Journal of Information Systems Education

Volume 36
Issue 4
Fall 2025

Teaching Tip

Establishing a GenCyber Student Camp for High School Students in Underserved Communities

Anh Duong, Maria Valero, John Oakley, and Miloslava Plachkinova

Recommended Citation: Duong, A., Valero, M., Oakley, J., & Plachkinova, M. (2025). Teaching Tip: Establishing a GenCyber Student Camp for High School Students in Underserved Communities. *Journal of Information Systems Education*, 36(4), 367-378. https://doi.org/10.62273/IYTO9802

Article Link: https://jise.org/Volume36/n4/JISE2025v36n4pp367-378.html

Received: March 23, 2025
First Decision: June 30, 2025
Accepted: July 24, 2025
Published: December 15, 2025

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Journal of Information Systems Education, 36(4), 367-378, Fall 2025
https://doi.org/10.62273/IYTO9802

Teaching Tip
Establishing a GenCyber Student Camp for High School Students in Underserved Communities

Anh Duong
Department of Computer Science
Kennesaw State University
Marietta, GA 30060, USA
aduong2@students.kennesaw.edu

Maria Valero
John Oakley
Department of Information Technology
Kennesaw State University
Marietta, GA 30060, USA
mvalero2@kennesaw.edu, joakley7@students.kennesaw.edu

Miloslava Plachkinova
Department of Information Systems and Security
Kennesaw State University
Kennesaw, GA 30144, USA
mplachki@kennesaw.edu

ABSTRACT

This teaching tip offers valuable insights into establishing a GenCyber student camp in underserved communities. It provides teaching tips and best practices for designing a curriculum tailored to high school students. The study highlights effective strategies for recruiting a diverse group of participants, addressing the global shortage in the cybersecurity workforce. Over a six-month period, students participated in a variety of online and in-person activities. The study presents practical assignments used to boost student engagement and participation. Experiential Learning Theory was applied to develop and implement learning objectives, with adapted scales to measure outcomes specific to the program's needs. Overall, students demonstrated increased cybersecurity knowledge upon completing the camp. This teaching tip serves as proof of concept, encouraging others to seek NSA funding for GenCyber grants to benefit their local communities.

Keywords: GenCyber, Cybersecurity, Computing education, Experiential learning & education, Teaching tip, STEM

1. INTRODUCTION

With the rapid growth of emerging technologies in various sectors, including education, healthcare, finance, and manufacturing (Yaacob et al., 2023), cybersecurity — the technique of protecting networks from unauthorized access and the practice of ensuring the confidentiality of information — is essential to preventing risks and attacks in organizations. Cybersecurity is a rapidly growing industry with an estimated increase of 32% from 2022 to 2032 and over 700,000 open roles in the United States alone (Hellmann, 2023). Even though it is a growing field, the Cybersecurity Workforce Study has shown that there is a global shortage of nearly four million cybersecurity professionals in 2023, which increases the chance of organizations being at moderate or extreme risk of cybersecurity attacks (ISC2, 2023).

From a survey of 1,885 information technology (IT) and cybersecurity decision makers conducted by Fortinet in 2023, 84% of organizations experienced at least one cybersecurity breach in the past 12 months, and 65% of organization leaders expected a 20% increase in cyberattacks within the next 12 months. As a result, 85% of organizations have been adopting security education, training, and awareness (SETA) programs for their employees, while 73% of organizations without a training program are looking for one. Despite the active emergence of these SETA programs, 56% of leaders still

believe their employees lack cybersecurity knowledge, and the gaps in training still persist within organizations (Fortinet, 2023).

With the current shortage of professionals, high risks of cyberattacks, and a defined diversity gap within the organizations (Lachow, 2022), along with a lack of effective training and employees with weak cybersecurity foundations, it is important to increase cybersecurity foundations and awareness within the workforce and the education system, from K-12 to higher education. Educational programs, cybersecurity awareness enforcement, and curriculum development are the solutions to building a stronger foundation and preparing the next generation to proactively respond to the rapid growth of cyberattacks (The EdWeek Research Center, 2020). To increase the strong foundation of cybersecurity knowledge, the U.S. government has been providing numerous federal funding opportunities to support educational programs and projects. Some federal fundings that advocate cybersecurity in K-12 education include the National Science Foundation (NSF), the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), State and Local Cybersecurity Grant Program (SLCGP), and the Tribal Cybersecurity Grant Program (TCGP) by the Department of Homeland Security (DHS). These funding opportunities were created as part of the efforts to increase the qualified workforce needed by the nation and to establish standards for cybersecurity curriculum in education (National Security Agency, 2024).

One of the educational programs supported by federal funding is the GenCyber program. It is funded by the NSA and NSF. GenCyber aligns with the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program to sustain cybersecurity interest at the K-12 level and increase awareness of K-12 cybersecurity content for students and educators. GenCyber provides four different types of programs — student camps, teacher camps, combination (student and teacher) camps, and student language camps—which serve mainly students and teachers with the goals of (i) increasing awareness of cybersecurity content and career opportunities for participants; (ii) increasing student diversity and career readiness pathways; and (iii) facilitating teacher readiness to deliver content for the classroom. With its dedicated goals and offers, GenCyber strives to be a part of the solution to the nation's shortage of skilled cybersecurity professionals while having a nationwide impact on the K-12 cybersecurity education ecosystem.

