Lessons Learned from a Cybersecurity Summer Camp

Dr. Te-shun Chou, East Carolina University

Dr. Te-Shun Chou is a Professor in the Department of Technology Systems (TSYS) at East Carolina University's College of Engineering and Technology (CET). He coordinates the Master's program in Information and Cybersecurity Technology for TSYS and is the lead faculty for the Digital Communication Systems concentration within the Consortium Universities of the Ph.D. program in Technology Management. Additionally, he serves as the point of contact for the Center of Academic Excellence in Cyber Defense (CAE-CD) at ECU. Dr. Chou has extensive experience supervising theses, practicums, and research projects for both graduate and undergraduate students. He has published articles in the areas of cybersecurity, machine learning, and technology education.

Xi Lin, East Carolina University

Dr. Xi Lin is an associate professor at East Carolina University, US. Her research focuses on seeking best practices to enhance student engagement and interaction in online learning environments. More information can be found at http://whoisxilin.weebly.com/

Dr. Biwu Yang, East Carolina University

Dr. Biwu Yang is a professor in the Department of Technology Systems, East Carolina University. He teaches in the field of data networking, information technology, and information security. He has served as the key technology person in all aspects of Gl

Dr. Tijjani Mohammed, East Carolina University

Tijjani Mohammed is an associate professor and chairperson in the department of Technology Systems, within the College of Engineering and Technology, at East Carolina University. His areas of intertest include computer networks, digital and microprocesso

Lessons Learned from a Cybersecurity Summer Camp

Abstract

During the summer of 2024, East Carolina University hosted a five-day GenCyber camp specifically designed for high school STEM teachers from grades 9-12 in Eastern North Carolina. A total of eleven teachers took part in the camp. The camp aimed to enhance their knowledge and skills in cybersecurity by offering a comprehensive blend of theoretical lessons and hands-on activities. The curriculum not only focused on technical aspects, but also emphasized the importance of ethical and legal considerations when navigating the digital realm. Throughout the course of the camp, participants were encouraged to reflect on their learning by developing detailed lesson plans, which they then presented on the final day. In addition, an exit survey was conducted on the last day to assess the camp's overall effectiveness. Overall, the camp's combination of theoretical and practical components ensured that the participants gained both expertise and confidence needed to integrate cybersecurity education into their curricula. The teachers were well-prepared to guide their students in addressing the growing cybersecurity challenges in today's digital world.

Keywords: Cybersecurity; cyberattack; cyber defense; teacher education

1. Introduction

In today's rapidly advancing technological world, a vast number of cyberattacks occur daily. According to the 2023 Internet Crime Report by the Internet Crime Complaint Center, 880,418 complaints were received from the American public, with potential losses surpassing $12.5 billion. This represents a 10% increase in complaints and a 22% rise in losses compared to 2022 [1]. As cybercrime emerges as the most significant threat to individuals, private industries, and government agencies, the urgency to strengthen cybersecurity education and develop well-trained cybersecurity professionals has never been greater. This is essential to safeguard our citizens, businesses, and critical infrastructure from cyberattacks.

Supported by the GenCyber grant program, eleven STEM teachers (6 male and 5 female) from nine public high schools in Eastern North Carolina were invited to participate in a five-day cybersecurity camp during the summer of 2024. The camp was designed to deepen participants' understanding of cybersecurity, covering all GenCyber Cybersecurity Concepts. The comprehensive curriculum aimed to equip these educators with the knowledge and skills necessary to teach cybersecurity effectively, thereby fostering the next generation of cybersecurity professionals. The curriculum covered all GenCyber Cybersecurity Concepts:

- Defense in Depth: A comprehensive strategy of including multiple layers of security within a system so that if one layer fails, another layer of security is already in place to stop the attack/unauthorized access.
- Confidentiality: The property that information is not disclosed to individuals, devices, or processes unless they have been authorized to access the information.
- Integrity: The property that information, an information system, or a component of a system has not been modified or destroyed in an unauthorized manner.
- Availability: The property that information or information systems are accessible and usable upon demand.

