Applied Human Factors and Ergonomics (AHFE2025), Vol. 199, 2025, 2326–2333
https://doi.org/10.54941/ahfe1007045

Engaging K-12 Students With Real-World Experiences From Cybersecurity Professionals

Sandra B. Nite[1], Halle W. Gray[1], Wesley A. Brashear[1], Seonhu Lee[2], and Dhruva K. Chakravorty[1]

[1]Texas A&M University, College Station, TX 77843, USA
[2]University of Texas, Austin, TX 78712, USA

ABSTRACT

Cybersecurity is a topic of critical importance in our world today, and it is increasingly important for middle school and high school students to learn the concepts of cybersecurity. At this point in time, students are not required to take a course in cybersecurity, although it is available as an elective in some schools. They are often given only bits and pieces of information about cybersecurity and personal safety at school. Thus, summer camps focused on cybersecurity are a great way for students to learn more about this topic. In summer camps at Texas A&M University, students learned about cybersecurity through experiential learning in safe environments, games, lectures, and presentations from university faculty and cybersecurity professionals. In this paper, we focus on the presentations from cybersecurity professionals from various university departments and from outside the university. We identify six cybersecurity concepts: availability, keeping it simple, defense in depth, confidentiality, thinking like an adversary, and integrity. We describe some of the presentations that students heard that illustrated these concepts and how they applied to students' lives. Some of the presentation topics we discuss center around safe online behavior, social engineering, and cyber attacks. In addition, the increasing need for cybersecurity professionals in many different fields was shared with students, along with several different pathways to take towards those careers. We provide the results from students' daily reflections about their learning from these presentations. The results include frequencies from multiple-choice questions about the level of learning they gained from the presentations and free response questions for which they chose an activity or presentation as their greatest learning opportunity of the day, and explained what they learned. Finally, we discuss how the camp experience and knowledge gained by students is an important part of their learning regarding cybersecurity, with suggestions about carrying on the work of educating secondary students about cybersecurity is important in decisions they make regularly in their lives.

Keywords: K12 engagement, K12 summer camp, K12 cybersecurity education

INTRODUCTION

As members of a digital society, we all understand that cybersecurity affects our lives every day in many ways. To remain cyber-safe, individuals must

have some knowledge about how to navigate the digital world safely. Thus, people of all ages who have contact with digital devices need to know what it means to keep digital information confidential, available when it is needed, and something about how cyber criminals think and operate (i.e., thinking like an adversary). Individuals want to know that their digital records have not been tampered with (i.e., data integrity), but also to have a system of safekeeping that is simple but multilayered (e.g., passwords in conjunction with texted or emailed verification codes).

Cybersecurity education should begin as soon as children become acquainted with digital devices, at an age-appropriate level. Students in middle school and high school are capable of learning quite a lot about cybersecurity, but they are not often exposed to enough learning to gain the understanding they need to deal with cybersecurity issues. Summer camp experiences can have an effect on students' knowledge and interest in cybersecurity applicable to their daily lives (Sudha et al., 2023).

A second reason to provide cybersecurity education for students is that there is a shortage of cybersecurity professionals in the United States and across the globe. Students should learn about the range of careers in cybersecurity that are available today as they begin to explore various college majors. Educating high school students who are thinking about their future educational and career plans can help increase interest in cybersecurity careers and recruit students to choose a career path involving cybersecurity (Ileleji and Joseph, 2018; Hossain et al., 2024). High Performance Research Computing (HPRC) at Texas A&M University has been hosting data science and cybersecurity summer camps for secondary students since 2017. They have reported on their work and methods in the areas of computational thinking (Chakravorty et al., 2020), data science (Chakravorty et al., 2022), teaching Python (Brashear et al., 2025), Project-Based Learning (Nite et al., 2025), and strategies to engage students in cybersecurity education (Nite et al., 2024). This paper adds to that research by exploring the aspect of guest lecturers by cybersecurity professionals and how these sessions add to students' knowledge and interest in cybersecurity.

METHODOLOGY

In the summers of 2023 and 2024, High Performance Research Computing (HPRC) at Texas A&M University hosted a total of five (5) week-long camps focused on cybersecurity. The curriculum consisted of a mix of games, hands-on activities, Python programming interactive lessons, tours, guest speaker lecture, and a final secure system design team project. Throughout the week students had opportunities to work individually and in groups. Table 1 shows a sample schedule for a week of the camp.