As part of the efforts to address the shortage of cybersecurity professionals, we saw the significance of impacting the local community and inspiring the younger generation. We received strong input from Atlanta Metropolitan Area schools that students are barely exposed to cybersecurity fundamentals due to a lack of opportunities and an engaging curriculum. The current Georgia Department of Education's (2023) guidelines include three courses - information technology, introduction to cybersecurity, and advanced cybersecurity. These guidelines fall short of providing valuable experiences to learners through career cybersecurity professionals, such as ethical hackers and cyber forensics professionals. Moreover, Georgia is the eighth most populous state in the US and currently has 15,000+ cybersecurity-related positions available according to CyberSeek.org (2024). However, there is not a sufficient workforce to fill these positions. There is currently a very limited number of GenCyber camps through federal funding support to attract high school students to inspire and motivate them to pursue cybersecurity careers and degree programs. As such, a new student camp at Kennesaw State University (KSU) can tremendously help the Atlanta metro area and surrounding county high school students to get early exposure to cybersecurity and pursue cyber-related degree programs at KSU and other schools.

Thus, in the summer of 2023, we hosted the first GenCyber Camp at KSU to expose high school students within the area to foundational cybersecurity knowledge. This paper is focused on the curriculum and implementation of the GenCyber program at KSU. It provides valuable teaching tips and technical labs for others who may be interested in pursuing NSA-funded GenCyber grants in the future. We explain the key elements of developing the high school curriculum as well as the relevant scales and metrics to evaluate the program's effectiveness. Our approach is based on Experiential Learning Theory (ELT), which allowed us to build a solid foundation and achieve practical results. Finally, we present insights related to attracting a diverse cohort, which, in turn, can result in the diverse cybersecurity workforce of the future.

In Section 2, an overview of the curriculum development of the KSU GenCyber camp is presented. Section 3 presents the implementation of the camp. Section 4 presents the evaluations and outcomes of the camp. The paper is concluded by presenting the discussion and conclusion in Section 5 and Section 6, respectively.

2. CURRICULUM DEVELOPMENT

2.1 Institutional Background and Program Goals

Eight professors hosted this GenCyber program at KSU – a large public university designated as a National Center of Academic Excellence in Cyber Defense Education (CAE/CDE). The current camp catalog indicates that institutions of various sizes and types can obtain GenCyber funding (DoD, 2025), so when developing our teaching tips and lessons learned we made sure they are generalizable and can be utilized at other institutions.

Aligning with the GenCyber program's main goals, the KSU GenCyber camp aimed to:

- Increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation.
- Enable all learners to understand cyber ethics and best practices.
- Enable learners to pursue cybersecurity-related programs.

Furthermore, the program was designed to recruit high school students from underrepresented minority groups without any prior GenCyber experience or limited knowledge of cybersecurity, computers, and technology. We believed that doing so would increase interest and student diversity in the cybersecurity workforce and educational program. Hence, our goals matched with the goals of the GenCyber program while contributing to closing the gap of the nation's cybersecurity professional shortage.

2.2 Program Development

We utilized ELT (Figure 1) developed by Kolb (1984) to guide

the development of the GenCyber program and to ensure it provides students with relevant and meaningful learning opportunities. ELT is a holistic framework that describes how individuals learn through direct experience. Kolb's model (1984) suggests that learning is an ongoing process that involves four key stages: concrete experience, reflective observation, abstract conceptualization, and active experimentation. These stages are interconnected and cyclical, forming the "Experiential Learning Cycle." Before engaging in the ELT cycle, we introduced students to the program through a virtual orientation. This included an overview of the camp structure, expectations, and available resources. Students were familiarized with the learning management system and introduced to faculty and staff. This phase helped establish a foundation for engagement and set the stage for experiential learning. The following is a description of each stage and what activities we performed.

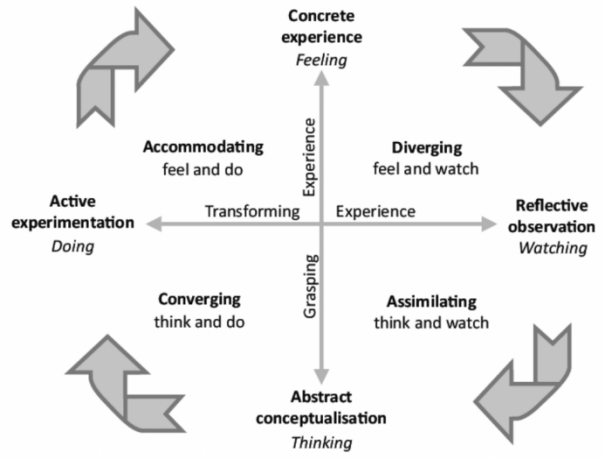


Figure 1. Experiential Learning Theory

- Concrete Experience (CE): This stage involves direct, hands-on experiences or encounters with phenomena in the real world. To provide authentic firsthand experiences, we engaged students in interactive cybersecurity labs using NetLab, where they explored real-world scenarios such as network breaches and forensic investigations. These activities allowed students to actively participate in cybersecurity tasks and gain practical exposure to the field.
- Reflective Observation (RO): After engaging in hands-on labs, students reflected on their experiences through asynchronous online discussions, quizzes, and collaborative activities. They shared insights, discussed challenges, and analyzed their learning outcomes. This stage enabled students to process their experiences and connect them to broader cybersecurity concepts.
- Abstract Conceptualization (AC): In this stage, learners developed a deeper understanding of cybersecurity principles by connecting their experiences to theoretical frameworks. During the in-person component of the camp, instructors delivered lectures on cryptography, risk management, ethics, and other core topics. Students synthesized these concepts and integrated them with their prior experiences.
- Active Experimentation (AE): Finally, students applied their knowledge in new contexts through advanced lab exercises and interactive sessions with guest speakers. These activities encouraged experimentation, problem-solving, and the application of cybersecurity strategies in simulated environments. Students received feedback and iterated their approaches, reinforcing their learning through practice.