- Think Like an Adversary: The strategy of putting yourself inside the mindset of a potential attacker that allows you to anticipate attack strategies and defend your systems accordingly.
- Keep It Simple: The strategy of designing information and security systems to be configured and operated as simply as possible; all systems perform best when they have simple designs rather than complex ones.

During the summer camp, participants not only received theoretical instruction but also engaged in practical exercises to reinforce key concepts. Each morning featured interactive lectures on essential topics such as network security threats, cyberattack defense mechanisms, mitigation strategies, and cyber ethics. In the afternoons, teachers participated in hands-on sessions to apply the knowledge gained from the morning lectures, enhancing their practical skills and confidence in utilizing cybersecurity tools and techniques.

A dedicated learning platform, Canvas, was set up to host all instructional resources, providing ongoing access to materials both during and after the camp. The curriculum also emphasized cyber ethics and the ethical responsibilities of cybersecurity professionals. To further enrich the experience, three guest speakers from industry and academic institutions were invited to discuss current cybersecurity tools, applications, technologies, challenges, and trends.

To help participants integrate new knowledge into their teaching practices, the camp included sessions for developing lesson plans. Each teacher created and presented lesson plans tailored to the needs of their classroom on the final day, showcasing their ability to teach cybersecurity concepts effectively. The camp also fostered collaborative learning by dividing participants into three groups for discussions and activities aimed at incorporating cybersecurity into lesson plans. Handouts on educational theories, lesson plan templates, and research studies were provided for reference. The camp concluded with group presentations and a post-camp survey, which offered valuable feedback on the program's effectiveness.

This paper is organized as follows: Section 2 examines the survey assessment and its results. Section 3 discusses our observations. Finally, we conclude our work in the last section.

2. Assessment

The primary goal of the summer camp was to equip high school teachers with essential cybersecurity knowledge and skills for effective curriculum development and instruction. To facilitate reflection on their learning and gather feedback, an assessment survey was designed to evaluate the participants' knowledge and skills, perceptions of the camp, and self-efficacy in teaching and integrating cybersecurity into their classrooms. Out of the eleven teachers who attended the camp, nine completed the exit survey, while two left early on the final day due to personal reasons.

The survey was created using Google Forms and included both Likert-scale and open-ended questions. It was divided into three categories to gauge the effectiveness of the camp activities: (1) self-assessment of participants' knowledge levels regarding GenCyber Cybersecurity Concepts before and after attending the camp, (2) evaluation of the camp experience, and (3)

overall perspective on the summer camp. The results of this survey are intended to provide insights for improving the relevance and effectiveness of future camp activities, ensuring they better meet participants' learning needs.

2.1. Cybersecurity Knowledge Level Self-Assessment

Six questions were crafted to evaluate participants' knowledge levels concerning the GenCyber Cybersecurity Concepts. Table 1 presents the survey questions, and Figure 1 illustrates the results.

Before attending the camp, participants completed a pre-survey, and they rated their proficiency in GenCyber Cybersecurity Concepts with the highest "above good" scores (good, very good, and excellent) for questions Q1.3 and Q1.4, achieving a rate of 66.67%. This high rating was likely due to the relatively greater familiarity with topics of integrity and availability compared to other subjects. After attending the camp, all "above good" rates significantly increased to 100%. Yet, for Q1.5, the improvement was less pronounced. It is possible that the camp did not focus extensively on hacker techniques for attacking cyber resources.