To keep students engaged, a variety of educational strategies were used. As students arrived, they checked out a laptop for the day and spent a few minutes talking with their project teams. After everyone settled, the day began with a game to reinforce cybersecurity concepts and have a little fun. After getting their adrenaline going with the game, the morning activities were usually those where the most focus was needed. This was planned because they would be fresh after a little warmup. Most activities and lectures were interactive, with students engaged in answering questions from the

speaker or doing coding along with the Python instructor. The most active sessions, in which students were physically moving around, were planned in the afternoon when many people tend to become a little drowsy at times.

In addition to the logistics of the schedule to facilitate engagement, we used the results of our study of student reflections from summer camps to design activities and lectures that have been shown to increase engagement. One of those strategies is to use real-life situations (Nite et al., 2024). With cybersecurity, it is easy to use real-life situations because it is part of our everyday lives. We hear about cyber attacks often, and we encounter social engineering instances in many areas of our digital encounters. The lecture on social engineering that will be described later was engaging to students because it was real and because it gave them information they had not known before. This was mentioned by the majority of students when asked what they had learned most from that day.

Peer collaboration and problem solving are two other items that can increase student engagement in learning activities (Nite et al., 2024). These were combined in the simulated cyber attack activity designed by one of our industry guest speakers. This activity, along with the social engineering lecture are the two examples that we describe in detail in the next section.

Table 1: Sample summer camp schedule.

Start	End	Monday	Tuesday	Wednesday	Thursday	Friday
8:00	8:30	Arrival/Dropoff				
8:30	8:45	Orientation	Group projects "secure systems presentation"			
9:00	9:15	Check out laptops	GenCyber concepts game	GenCyber concepts game	GenCyber concepts game	Group projects
9:15	9:30		Social engineering	Cryptography with Python	Guest speaker - visualization	
9:30	9:50	GenCyber concepts game				
9:50	10:00	*Break*	Campus tour			
10:00	10:45	Cybersecurity principles	Genomics	Guest speaker - industry	Intro to AI/ML	Campus tour
10:45	11:00	*Break*				
11:00	11:30	Python coding	Safe online behavior	Guest speaker - industry	AI/ML activity	
11:30	12:00					Admissions
12:00	13:00	*Lunch break*				
13:00	13:50	Python coding	Python coding	Flying drones	Intro to cryptography	Group projects
13:50	14:00	*Break*				
14:00	14:50	Presentation guidance	West campus data center tour	Drone security	Cryptography activity	Group project presentations Session
14:50	15:00	*Break*		*Break*	*Break*	

Continued

Table 1: Continued

Start	End	Monday	Tuesday	Wednesday	Thursday	Friday
15:00	15:50	Guest speaker - TAMU security		Secure system guidance	Cryptography activity	Survey & Closing
15:50	16:00	*Break*				
16:00	16:20	Office hours				
16:20	16:40	Cleanup				
16:40	17:10	Dismissal/Pickup				

GUEST SPEAKER SESSIONS

The guest speaker sessions covered a wide range of topics in cybersecurity. These included a discussion about what is involved in having a secure system, led by the High Performance Research Computing's Senior Security Engineer. One of the very popular lectures was given by one of associate directors of the A&M University Technology Services department. The students often cited that lecture as a favorite because the speaker gave real life examples of cybersecurity breaches in he experienced. They had never realized the complexity of secure systems at educational institutions. Another speaker with real-life stories about cybersecurity was the director of the Cybersecurity Center at Texas A&M University. Professors in several departments spoke about the importance of cybersecurity in the research arena. Two of the most popular sessions are described in more detail below. These include the social engineering lecture and a simulated cyber attack designed by one of our cybersecurity experts in industry. She also spoke about opportunities for careers in cybersecurity, and the students frequently cited that as one of their favorite activities or one in which they learned the most for that day or for the week.

Social Engineering

One of the students' favorite guest speaker sessions covered safe online behavior with a particular focus on social engineering. The speaker covered various types of social engineering strategies, including "phishing", "SMSishing", "vishing", "dumpster diving", "shoulder surfing", and face-to-face attacks. The speaker drew on his own experience working in cybersecurity in the military, engaging students with personal narratives throughout the presentation. Alongside these personal stories, the presentation also included multiple videos and real-world examples of previous cyber attacks that employed social engineering. The students learned about the growing prevalence of deep fakes, the importance of wifi router updates, the dangers of public WiFi networks, and virtual private networks (VPNs), all of which the speaker touched on when discussing his own experiences in the field of cybersecurity.

