase implementation (camps versus weekend events) to determine student enjoyment and knowledge retention via exit tickets and end of course surveys. We intend to perform an in-depth empirical analysis using post surveys from the workshop sessions. Overall, we hope to use this experience to present implementation recommendations and insights regarding cybersecurity education, language accessibility, and material extendability. Future work should look at the longitudinal impacts of these interventions.

ACKNOWLEDGMENTS

This material is based upon work supported by the Funding Agency under Grant Nos. (2207008) and (2206921). Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Funding Agency.

REFERENCES

[1] [n. d.]. https://www.unicef-irc.org/publications/pdf/GKO%20LAYOUT%20MAIN%20REPORT.pdf

[2] AI4K12.org. 2021. The State of K-12 AI Education inYour State Workshop: Executive Summary. Retrieved from https://ai4k12.org/wp-content/uploads/2021/08/Executive-Summary-AI-Education-in-Your-State-v1.0.docx.pdf.

[3] LC Amo, M Zhuo, S Wilde, D Murray, K Cleary, C Amo, S Upadhyaya, and HR Roa. 2015. Cybersecurity engagement and self-efficacy scale. *Unpublished instrument* (2015).

[4] Terry Anderson and Julie Shattuck. 2012. Design-based research: A decade of progress in education research? *Educational researcher* 41, 1 (2012), 16–25.

[5] Erik Barendsen and Tim Steenvoorden. 2016. Analyzing conceptual content of International Informatics Curricula for Secondary Education. *Informatics in Schools: Improvement of Informatics Knowledge and Perception* (2016), 14–27. https://doi.org/10.1007/978-3-319-46747-4_2

[6] Torsten Brinda, Matthias Kramer, and Yannick Beeck. 2018. Middle school learners' conceptions of social networks: Results of an Interview Study. *Proceedings of the 18th Koli Calling International Conference on Computing Education Research* (2018). https://doi.org/10.1145/3279720.3279723

[7] Veronica Cateté, Nicholas Lytle, Yihuan Dong, Danielle Boulden, Bita Akram, Jennifer Houchins, Tiffany Barnes, Eric Wiebe, James Lester, Bradford Mott, and et al. 2018. Infusing computational thinking into Middle Grade Science classrooms: lesson learned. *Proceedings of the 13th Workshop in Primary and Secondary Computing Education* (2018). https://doi.org/10.1145/3265757.3265778

[8] Code.org, CSTA, and ECEP Alliance. 2022. 2022 State of Computer Science Education: Understanding Our National Imperative. Retrieved from https://advocacy.code.org/stateofcs.

[9] Cyber.org. 2023. K-12 Cybersecurity Learning Standards. Retrieved from https://cyber.org/standards.

[10] Susan Edwards, Andrea Nolan, Michael Henderson, Ana Mantilla, Lydia Plowman, and Helen Skouteris. 2016. Young Children's everyday concepts of the internet: A platform for cyber-safety education in the early years. *British Journal of Educational Technology* 49, 1 (2016), 45–55. https://doi.org/10.1111/bjet.12529

[11] Sirpa Eskelä-Haapanen and Carita Kiili. 2019. 'it goes around the world' – children's understandingof the internet. *Nordic Journal of Digital Literacy* 14, 3–4 (2019), 175–187. https://doi.org/10.18261/issn.1891-943x-2019-03-04-07

[12] Katrina Falkner, Sue Sentance, Rebecca Vivian, Sarah Barksdale, Leonard Busuttil, Elizabeth Cole, Christine Liebe, Francesco Maiorana, Monica M. McGill, and Keith Quille. 2019. An international comparison of K-12 computer science education intended and enacted curricula. *Proceedings of the 19th Koli Calling International Conference on Computing Education Research* (2019). https://doi.org/10.1145/3364510.3364517

[13] Ruthe Farmer, Tina Boyle Whyte, and Anthony Todd Taylor. 2020. Engaging JROTC Youth in CS Pathways: A Community Discussion of K-12 Cyber Security and Data Science Topics. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*. 1405–1405.

[14] Diana Franklin, Jean Salac, Cathy Thomas, Zene Sekou, and Sue Krause. 2020. Eliciting student scratch script understandings via scratch charades. *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (2020). https://doi.org/10.1145/3328778.3366911

[15] Tereza Hannemann, Tereza Stárková, Pavel Ježek, Kristina Volná, Kateřina Kačerovská, and Cyril Brom. 2019. Eight-year-olds' conceptions of computer viruses. *Proceedings of the 14th Workshop in Primary and Secondary Computing Education* (2019). https://doi.org/10.1145/3361721.3361726

[16] Amy Isvik, Veronica Catete, Erynn Elmore, and Tiffany Barnes. 2021. Examining equity in computing-infused lessons made by novices. *2021 Conference on Research in Equitable and Sustained Participation in Engineering, Computing, and Technology (RESPECT)* (2021). https://doi.org/10.1109/respect51740.2021.9620700

[17] Amy Isvik, Veronica Cateté, and Tiffany Barnes. 2021. Investigating the impact of computing vs pedagogy experience in novices creation of computing-infused curricula. *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 1* (2021). https://doi.org/10.1145/3430665.3456319