Table 1. Self-assessment of knowledge level in the subjects of cybersecurity Before and after attending the camp

Questions	Subjects
Q1.1	Defense in Depth
Q1.2	Confidentiality
Q1.3	Integrity
Q1.4	Availability
Q1.5	Think Like an Adversary
Q1.6	Keep It Simple

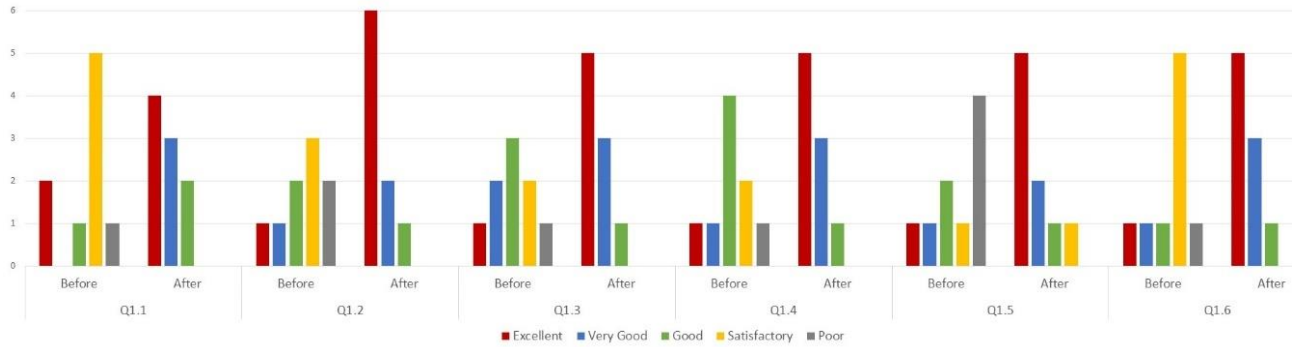

Figure 1. Survey results

Statistical methods were also employed to analyze the survey data, A paired t-test was conducted with Table 2 comparing the pre- and post-camp assessment results. The data demonstrated high significance, with the p-value significantly below 0.05. The mean scores for responses before the camp were below 3.0, while those after the camp were above 4.0. These results indicate that

participants held very positive attitudes towards both the lectures and the hands-on activities provided during the camp.

Table 2. Statistical analysis

	Before		After		
	Mean	SD	Mean	SD	P-Value
Q1.1	2.67	1.41	4.22	0.83	8.74E-04
Q1.2	2.56	1.33	4.56	0.73	1.62E-04
Q1.3	3.00	1.22	4.44	0.73	1.68E-04
Q1.4	2.89	1.17	4.44	0.73	1.02E-04
Q1.5	2.33	1.50	4.22	1.09	3.32E-04
Q1.6	2.56	1.24	4.33	1.00	2.91E-04

Additionally, participants were asked two questions regarding their understanding of cybersecurity ethical responsibilities and their overall cybersecurity knowledge before and after the camp. The questions were: Q1.7: "How would you rate yourself on the ethical responsibilities of cybersecurity professionals?" and Q1.8: "How would you rate yourself on your overall cybersecurity knowledge?" Figures 2 and 3 present the survey results. All participants reported an improved understanding of the ethical responsibilities of cybersecurity professionals and a significant enhancement in their overall cybersecurity knowledge.

Figure 2. Survey result of Q1.7

Figure 3. Survey result of Q1.8

2.2. Assessment of Camp Experience

Table 3 displays eight agree/disagree questions designed to assess participants' perceptions of the camp. A 5-point scale was used, where 1 indicates strong disagreement and 5 indicates strong agreement. Figure 4 presented the survey results. The mean scores for all questions were above 4.0. Participants indicated that they appreciated learning about cybersecurity and valued the presentations from guest speakers. They also found the lesson plan development to be beneficial for their future teaching in cybersecurity.

Table 3. The assessment of camp experience

Questions	Assessments
Q2.1	I enjoyed listening to the lectures.
Q2.2	The lectures were helpful in getting theoretical knowledge of cybersecurity.
Q2.3	I enjoyed conducting the hands-on lab activities.
Q2.4	The hands-on labs were helpful in getting practical experiences of cybersecurity.
Q2.5	I enjoyed the presentations by the guest speakers.
Q2.6	The guest speaker presentations were helpful in enhancing my understanding of cybersecurity.
Q2.7	I enjoyed the lesson plan development activities.
Q2.8	The lesson plan development was helpful in developing my future lesson plan related to cybersecurity.