While each stage of the cycle can be repeated, we had a limited amount of time, only one week of in-person interaction, to complete all four stages. In a semester-long course format, we recommend instructors utilize the iterative aspect of ELT to better support learning outcomes. We chose to utilize the Kolb model (1984) for our GenCyber student camp because effective learning occurs best when individuals actively engage with their experiences, critically reflect on them, make meaning through conceptualization, and apply their understanding in practical contexts. By engaging in experiential learning, students develop not only knowledge and skills but also deeper insights, self-awareness, and the ability to adapt and learn from their experiences.

2.3 Instructional Materials and Methods

The KSU GenCyber program covered topics aligning with Georgia's High School curriculum guidelines and High School Cybersecurity Curriculum Guidelines (2021) from TeachCyber to provide a well-balanced perspective of the cyber domain. The goal was for each of the participants to have sufficient knowledge to complete the onsite workshop activities. The seven module areas included fundamentals of cybersecurity, ubiquitous connectivity for cybersecurity, data security fundamentals, system security fundamentals, risk management, cyber ethics, and cyber career paths. The program delivered knowledge and activities on the seven module areas as follows:

- Fundamentals of Cybersecurity - Delivered through lectures and quizzes, this module introduced foundational concepts such as defense in depth, CIA triad, and adversarial thinking. These activities supported AC by helping students build a theoretical framework.
- Ubiquitous Connectivity for Cybersecurity - Students explored Internet architecture, network protocols, and security technologies through lectures and quizzes (AC), followed by hands-on labs using the NetLab NISGTC Network. These labs provided CE through real-world simulations and AE as students applied concepts in interactive environments.
- Fundamentals of Data Security - Covered encryption, Python programming, data integrity, and access controls. Lectures and discussions supported AC and RO, while hands-on exercises and coding tasks reinforced CE and AE.
- Fundamentals of System Security - Focused on hardware/software vulnerabilities, malware, and digital forensics. Lectures supported AC, NetLab-based labs offered CE and AE, and post-lab reflections contributed to RO.
- Fundamentals of Risk Management - Introduced risk modeling, threat analysis, and vulnerability scanning. Students engaged in CE and AE through tool-based

assessments, while lectures and discussions facilitated AC and RO.

- Cyber Ethics - Delivered through curated lectures, interactive discussions, and quizzes. These activities supported RO and AC by encouraging ethical reflection and conceptual understanding.
- Cybersecurity Career Paths - Included guest speakers, resume-building, and job exploration activities. These sessions supported CE through real-world engagement and AE as students applied insights to career planning.

By aligning each module with specific ELT stages, the program guided students through the full cycle—CE → RO → AC → AE—to reinforce both theoretical knowledge and practical skills in cybersecurity.

2.4 Program Model

The KSU GenCyber Camp was hosted as a hybrid camp, divided into three phases: pre-workshop, on-campus workshop, and post-workshop. The camp was designed to provide 60 hours of instruction, with 15 hours of pre-workshop activities, 30 hours of on-campus workshops, and 15 hours of post-workshop activities.

The extended timespan between these phases was intentional. It allowed students to gradually build foundational knowledge before the in-person experience, and to reinforce and apply their learning afterward. This structure supports spaced learning, which can enhance retention and engagement (Kondratjew & Kahrens, 2019). However, we acknowledge that long breaks may pose challenges in maintaining continuity and student motivation, which we addressed through regular communication and structured assignments.

The on-campus workshop included 14 lecture topics, 12 hands-on lab sessions, and 5 guest speaker sessions. These activities were directly aligned with the seven module areas: fundamentals of cybersecurity, ubiquitous connectivity, data security, system security, risk management, cyber ethics, and cybersecurity career paths. Each lecture and lab session were mapped to one or more of these modules to ensure comprehensive coverage and coherence. Guest speakers were selected to complement the module topics and provide real-world context and professional insights.

The pre-workshop phase began during late Fall 2022-Spring 2023. Learners were invited to a virtual program orientation event given in late Fall 2022, where they were provided access to the KSU Learning Annex system and an overview of how to navigate resources. Pre-workshop activities were led by eight highly qualified professors (Ph.D.) from the Department of Information Technology and the Department of Information Systems & Security in the College of Computing and Software Engineering and the College of Business at Kennesaw State University. The online activities were hosted in the Annex learning management system (LMS) with seven different modules and thirteen topics.

The 30-hour on-campus GenCyber Camp at KSU was during the Summer of 2023 (June) where 30 hours of instruction consisted of 14 different lecture topics, 12 hands-on lab sessions, and 5 guest speaker sessions. The team leveraged KSU resources like NetLab to enable learners to practice the concepts using a hands-on approach.

The post-workshop took place from Fall 2023 to Spring 2024 to engage participants with activities related to workshop lesson plans, which included specific assignments related to subject topics and career development. All participants were enrolled as part of a Listserv mailing group for future communication on opportunities such as degree programs, scholarships, and opportunities related to cybersecurity.

2.5 Assessment Strategies

Assessment of learning modules was performed by discussion, auto-graded quizzes, and attendance or completion of items. We used NetLab resources which come with a virtual cyber range environment having computers, software, and networks to access from anywhere. The students were allowed to look up resources during the assessment, and the focus was to enable group learning and hands-on activities. In addition, the team did pre- and post-workshop surveys to ensure learners had increased interest in pursuing cybersecurity careers and future degree programs at KSU or other schools offering cyber programs. Section 4 covers the evaluation of the assessment of pre- and post-workshop surveys in detail.