Simulated Cyber Attack

Another popular guest speaker was a cybersecurity expert from private industry, whose activity consisted of a simulated cyber attack to which the students worked together in various roles to resolve. Roles the students played included Chief Information Officer, Information Security Engineers,

Analysts, and Administrators, Network Managers, System Administrators, Software Developers, User Support Technicians, and Business Owners. Each of these roles was given a set of actions they could execute with each action costing the team a predetermined amount of time. For example, the Information Security team's actions included: 1) gathering initial malicious activity information (15 minutes), 2) work with other teams and a forensics firm to determine the accounts used for the attack (30 minutes), 3) work with the System Administrators to determine the last known backup suitable for recovery, 4) block/ban all malicious program files (15 minutes), 5) work with a security forensics firm for a full report regarding the attack, including the malicious actor's chain of events, the techniques used, and which vulnerabilities were exploited (4 hours). The students playing various roles worked together to resolve the cybersecurity issue as quickly as possible.

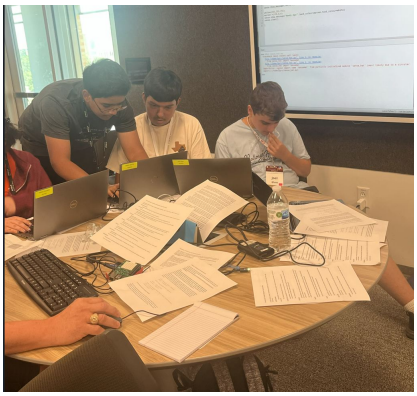

Figure 1: Students collaborating to mitigate the effects of a cyber attack.

At the end of each day of camp, students filled out a brief reflection about their learning for that day. They were asked about the level of learning they experienced with each lecture or activity of the day and which was their favorite. They were also asked which, if any of the 21st century skills of collaboration, critical thinking (problem solving), communication, and creativity they experienced in the various activities as well as whether it was fun.

RESULTS

Figure 2 below shows the results from the June 2023 camp for the question about how much students learned from three of the most popular sessions for the week. For all three of these activities, the vast majority of students learned "a lot" or "quite a bit". Social engineering had the highest number for "a lot" and students commented in the free responses how much they had never known before.

Students were also asked how much they experienced collaboration, creativity, communication, and problem solving in each of the activities for the day. Not all activities were designed to incorporate all of these skills, but

it some answers were surprising when students recognized the use of skills we had not thought about as part of that activity. The social engineering lecture was very engaging, as the speaker switched frequently between personal experiences, video clips, and direct teaching, keeping his audience on the edge of their seats to see what would happen next. The graph in Figure 3 shows that the students had a high degree of fun with that lecture as well as learning a lot. In the case of the cyber attack simulation, students did a lot of problem solving. They competed with other teams to see how well and quickly they could figure out and implement the required strategies to stop or mitigate the damage. Although this activity did not rate as high as others on the fun scale, it was at the top of the list for what they learned. Many of the other guest lectures received high marks in learning and 21st century skills, but the ones discussed in this paper are examples of a few of the favorites for the 2023 and 2024 cybersecurity camps.

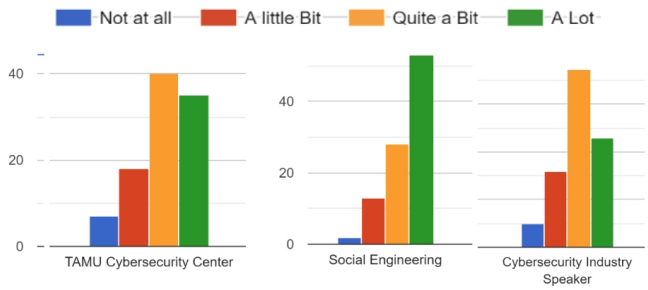

Figure 2: Student responses to "How much did these activities add to your learning about cybersecurity?".