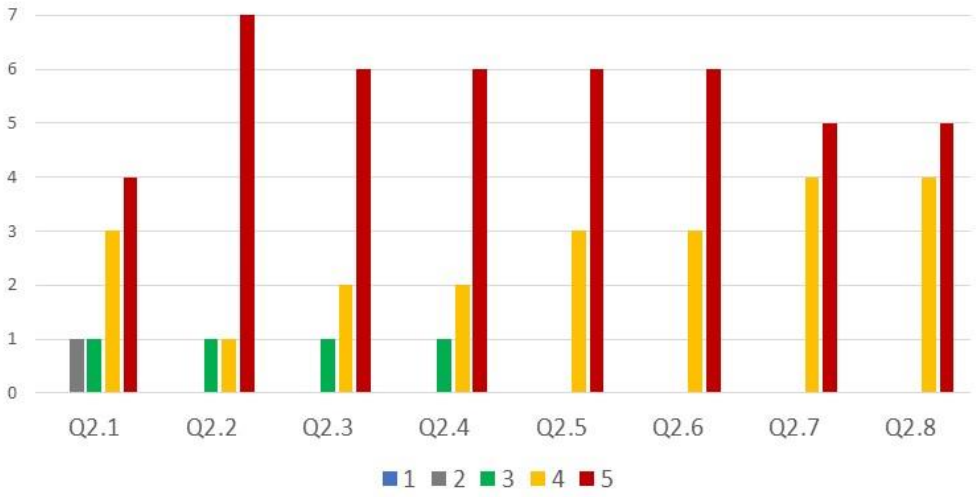

Figure 4. Survey results

2.3. Overall Perspective of the Camp

Table 4 presents seven open-ended questions designed to gather feedback from participants. All respondents expressed a highly positive attitude towards the camp activities. A multiple-case study approach was conducted to qualitatively analyze participants' responses to open-ended questions. This method was particularly effective in exploring the “how” and “why” of class engagement, emphasizing current events while allowing researchers limited control over the data [2]. Each participant was regarded as an individual case in the study. Thematic analysis, based on Braun and Clarke’s [3] guidelines, was then used to assess the feedback from participants, which enabled the representation of their authentic voices. The initial coding phase was based on each participant’s responses, leading to the development of a codebook. In the second analysis phase, an inductive open-coding approach was implemented, with the authors collaborating to identify significant themes. Ultimately, the themes were refined in the final round, ensuring the generation of robust and compelling findings for the study [2][4]. Five themes were generated.

Table 4. Open-ended questions

Q2.1	What is your overall experience of the lectures? Please tell us about any benefits, difficulties, and areas for improvement.
Q2.2	What is your overall experience of the lab and hand-on activities? Please tell us about any benefits, difficulties, and areas for improvement.
Q2.3	What is your overall experience of the lesson plan development? Please tell us about any benefits, difficulties, and areas for improvement.
Q2.4	How would you rate the overall effectiveness of the 2024 GenCyber Summer Camp in equipping you with cybersecurity knowledge and skills to deliver the content to your students? Please provide specific reasons and examples.
Q2.5	What recommendations do you have for improving future GenCyber Summer Camp?
Q2.6	If you are available, are you interested in attending our GenCyber summer camp again if we host it in different cybersecurity topics in the future?
Q2.7	Will you recommend your friends/colleagues to attend our GenCyber summer camp if we host it again in the future?

2.3.1. Theme 1: Effective and Engaging Instruction

First, participants in the GenCyber Summer Camp appreciated the structured and organized delivery of content. They highlighted the detailed lectures and well-organized slide presentations as particularly effective in facilitating learning. One participant noted, “Lectures was very detail and easy to follow.” Another participant noted, “The slide presentations were well organized and informative. The lectures allowed us to ask questions and ‘dig deeper’ into concepts.” Despite the wealth of information presented, some participants expressed challenges in keeping pace, acknowledging that while the lectures were excellent, they found it tiring at times, “The whole lecture was excellent. I was a bit tired and it was hard for me to keep the pace. But I did my best to follow every single one.”