[18] Robin Jocius, Deepti Joshi, Yihuan Dong, Richard Robinson, Veronica Cateté, Tiffany Barnes, Jennifer Albert, Ashley Andrews, and Nicholas Lytle. 2020. Code, Connect, Create: The 3C Professional Development Model to Support Computational Thinking Infusion. *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (2020). https://doi.org/10.1145/3328778.3366797

[19] Gurmeher Kaur, Kris Jordan, and Jasleen Kaur. 2023. Using foundational CS1 curricula for Middle School & Early High School Computer Programming Education. *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1* (2023). https://doi.org/10.1145/3545945.3569877

[20] J J LaBouliere, Amanda Pelloth, Chiao-Ling Lu, and Jason Ng. 2015. An exploration of the attitudes of young girls toward the field of computer science. In *2015 IEEE Frontiers in Education Conference (FIE)*. 1–6. https://doi.org/10.1109/FIE.2015.7344265

[21] Anna Lamprou, Alexander Repenning, and Nora A. Escherle. 2017. The Solothurn Project - Bringing Computer Science Education to Primary Schools in Switzerland. *Proceedings of the 2017 ACM Conference on Innovation and Technology in Computer Science Education* (2017). https://doi.org/10.1145/3059009.3059017

[22] Ákos Lédeczi, MiklÓs MarÓti, Hamid Zare, Bernard Yett, Nicole Hutchins, Brian Broll, Péter Völgyesi, Michael B Smith, Timothy Darrah, Mary Metelko, et al. 2019. Teaching cybersecurity with networked robots. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. 885–891.

[23] Nicholas Lytle, Veronica Cateté, Danielle Boulden, Yihuan Dong, Jennifer Houchins, Alexandra Milliken, Amy Isvik, Dolly Bounajim, Eric Wiebe, and Tiffany Barnes. 2019. Use, Modify, Create: Comparing Computational Thinking Lesson Progressions for STEM Classes. *Proceedings of the 2019 ACM Conference on Innovation and Technology in Computer Science Education* (2019). https://doi.org/10.1145/3304221.3319786

[24] M.M McGill. 2021. Cybersecurity Engagement and Self-Efficacy Scale, Version 2.0. Adapted from the Cybersecurity Engagement and Self-Efficacy Scale (2015) by Amo, L.C. and Zhuo, M. and Wilde, S. and Murray, D. and Cleary, K. and Amo, C. and Upadhyaya, S. and Roa, H.R. Retrieved from https://sites.google.com/site/amoceses/home (2015) and https://csedresearch.org/tool/?id=260 (Version 2.0, 2021)..

[25] Monica M McGill, Sarah B Lee, Litany Lineberry, John Sands, and Leigh Ann DeLyser. 2021. Piloting the air force jrotc cyber academy for high school students. In *Proceedings of the 52nd acm technical symposium on computer science education*. 597–603.

[26] Robert Pucher and Martin Lehner. 2011. Project Based Learning in Computer Science – a review of more than 500 projects. *Procedia - Social and Behavioral Sciences* 29 (2011), 1561–1566. https://doi.org/10.1016/j.sbspro.2011.11.398

[27] Manuel Riel and Ralf Romeike. 2020. It security in secondary CS Education: is it missing in today's curricula? A qualitative comparison. *Proceedings of the 15th Workshop on Primary and Secondary Computing Education* (2020). https://doi.org/10.1145/3421590.3421623

[28] Jean Salac, Cathy Thomas, Bryan Twarek, William Marsland, and Diana Franklin. 2020. Comprehending Code: Understanding the Relationship between Reading and Math Proficiency, and 4th-Grade CS Learning Outcomes. *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (2020). https://doi.org/10.1145/3328778.3366822

[29] Umar Shehzad, Mimi Recker, and Jody Clarke-Midura. 2023. A literature review examining broadening participation in Upper Elementary CS Education. *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1* (2023). https://doi.org/10.1145/3545945.3569873

[30] Gordon Stein and Akos Lédeczi. 2021. Enabling collaborative distance robotics education for novice programmers. In *2021 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*. IEEE, 1–5.

[31] Katerina Tsarava, Manuel Ninaus, Tereza Hannemann, Kristina Volná, Korbinian Moeller, and Cyril Brom. 2020. Fostering knowledge of computer viruses among children: The Effects of a Lesson with a Cartoon Series. *Koli Calling '20: Proceedings of the 20th Koli Calling International Conference on Computing Education Research* (2020). https://doi.org/10.1145/3428029.3428033

[32] L. S. Vygotskiĭ, Michael Cole, Sally Stein, and Allan Sekula. 1978. *Mind in society: The development of Higher Psychological Processes*. Harvard University Press.

[33] Rick Wash. 2010. Folk models of Home Computer Security. *Proceedings of the Sixth Symposium on Usable Privacy and Security* (2010). https://doi.org/10.1145/1837110.1837125

[34] David Weintrop, Margaret Walton, Andrew Elby, Janet Walkoe, et al. 2020. Mutually supportive mathematics and computational thinking in a fourth-grade classroom. (2020). International Society of the Learning Sciences (ISLS).