3. IMPLEMENTATION OF KSU GENCYBER PROGRAM

3.1 Student Recruitment

The program targeted high school students from grades 9 to 12, giving priority to students from underrepresented groups and students who never participated in a GenCyber camp before. Efforts were made to recruit a balanced number of male and female students. Participant applicants must meet the following criteria:

- Be a U.S. citizen or permanent resident.
- Have a minimum GPA of 3.00.
- Have not participated in a previous GenCyber program.

To recruit the greatest number of minority students possible, efforts were made to heavily advertise the program in the most diverse high schools in Georgia. Recruitment took place in three forms: (i) printed brochures mailed to high school principals in Cobb County, Fulton County, Gwinnett County, Douglas County, Dekalb County, Cherokee County, and others within the university's 20-county service area; (ii) emails sent to over 500 high school advisement counselors and instructors in the region – the email campaign consisted of initial notification and regular update communications; and (iii) a program website set up in KSU website (https://www.kennesaw.edu/coles/centers/cyber-center/events/gencyber.php) and press releases from institutional university relations staff disseminated electronically.

Interested students were required to submit an electronic application that included student information (name, address, contact information, gender, ethnicity), parent or legal guardian information (name, contact information), school performance information (school name, grade, GPA, disclose of prior participation in GenCyber), supporting teacher/counselor reference (name, contact information, course), unofficial copy of transcripts, and a statement from the student describing why they are interested in participating in the program. Interviews were conducted for the preliminary group of students.

3.2 Selection

By the end of the recruitment process, we received a total of 118 applications from four different school districts in the Atlanta Metropolitan area. The applications were then sorted and normalized into a consistent format based on the information provided by the students. The program coordinators then reviewed and chose the top applications based on the student's GPA, statement of interest, and levels of exposure to technology. The top 66 applicants were selected with priority consideration given to students from underrepresented minority groups or with no prior GenCyber experience. The acceptance rate of the program was 55% in its first year and we are optimistic that student interest would remain strong if the camp is offered on an annual basis.

From the final number of 66 selected candidates for the KSU GenCyber camp, 19 students were female and 47 were male, with the respective percentage of 29% to 71% (Figure 2). The selected students were from 11 schools and three different school districts. The majority of the selected students were from 9th grade (34.85%) followed by 28.79% from each of 10th and 11th grade, respectively (Figure 3). Of the selected students, 31.82% chose "1" as their cybersecurity comfort level, where levels 2-6 were in the range of 10%-15%. Only 4.55% of the candidates chose the highest level 7. 10.61% of the students identified themselves as Caucasian and 72.73% represented minority groups (37.88% Black or African American, 22.73% Asian, 10.61% Hispanic or Latino, and 1.52% American Indian or Alaska Native) (Figure 4).

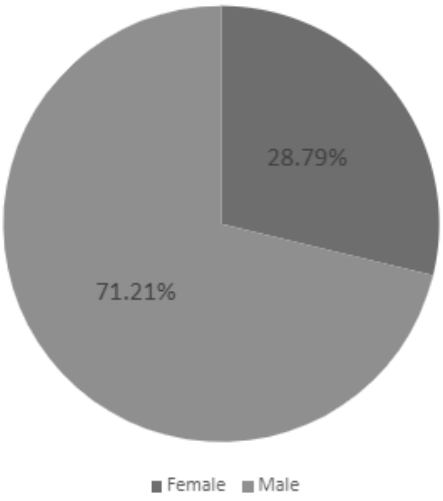


Figure 2. Gender Makeup of Participants

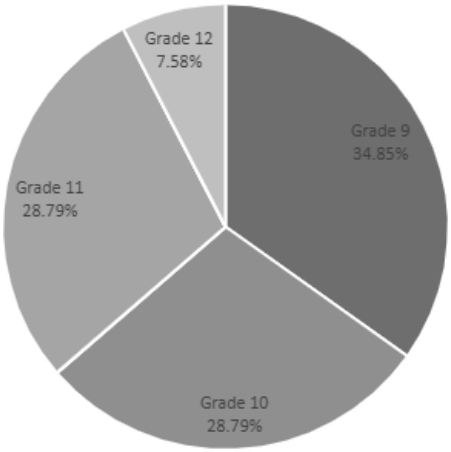


Figure 3. Participants by Grade Levels

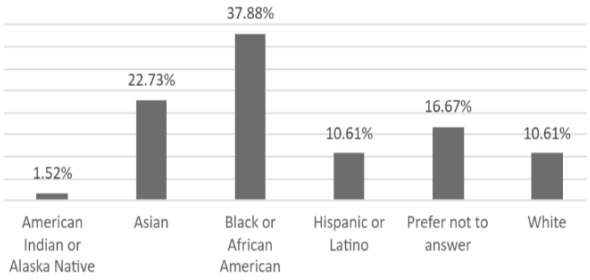


Figure 4. Racial Makeup of Participants

3.3 On-Campus GenCyber Camp at KSU

The official KSU GenCyber camp was hosted at the College of Computing and Software Engineering at KSU. The program was from June 5th-9th from 8:00 AM to 4:00 PM each day. Program staff were at the camp at 7:30 AM each day, and students were welcomed on-site as early as 7:45 AM each day for time to settle and have breakfast before class. Each day, breakfast, lunch, and break sessions were conducted. Class began at 8:00 AM with a 15-minute break every two hours.

To provide a clearer picture of how the on-campus workshop was structured, the five-day on campus schedule is available in Appendix A. It outlines the integration of lectures, hands-on labs, and guest speaker sessions, demonstrating how different instructional formats were combined to enhance student engagement and learning outcomes. This variety of activities we had kept students engaged and allowed them ample time to absorb and apply the material.