2.3.2. Theme 2: Value of Hands-On Learning

Second, the hands-on labs were a standout feature of the camp, with participants valuing the opportunity to engage in practical activities both during and outside of class. Many participants expressed that these labs were instrumental in broadening their understanding of cybersecurity. One participant stated, “I enjoyed the hands-on labs and appreciate the accessibility to work on them both during and after class. The labs stretched my thinking concerning cybersecurity.” Similarly, others expressed, “[I] love it [the lab activity], [I] will do some at home,” and “[I] love the hands-on activities.” However, there was a common desire for more time to fully engage with the various lab activities. As noted, “I like to have more time on labs”, and “…more time on hands-on activity and possible field trip.” Overall, participants found the hands-on activities to be excellent, reinforcing their appreciation for this interactive learning format.

2.3.3. Theme 3: Collaborative Learning Environment

Additionally, collaboration emerged as one benefit during the camp, particularly in the development of lesson plans. Participants enjoyed working with their peers, which fostered a

supportive learning environment. One participant expressed, “I love creating lesson plans and enjoyed working with our group members.” This collaborative approach was complemented by the K-12 pedagogical expert’s effective handouts and innovative methods, which participants found helpful in the lesson planning process. Another participant also remarked, “…very thorough and gained a lot of experience,” emphasizing the richness of the collaborative experience. Overall, the opportunity to share ideas and strategies with others contributed positively to their learning journey.

2.3.4. Theme 4: Increased Confidence in Teaching Cybersecurity

Another significant outcome of the camp was the enhancement in participants’ confidence regarding their ability to teach cybersecurity concepts. Many participants reported feeling more equipped to share their new gained knowledge with their students and colleagues. As one participant highlighted, “…I feel more confident in sharing the concepts of cyber security and digital safety with my students and fellow teachers.” The depth of knowledge gained during the camp was profound, with one participant stated, “Words cannot describe the knowledge I gained concerning cyber security...” and “This experience has been amazing, and I am walking away with so much more than what I arrived with.” This increased confidence demonstrates the effectiveness of the camp in enhancing teachers’ professional readiness.

2.3.5. Theme 5: Enthusiasm for Future Participation

Lastly, participants expressed strong interest in attending future GenCyber Summer Camps, showing overall satisfaction with their experience. Many participants conveyed their desire to return, such as “I enjoyed being here,” and “I would love to come back.” The camp was described as an enriching experience, with some participants noting, “The camp exceeded my expectations,” “It was an awesome experience,” and “Thank you for this amazing learning opportunity.” Additionally, participants expressed their intention to recommend the program to friends and colleagues such as, “I will recommend the program to their friends and colleagues.” This enthusiasm reflects the positive impact of the camp on participants and their eagerness to continue their professional development in cybersecurity education.

3. Discussion

3.1. Lectures and Hands-On Activities

During the camp, an extensive range of cybersecurity topics was addressed, including fundamental cybersecurity concepts, network security threats and attacks, defense mechanisms against cyberattacks, mitigation strategies, countermeasures, and management techniques, as well as cyber ethics and wireless-based attacks. However, the comprehensive coverage of these subjects limited the time available for hands-on exercises, which many participants had hoped to engage in more fully.

The practical exercises are particularly valuable as they enable participants to apply theoretical knowledge, become adept at using relevant technologies, and ultimately gain the confidence to teach these concepts to their students. Therefore, it might be beneficial to consider reducing the

number of topics covered in each subject or to streamline the depth of content in future camps. This adjustment would allow participants to dedicate more time to hands-on activities, thereby enhancing their practical skills and overall learning experience.

3.2. Lesson Plan Development

To enhance collaboration among the participating teachers, the eleven attendees were organized into three groups. Interactive games were incorporated to stimulate brainstorming and foster creativity. Each day, the participants received comprehensive instructions to guide their activities. All of the teachers reported that they enjoyed the collaborative process and working closely with their group members.

