Virtual Cybersecurity Camps: Lessons Learned

Marc J. Dupuis
marcjd@uw.edu
University of Washington
Bothell, Washington, USA

Joshua Bee
jbee@columbiabasin.edu
Columbia Basin College
Pasco, Washington, USA

Ann Wright-Mockler
ann.wrightmockler@pnnl.gov
Pacific Northwest National Laboratory
Richland, Washington, USA

ABSTRACT

Cybersecurity camps provide participants with an opportunity to learn about cybersecurity in a fun and safe environment. Traditionally, such camps, like many others, are held in-person. However, the COVID-19 pandemic created unique challenges and also an opportunity to counter those challenges—holding a cybersecurity camp virtually. While countless other camps, both cybersecurity-related and others, moved to a virtual environment so that such camps could continue to be held, this paper presents some lessons learned and suggestions that may be helpful to others deciding to hold a virtual camp in the future. Some of the lessons learned may be specific to a cybersecurity camp, but most would be applicable to a broad audience.

CCS CONCEPTS

• **Applied computing → Education**.

KEYWORDS

virtual camp, cybersecurity, lessons learned, under-representation in computing

ACM Reference Format:
Marc J. Dupuis, Joshua Bee, and Ann Wright-Mockler. 2022. Virtual Cybersecurity Camps: Lessons Learned. In *The 23rd Annual Conference on Information Technology Education (SIGITE '22), September 21–24, 2022, Chicago, IL, USA.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3537674.3555787

1 INTRODUCTION

In March of 2020, the entire landscape for summer camps began to shift dramatically. What would soon become clear was that holding in-person camps for the upcoming summer as originally planned was ill-advised given the continued uncertainty related to the pandemic and the path it may take. Suddenly, like the plans for many activities involving close proximity with one another, were being cancelled, moved to a virtual environment, and/or delayed indefinitely.

Funding agencies were forced to provide additional flexibility in the wake of such massive disruptions to our entire way of life. For example, the National Security Agency (NSA) allowed for GenCyber camps originally planned for the summer of 2020 to be postponed a year. They also began to allow virtual camps, which allowed for greater certainty with respect to planning and recruitment. This paper details some of the lessons learned and suggestions for others as it relates to hosting a virtual camp.

SIGITE '22, September 21–24, 2022, Chicago, IL, USA

ACM ISBN 978-1-4503-9391-1/22/09.
https://doi.org/10.1145/3537674.3555787

2 BACKGROUND

The original cybersecurity camp was going to consist of two one-week-long in-person camps in two geographically distant locations. There were going to be 60 participants for each week of camp with a goal of an approximate even gender identification split between those that identify as males and those that identify as females. Recruitment was to be focused on those entering 7th-12th grade for the upcoming school year. Participants were going to be recruited from the immediate geographic area of each camp location given that it was a day camp and not residential.

Once flexibility was provided to move to a virtual camp, we proceeded accordingly. Our original plans did not include the use of Raspberry Pis since camp participants were going to be in computer labs equipped with all necessary hardware and software. However, issues related to equity and access caused us to rethink how we would approach a virtual camp and ensure a fun and engaging experience for everyone. Thus, the decision was made to use Raspberry Pis as part of the camp experience.

3 RECRUITMENT

Recruitment efforts had to be altered substantially to take into account the change from an in-person camp to a virtual camp experience. While prior contacts and avenues for recruitment could still be used, the shift to virtual provided a unique opportunity to reach participants from across the entire state and beyond. A short recruitment video was created that provided an overview of the camp and was overlayed with lively music, graphics, and text (https://youtu.be/UG3QrBlzzrE). A website was also created with information on the camp, how to register, and a substantial FAQ section. Finally, we also made a one-page flier that could be used for quick reference of pertinent information. These various recruitment materials were shared during our recruitment efforts.

3.1 Organizations and Social Media

Each member of the team reached out to organizations they were familiar with, such as school district contacts, Girls Who Code advisors, and community leaders. We received responses from several of these efforts that they had in fact shared the information with eligible individuals that they had contact with in their professional and personal capacities.

Social media was used extensively in the recruitment of 7th-12th graders from across the state. In particular, Facebook was

used to reach communities from all geographic regions within the state with an emphasis on communities that have large numbers of individuals from backgrounds traditionally under-represented in the computing disciplines.

While advertising on the platform could have been used and targeted to these specific communities, we instead chose to join several community groups representing these cities, towns, and neighborhoods. Once we were a part of these groups on Facebook, we would create posts that clearly indicated that the camp was free and sponsored by the federal government. Although this was somewhat time-consuming initially, the results were quite promising.

3.2 Results

Through our various recruitment efforts and with a strong emphasis on providing opportunities to those with backgrounds that are traditionally under-represented in computing [7], we were able to achieve over 260 registrations for the camp for an initial 120 spots (60 per week).