4. OUTCOME ASSESSMENT

Assessment of learning modules was performed by discussion posts, auto-graded quizzes, and attendance or completion of items. Assessments were given to the students to investigate the effectiveness of the program in two phases: pre-camp workshop and on-campus workshop with the purposes of (i) monitoring students' progress and engagement rate; (ii) evaluating

students' understanding of the material; (iii) improving the curriculum of the program and documenting the impact that the GenCyber program has on the students. We combined and evaluated two types of assessments: pre-workshop assessment and in-person survey. The pre-workshop assessment consisted of all the discussion posts, quizzes, and assignments in seven modules within the Annex LMS. This assessment was evaluated to monitor students' progress and engagement rate while assessing their understanding of the materials in the pre-workshop phase, which was conducted virtually. The in-person survey was conducted during the GenCyber camp at KSU. The survey was a combination of a pre-camp survey and a post-camp survey, which were conducted at the beginning of the in-person and the end of the camp, respectively.

4.1 Pre-Camp Workshop Assessment

Pre-camp workshop was hosted virtually for 15 hours on the KSU Annex LMS. Of the 66 students who were accepted into the program, 58 ultimately participated in the pre-camp and on-campus activities. The remaining seven students were unable to attend due to personal scheduling conflicts, transportation challenges, or changes in summer plans. The final 58 students participated at their own pace in reading articles, watching video-recorded lectures and slides, completing activities, and taking quizzes in each module. The assessment for pre-camp workshop focused on evaluating the engagement rate of the participants in each module. This includes evaluating the engagement rate and student participation by views in each activity, depth of input answers in discussion posts, and average quiz scores for activities.

We analyzed students' performance in each of the seven camp modules. Table 1 provides information about the view counts for activities in each module, demonstrating a consistent student interest. Table 2 depicts the average scores students achieved for the Ubiquitous Connectivity for Cybersecurity module. The maximum score students could get was 100; overall, they demonstrated a good comprehension of the material (72.73%) given the short timeframe of the camp. Table 3 shows positive results for the engagement and depth of students' inputs for discussion posts in two camp modules where students' engagement and participation were demonstrated through the view counts and high averages for replies and word counts. Teaching software fundamentals is inherently challenging, so in the future, we recommend using additional materials and resources to support students' learning when it comes to vulnerability analysis. We also suggest integrating generative AI tools into some modules to introduce students to these technologies and demonstrate how they can be successfully used to achieve various learning outcomes.

4.2 GenCyber Camp Survey

To measure learning objectives and student success, we administered a short pre- and post-survey at the beginning and the end of the in-person camp activities. We adapted the survey instrument developed by Giboney et al. (2023). Our survey consisted of four items (see Appendix B for more details). Following is an explanation of each one in the context of Bloom's taxonomy (Bloom et al., 1956). We utilized this framework because it provides a structured guideline for educators to design learning objectives that promote higher order thinking, enabling students to progressively develop deeper understanding and mastery of a subject.

Question 1 presented students with eight different stories and six principles of cybersecurity that GenCyber focused on - defense in depth, integrity, confidentiality, thinking like an adversary, availability, and ethics. The students were asked to match each principle to the story or stories that fit(s) the principle the most. This question relates to the concept of understanding or constructing meaning from written material or graphics. The second question asked students about their interest in cybersecurity. We used this question to understand participants' needs and how they related to the GenCyber camp. This is again a demonstration of understanding. The third question asked students to list some personal reasons for choosing cybersecurity as a career. This is an example of applying a concept because it is asking students to use information in a new situation, since they may not have been exposed to cybersecurity careers before. Finally, the fourth question asked students to match 13 security terms into offensive or defensive security categories. This activity relates to both understanding and application of knowledge, because it shows whether students can meaningfully distinguish between the two categories and classify the provided terms.

We saw the most increase in the first and fourth questions because they required a demonstration of specific knowledge. Interest in cybersecurity remained almost unchanged and we explain this phenomenon with the short amount of time between the two surveys (only five days). Students who are already interested in cybersecurity are more likely to apply and complete the GenCyber camp. Although we did not see a significant change in this pre- and post-camp score, we believe that a longitudinal study might have a much more significant effect. When analyzing question 3, we only counted the number of reasons students gave without assigning any particular value to them. Similar to question 2, we expect to see a much larger difference after some time, rather than immediately upon completing the camp. However, questions 2 and 3 were helpful to better understand the students' mindsets, their interest in the field, and their career expectations. We used that data to customize our content and ensure the activities offered resonated with students' experiences.

Table 4 shows the average score for each question for pre-camp and post-camp surveys. We also conducted a paired t-test to evaluate the statistical significance of the observed differences in pre-camp and post-camp scores. The t-statistic value is 2.1655 and the p-value is 0.1190. Although the post-camp scores were consistently higher across most questions, the difference was not statistically significant at the conventional 0.05 level. This outcome may be attributed to the small number of survey questions ($n = 4$). However, the survey instrument we used has been previously validated by Giboney et al. (2023) and is one of the few specifically available scales to measure GenCyber outcomes. We acknowledge this limitation and plan to incorporate a more robust evaluation framework in future iterations of the camp, including larger sample sizes and additional assessment items to strengthen the validity of our findings. Additionally, we recommend others to also consider more interactive survey forms, because they can actively engage students, provide real-time feedback, assess understanding, personalize learning experiences, and foster student participation, ultimately improving both teaching effectiveness and learning outcomes.

Overall, we observed a positive trend in students' knowledge during the short, five-day, GenCyber camp. We

encourage others to continue collecting data and examine long-term knowledge acquisition. Our survey instrument builds upon prior work (Giboney et al., 2023) and our results add value by empirically validating prior scales and adding new ways of measuring GenCyber learning objectives.