The positive feedback underscores the importance of structured guidance in helping teachers develop effective lesson plans. By providing clear instructions and facilitating teamwork, the camp ensured that teachers could engage in meaningful collaboration, exchange ideas, and refine their educational strategies. This approach not only enhanced the development process but also contributed to a more cohesive and productive learning environment. Consequently, structured guidance and collaborative activities are crucial in supporting teachers to create successful and innovative lesson plans.

3.3. Social Engineering in K-12 Education

Social media has become a fundamental part of daily life for most people, particularly the youth, who use it almost constantly. Reflecting this reality, all three group presentations and eight out of eleven lesson plans during the camp were focused on social engineering. This indicates a strong desire among the participant teachers to impart knowledge about social engineering to their students.

One teacher highlighted the importance of awareness, stating, "The awareness of the risk and the need for students to realize what they’re clicking could harm them is crucial. It’s been eye-opening to me. I had no idea." She emphasized the need to extend online protection beyond the school environment, saying, "I’m not so concerned about their school devices. I’m concerned about their home use of cell phones. They get on social media and click on ads without knowing how easy it is for cyberattacks." [5]

Given these insights, it is evident that more time should be devoted to teaching social engineering topics such as phishing, vishing, and smishing. Additionally, it is essential to emphasize ethics and legal issues to ensure students understand the broader implications of their online activities. By doing so, teachers can better prepare their students to navigate the digital world safely and responsibly.

3.4. Guest Speakers

Three guest speakers from industry and academic institutions were invited to present on critical infrastructure, the cybersecurity landscape, and privacy threats. The participants were highly engaged, asking numerous questions and having excellent interactions with the speakers.

We strongly believe that guest speakers play a crucial role in a cybersecurity camp. They can introduce topics that may not be covered in the camp curriculum and provide the latest information on cybersecurity tools, applications, technologies, challenges, and trends. By bringing in experts from the field, participants can gain a broader understanding of the current state of cybersecurity and therefore enhance their overall learning experience.

Conclusion

The GenCyber camp was an intensive and engaging program that successfully covered a wide range of cybersecurity topics through lectures, hands-on activities, and collaborative lesson plan sessions. Over the course of five days, participants were immersed in subjects including cybersecurity concepts, network security threats, cyberattack defenses, and cyber ethics. Although the comprehensive nature of the lectures limited time for practical exercises, participants remained active and engaged, frequently interacting with the instructors and their peers. The inclusion of hands-on labs allowed participants to apply their theoretical knowledge in real-world scenarios, significantly enhancing their practical skills.

Moreover, the camp featured enriching sessions with guest speakers from industry and academia. These sessions provided participants with up-to-date information on cybersecurity and hence fostered them a deeper understanding of the field. Additionally, the collaborative lesson plan sessions facilitated brainstorming and creativity, supported by structured guidance and interactive games. Participants appreciated the opportunity to work closely with their peers, resulting in well-designed and effective lesson plans showcased on the final day. The overwhelmingly positive feedback from post-camp surveys underscores the camp's success in promoting a robust learning environment and equipping teachers with the skills and confidence needed to educate their students about cybersecurity.

References

1. "2023 Internet Crime Report," Internet Crime Complaint Center (IC3), *Federal Bureau of Investigation (FBI)*, 2023. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
2. R. K. Yin, *Case Study Research: Design and Methods (Applied Social Research Methods)*, Fifth Edition, SAGE Publication, Inc., 2013.
3. V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77-101, 2006.
4. R. Thornberg and K. Charmaz, "Grounded theory and theoretical coding," in *The SAGE Handbook of Qualitative Data Analysis*, 2014, pp. 153-169.
5. K. Buday, "High School Teachers Learn About Cybersecurity Through Unique Camp", *ECU News*, June 2024. [Online]. Available: https://news.ecu.edu/2024/06/27/high-school-teachers-learn-about-cybersecurity-through-unique-camp/