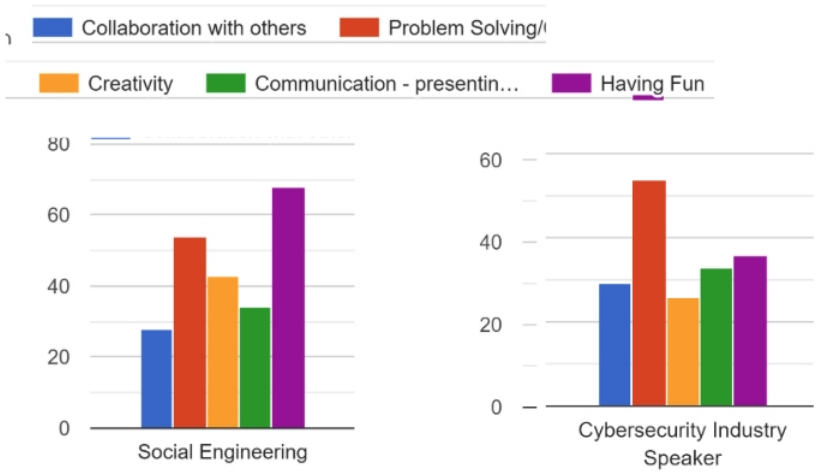

Figure 3: Student responses to "When, if at all, did you experience the following?".

CONCLUSION

Summer camps for middle and high school students are an excellent complement to the formal education students gain. A five-day camp can provide 30 hours of instruction, concentrated on a specific topic such as cybersecurity. This is approximately the same amount of time students spend on a specific class during a six-week time period. This learning is concentrated, and students are immersed in the subject during the week. To keep students engaged in the topic, it is important to change the pace frequently. Alternating between individual work and group work and interspersing less active lectures among interactive and hands-on sessions also helps students focus on the topic all day for a full week. University faculty and staff are ideally suited to provide experiences in cybersecurity education because they often have easier access to knowledgeable speakers within the university and through university collaborations with industry. In addition, they have the opportunity to encourage students to pursue college degrees and even increase interest in careers in the field of cybersecurity. In view of the increasing shortage of cybersecurity professionals in many domains, camps are a wonderful time to include information about career paths and even recruit students to obtain degrees at that particular university. Thus, these camps provide the knowledge students need in their everyday lives, information about career opportunities that benefit society, and possibly recruit students to the university.

ACKNOWLEDGMENT

The authors gratefully acknowledge the support of the National Security Agency and Norwich University through the GenCyber programs H98230-22-1-0152 and 22341-GC2303-01.

REFERENCES

Brashear, W.A., Nite, S.B., and Lawrence, R.L. (2025). Teaching Python to Secondary Students: A Backward Design Process. In 2025 Proceedings of the ASEE Annual Conference & Exposition: American Society for Engineering Education.

Chakravorty, D.K., He, Z., Nite, S. B., Lawrence, R.E., Perez, L.M., Francis, C.P., Brashear, W.A., Liu, H., Dronzmraju, N., Yang, X., Guleria, T., Kim, J. (2023). "Cybersecurity and Data Science Curriculum for Secondary Student Computing Programs." The Journal of Computational Science Education, Vol. 14, No. 2, pp. 6–9. https://doi.org/10.22369/issn.2153-4136/14/2/2

Chakravorty, D.K., Pennings, M., Liu, H., Thomas, X., Rodriquez, D., and Perez, L. M. (2020). "Incorporating Complexity in Computing Camps for High School Students — A Report on the Summer Computing Academy Program at Texas A&M University." Journal of Computational Science Education, Vol. 11, No. 1, pp. 12–20. https://doi.org/10.22369/issn.2153-4136/11/1/3

Hossain, G., Shin, M., and Alfrose, M. (2024). "Bridging the Gap: Exploring Cybersecurity Careers for High School Students.", proceedings of the Frontiers in Education Conference. DOI: 10.1109/FIE61694.2024.1089331

Ileleji, T. and Joseph, A. (2018). "Cybersecurity Talent Shortage and High School Students' Career Interests". 9th Annual International Conference on Computer Science Education: Innovation and Technology. Doi: 10.5176/2251-2195_CSEIT18.141

Nite, S. B., Gray, T. J., Lee, S., and Stebenne, S. (2024). "Engaging Secondary Students in Computing and Cybersecurity". In *Practice and Experience in Advanced Research Computing (PEARC'24)*, Providence, RI. ACM, New York. https://doi.org/10.1145/3626203.3670624

Nite, S.B., Brashear, W.A., Gray, T.J., and Chakravorty, D.K. (2025). "Project-Based Learning in K12 Cybersecurity Education." The Journal of the Colloquium for Information Systems Security Education, Vol. 12, No. 1. https://doi.org/10.53735/cisse.v12i1.209

Sudha, S. S., Sudha, S. S., Javaid, A., Niyaz, Q., and Yang, X. (2023). "Examining the Impact of Early Cybersecurity Education in the Selection of Cybersecurity as a Career among High School Senior and University Freshmen Students". Proceedings of the American Society for Engineering Education Conference. https://doi.org/10.18260/1-2-43512