Module Name	Syllabus	Module Overview	Slides	Lecture Videos	Quizzes	Activities
Fundamentals of Cybersecurity	115	101	145	72	1,179	0
Ubiquitous Connectivity for Cybersecurity	116	50	530	107	0	2,981
Fundamentals of Data Security	50	0	193	51	1,044	0
Fundamentals of System Security	22	30	100	71	1,592	174
Fundamentals of Risk Management	111	0	175	98	1,038	N/A
Cyber Career Paths	80	N/A	121	60	N/A	878
Cyber Ethics	27	20	78	45	N/A	738

Table 1. View Counts for Activities of Each Module

Ubiquitous Connectivity for Cybersecurity Module Activities	Average Activity Score
Your name in tag	78.18%
Network command	78.18%
Malware definitions	81.82%
Vulnerability analysis	52.73%
Average module score	**72.73%**

Table 2. Average Score for Activity

Module Name	Discussion Name	No. of Discussion Posts	Average Word Count	Average No. of Replies	Views
Cyber Career Paths	Cyber career goals	37	202	2	880
Cyber Ethics	Cyber ethics discussion	38	213	2	752

Table 3. Analysis of Discussions

Question No.	Average Score	
	Pre-Camp	Post-Camp
1	3.857	4.085
2	2.479	2.476
3	2.705	2.957
4	7.941	8.541

Table 4. Average Scores for Each Question for Pre-Camp and Post-Camp Surveys

5. DISCUSSION, LIMITATIONS, AND LESSONS LEARNED

While the presented GenCyber program was overall a success, there are certain limitations to the teaching tip provided. This was our first time running the school camp, so we encountered some challenges in the beginning. For example, we did not have a classroom large enough to accommodate all students, so we had to use an overflow room and either assign another instructor or project in real time the lab being conducted in the other classroom. Students had to follow the instructions on their own and the instructor would only come at the end to assist and answer any questions. This logistical problem can be avoided in the future by hiring additional instructors or using larger classrooms, if available.

There are also no established scales to measure the effectiveness of the GenCyber camp. While the survey we used was based on prior work (Giboney et al., 2023), we modified it according to the specific modules and objectives of our own program. In the future, we encourage our colleagues to establish a standardized tool for this purpose so that various camps across the country can measure and compare their outcomes based on the same survey instrument.

Another key takeaway from our experience was the need for curriculum flexibility. The rapid pace of technological change in cybersecurity requires continuous updates to the curriculum. The feedback from students and instructors indicated a desire for more real-time case studies and the inclusion of emerging topics such as artificial intelligence in cybersecurity and ethical hacking. Incorporating adaptive learning technologies can also allow for more personalized learning experiences, catering to the diverse knowledge levels and backgrounds of students.

The success of the KSU GenCyber camp highlights the potential of targeted educational initiatives to bridge the gap between K-12 education and cybersecurity career pathways.

However, to make a lasting impact on the cybersecurity workforce, these efforts must be sustained and scaled. Partnerships with local industries, government agencies, and higher education institutions can provide students with continuous learning opportunities and mentorship. Additionally, expanding the reach of GenCyber programs to include middle school students could cultivate an even earlier interest in cybersecurity, potentially leading to a more diverse and skilled workforce in the future.

Our work is proof of concept, and it demonstrates that combining a solid theoretical foundation such as Experiential Learning Theory and Bloom's Taxonomy with practical, hands-on activities can support student success through engaging and interactive activities and exercises. We encourage others to continue utilizing theory and positively impact their communities through projects like GenCyber.

6. CONCLUSION

One of the key lessons learned from this experience is the importance of creating an inclusive environment that supports students from diverse backgrounds. The success of our recruitment efforts, which resulted in over 72% of participants identifying as minorities, underscores the effectiveness of targeted outreach and engagement strategies. However, fostering long-term interest in cybersecurity among these students requires more than just initial exposure. It involves ongoing mentorship, access to resources, and opportunities for continued learning beyond the camp. Future GenCyber programs can provide a sustainable pipeline of diverse talent into the cybersecurity workforce by building solid partnerships with local schools, community organizations, and industry leaders. Additionally, incorporating culturally responsive teaching practices can enhance the relevance and impact of the curriculum, ensuring that all students feel valued and supported in their educational journeys.

7. ACKNOWLEDGEMENTS

Research reported in this publication was supported by the National Security Agency under Award Number H98230-22-1-0117. The content is solely the responsibility of the authors and does not necessarily represent the official views of the National Security Agency.

8. REFERENCES

Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (Eds.) (1956). *The Taxonomy of Educational Objectives: Classification of Educational Goals. Handbook I: Cognitive Domain.* New York: Longmans.

CyberSeek.org. (2024). *Cybersecurity Supply and Demand Heatmap*. https://www.cyberseek.org/heatmap.html

Department of Defense (DoD). (2025). *DoD Cyber Exchange*. https://public.cyber.mil/gencyber/camp-catalog/

Fortinet. (2023). *2023 Security Awareness and Training*. Fortinet Training Institute. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-security-awareness-and-training.pdf

Georgia Department of Education. (2023). *Title I, Part A - Improving the Academic Achievement of the Disadvantaged*. https://www.gadoe.org/School-Improvement/Federal-Programs/title-i/Pages/Disadvantaged-Children.aspx

Giboney, J. S., Dincelli, E., Wright, G., Taylor, Q., & Christensen, D. (2023). The Youth Cybersecurity Concepts Instrument (YCCI): Developing a Scale for the GenCyber Cybersecurity Concepts. *In Proceedings of 2023 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop.* June 22-23, 2023, Glasgow, Scotland, UK.

High School Cybersecurity Curriculum Guidelines. (2021). TeachCyber. https://teachcyber.org/cybersecurity-teaching-resources/curriculum-guidelines/

Hellmann, K. (2023). *See Yourself in Cybersecurity*. U.S. Department of Labor Blog. https://blog.dol.gov/2023/09/22/see-yourself-in-cybersecurity#::text=The\%20cybersecurity\%20field\%20is\%20booming

ISC2. (2023). How the Economy, Skills Gap and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce. *ISC2 Cybersecurity Workforce Study*. https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

Kolb, D. A. (1984). *Experiential Learning: Experience as the Source of Learning and Development*. Prentice-Hall, Upper Saddle River, NJ.

Kondratjew, H., & Kahrens, M. (2019). Leveraging Experiential Learning Training Through Spaced Learning. *Journal of Work-Applied Management*, 11(1), 30-52. https://doi.org/10.1108/JWAM-05-2018-0011

Lachow, I. (2022). *Diversity in the Cyber Workforce: Addressing the Data Gap*. https://www.mitre.org/news-insights/publication/diversity-cyber-workforce-addressing-data-gap

National Security Agency. (2024). National Centers of Academic Excellence in Cybersecurity. *National Security Agency/Central Security Service*. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence

The EdWeek Research Center. (2020). *The State of Cybersecurity Education in K-12 Schools: Results of a National Survey*. https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf

Yaacob, M. N., Idrus, S. Z. S., & Idris, M. (2023). Managing Cybersecurity Risks in Emerging Technologies. *International Journal of Business and Technopreneurship*, 13(3), 253-270. https://doi.org/10.58915/ijbt.v13i3.297

AUTHOR BIOGRAPHIES

Anh Duong holds a B.S. in computer science from Kennesaw State University. She was the inaugural recipient of the President's Award at KSU in recognition of her outstanding contributions to research and leadership. Her interests include cybersecurity education, outreach in underserved communities, and student leadership development.

Maria Valero is an associate professor in the College of Computing and Software Engineering, Department of Information Technology at Kennesaw State University. She earned her Ph.D. in Electrical and Computer Engineering from the University of Georgia. Dr. Valero directs the IoT as a Service Research Group, where her work explores sensor-based technologies for cybersecurity and healthcare. She has led NSA-funded cybersecurity education initiatives, including GenCyber camps, and serves as Principal Investigator on NSF and NIH awards focused on remote health monitoring and device innovation.

John Ethan Oakley holds a B.S. in information technology from Kennesaw State University. He has been recognized by the Office of Research for his contributions to scientific research. His interests include cybersecurity, applied data science, and promoting undergraduate research engagement.

Miloslava Plachkinova is the Assistant Department Chair and an associate professor of information security and assurance at Kennesaw State University. Her research interests include behavioral information security, cybercrime, and the legal and policy implications of cybersecurity. Her work has been published in top journals such as the *Journal of the Association of Information Systems*, *Information Systems Frontiers*, and the *Journal of Information Systems Education*. Dr. Plachkinova holds numerous professional certifications, including CISSP, CCSP, CISM, CISA, CDPSE, CRISC, CIPP/US, and PMP.

APPENDICES

Appendix A. GenCyber Camp Program

KSU GenCyber Student Camp 2023 Schedule
June 5th - June 9th 2023; Atrium Building

Session	Monday (6/5)	Tuesday (6/6)	Wednesday (6/7)	Thursday (6/8)	Friday (6/9)
7:45am-8am	Arrival to Atrium (J161)	Arrival to Atrium (J215B, J217)	Arrival to Atrium (J215B, 217)	Arrival to Atrium (J215B, 217)	Arrival to Atrium (J215B, 217)
8:00 am - 8:30 am	Welcome (Program Directors and Others)- J161	Introduction to Linux (Dr. Shahriar)	Introduction to devices - Raspberry PI (Dr. Bob Brown)	Recover information, analyze memory, disks, software (Dr. Valero)	Network Cybersecurity (Dr. Zhao)
8:30 am - 9:00 am	Orientation, Schedule, Particpnats Introduction (J161)	Lab - Practicing Linux Commands (Dr. Shahriar)	Introduction to devices - Raspberry PI (Dr. Bob Brown)	Lab - Netlab - Recovery (Dr. Valero)	Lab 11 - Scanning networks (Dr. Zhao)
9:00am - 10am	Fundamental of Cybersecurity (Dr. Li) Lab 1 + Discussion (J161)	Lab - Practicing Linux Commands (Dr. Shahriar)	Lab - Raspberry PI Practice (Dr. Brown and Mr. Kassif)	Lab - Netlab - Recovery (Dr. Valero)	Lab 11 - Scanning networks (Dr. Zhao)
10am - 10:15am	**BREAK**	**BREAK**	**BREAK**	**BREAK**	**BREAK**
10:15am - 11am	Access to computer, Ubiquitous Connectivity for Cybersecurity (Dr. Valero)	Cryptography - (Dr. Zhao)	Lab - Raspberry PI Practice (Dr. Brown and Mr. Kassif)	Lab - Netlab - Recovery (Dr. Valero)	Lab 11 - Scanning networks (Dr. Zhao)
11am - 11:30am	Lab - Internet, adversary, security issues (Dr. Valero)	Lab - Cryptography lab (Dr. Zhao)	Lab - Raspberry PI Practice (Dr. Brown and Mr. Kassif)	Fundamentals of System Security (Dr. Shahriar)	Guest Speaker - Dark web crawling (Juan Rodriguez)
11:30am - 12pm	Lab - Internet, adversary, security issues (Dr. Valero)	Lab - Cryptography lab (Dr. Zhao)	Lab - Raspberry PI Practice (Dr. Brown and Mr. Kassif)	Lab- Netlab- Computer Forensics (Dr. Shahriar)	Guest Speaker - cyber profession (Phillip Mahan)
12pm - 12:30 pm	Lab - Internet, adversary, security issues (Dr. Valero)	Guest Speaker (Keyaan Williams)	Lab - Raspberry PI Practice (Dr. Brown and Mr. Kassif)	Lab- Netlab- Computer Forensics (Dr. Shahriar)	Guest Speaker - cyber profession (Phillip Mahan)
~~12:30pm 1:30pm~~	LUNCH (Stinger Restaurant)				
1:30pm-2pm	Finishing Lab (Dr. Valero)	Fundamentals of risk management - Threat, Vulnerabilities, and Assets (Drs. Whitman, Mattord)	Data security and privacy (Dr. Pouriyeh)	Cybersecurity Careers (Drs. Whitman, Mattord)	Guest speaker- Cyber Apprenticeship for Freshman (Stephen Gay)
2pm - 2:30pm	CyberEthics Discussion (Dr. Plachkinova)	Fundamentals of risk management - (Drs. Whitman, Mattord)	Lab - Methods for data security (Dr. Pouriyeh)	NICE Workforce Cybersecurity (Drs. Whitman, Mattord)	Guest speaker- Cyber Apprenticeship for Freshman (Stephen Gay)
2:30pm - 3:15pm	Lab - Professional Obligations (Dr. Plackkinova)	Lab - Cyber Threats Practicum (Dr. Whitman)	Lab - Methods for data security (Dr. Pouriyeh)	Lab - Cyber Threats Practicum, Part 2(Dr. Whitman)	Guest speaker- Cyber Apprenticeship for Freshman (Stephen Gay)
3:15pm - 3:30pm	BREAK	BREAK	BREAK	BREAK	BREAK
3:30pm - 4pm	T-Shirt and Goodies Distribution	Guest Speaker - Deanna House (Cyber Ethics)	Lab - Methods for data security and review (Dr. Pouriyeh)	Q&A about professions	Closing Remarks; Required Survey
4:00pm	End of Session - Day1	End of Session - Day2	End of Session - Day2	End of Session - Day4	End of Session - Day5

Appendix B. GenCyber Camp Survey Instrument

1. As part of the 2023 GenCyber Camp at KSU, we want you to learn six ideas. It's fine if you don't know what they are or even ever heard of these terms. Can you draw a line from the ideas on the left to the stories on the right without help from a friend?

Some ideas have more than one story, and some stories don't have an idea.

Defense in depth	Tanisha has a password for the dairy on her computer.
Integrity	Malik makes sure his brothers don't change the time on his alarm clock.
Confidentiality	Brandon looks for a back door at his school that is always unlocked.
Think like an adversary	Klara uses three different types of locks to secure her bike.
Availability	Andre has a backup phone in case his first one doesn't work.
Ethics	Maria uses a helmet and kneepads when skating.
	Michael is trying to access his sister's phone password to see her texts without permission.
	Angie always asks an adult to help when using the Internet.

2. How interesting is cybersecurity? Circle one of the choices below.

Not at all A little A lot

Page 1 of KSU GenCyber Camp Survey

3. What are some reasons people choose a cybersecurity career? Name as many as you can think of.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

4. Put the following terms into offensive or defensive security categories. Some terms may not belong in either category.

Encryption

Exploits

Risk management

Network protocols

Ethical hacking

System hardening

Backups

Defense-in-depth

Trojan horse

Fake news

Secure app development

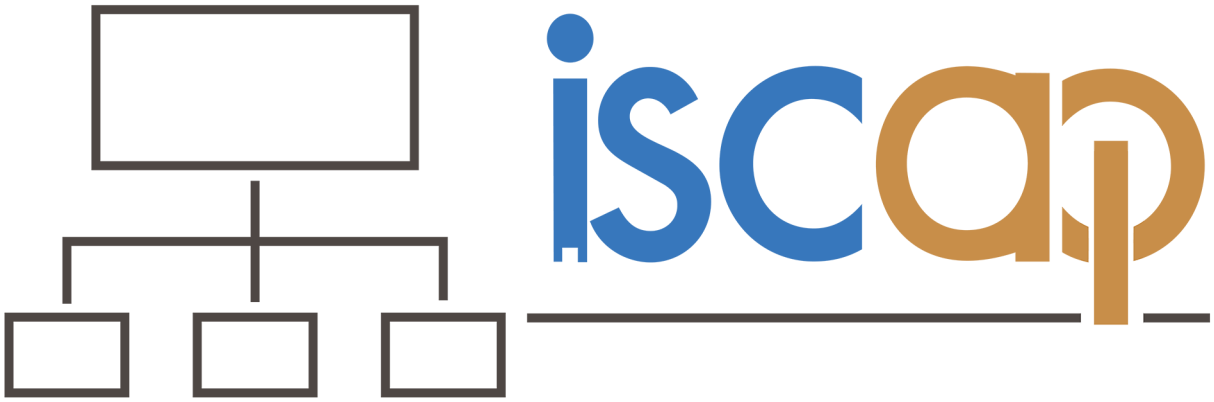
Door locks

Internet of Things (IoT)

OFFENSIVE SECURITY

DEFENSIVE SECURITY

INFORMATION SYSTEMS & COMPUTING ACADEMIC PROFESSIONALS



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)