By making adjustments to budget allocations, we were able to make room for an additional 42 participants for a total of 162 camp participants with 82 during the first week and 80 the following week. Approximately 74% of our participants came from backgrounds traditionally under-represented in computing with 81 identifying as female, 74 identifying as male, and seven indicating non-binary or other. Based on ethnic background identification, we had 59 individuals identify as Asian, followed by White (55), Other/Multi-Racial (26), Black/African American (16), and Hispanic (6).

4 LOGISTICS

There were three primary logistical challenges we faced in holding a virtual camp. First, acquiring enough Raspberry Pis quickly enough to then package them with the rest of the items and have them shipped to participants was a challenge. Part of what made this challenging is the overall cost, which requires different budgetary and bidding processes at the public institution level, as well as order limits placed by several vendors with respect to the number of Raspberry Pis that may be ordered at a time. Dozens of small orders had to be placed from a variety of vendors to ensure an adequate number of devices, including extra devices in the event of malfunction or theft (e.g., porch theft). Out of approximately 310 shipments (monitors were shipped direct from the vendor(s)), only two packages were stolen and both at the same house as they had two camp participants. Thus, it would not have been worthwhile to have required a signature with the packages that were shipped directly from us, which would have added approximately $5 per package.

Second, packaging and then shipping approximately 180 packages (participants and staff) requires significant planning and support. Boxes that were of sufficient size had to be purchased, as well as other items, such as snacks and giveaways. With respect to giveaways, such as t-shirts, there needs to be sufficient lead time for not just production and shipping, but also approvals for when institutional trademarks are used. In some instances, registrants did not provide full or accurate addresses. This added time to the process, which was often in short supply.

Third, communication with registrants poses a large logistical challenge as you are often interacting with both the minor and one or more guardians for each registrant. When final confirmations were requested, we did not rely on email alone. In addition to sending emails to each email address we had on file for a registrant (up to five each when including primary and secondary email accounts, GMail accounts, and parents/guardians), we also sent text messages to ensure they would see it and respond appropriately. We used a service called ClickSend, which allowed us to send bulk texts out in a cost effective and efficient manner, including through email. Similar to emailing, the text messages were sent to each of the phone numbers we had on file (up to three each when including parents/guardians).

4.1 Camp Staff

Although not a challenge unique to a virtual camp environment, hiring a staff of student leaders poses its own unique challenges. We wanted to hire student leaders that would help ensure the participants would have a fun, engaging, and safe time learning about cybersecurity. Additionally, we also wanted balance among our student leaders with respect to the backgrounds they bring to the camp. This, along with the variety of guest speakers we had, helps make it easier for the camp participants to see themselves in cybersecurity.

A challenge related to hiring student leaders is having a sufficient number of applicants for a 100-hour commitment in the middle of summer when many potential student leaders may be otherwise engaged in internships. Reaching out directly to prior students is an effective way to encourage additional applicants. Some student leaders chose to use their position as an internship as well. In those cases, additional work was assigned to meet the minimum number of hours necessary for internship credit. For example, some created video tutorials on how to complete specific labs, which were then made available to the camp participants.

Additionally, all camp staff had to undergo background checks and training specific to working with minors. While none of us had any physical proximity to camp participants, the training helps ensure that we all understand what is and what is not appropriate when interacting with minors. Each camp week had to be registered with the lead institution's office that handles youth programs. Then, each staff member had to be entered into the registration so that they may be contacted further for the requisite training and background check. This process can take some time and the requirements of each institution will likely vary substantially.

5 CURRICULUM

The curriculum we used came from a variety of sources, including curriculum that we had developed ourselves, Cyber.org, and TeachCyber.org, among others, including our own relevant research (e.g., [2–4, 6]. The focus was on as much hands-on active learning as possible. The shift in mindset from a college course (e.g., [1]) to a camp experience for youth is very important since developing interest and active engagement is key for camp participants rather than demonstrating memorization of specific principles at the end of a course.

We used the Canvas LMS platform to provide access to the learning materials for camp participants. Multiple formats were provided for each resource to ensure equitable access to participants that may be using a screen reader due to visual impairments. In addition to the guest speakers sharing their cybersecurity career paths with the participants, the three authors of this paper did that as well. Participants appeared to greatly appreciate hearing the different paths we each took, which helps them see themselves pursuing a career in cybersecurity. Both technical and non-technical pathways were emphasized throughout the camp.

6 CAMP EXPERIENCE

6.1 Structure

The general approach to the structure of the camp was to have everyone in the main Zoom room for general announcements, mini-lectures, guest speakers, and overviews of the day. Beyond that, participants spent most of their time in their breakout rooms with their assigned student leader that was maintained for the duration of the camp. Groups ranged in size from about eight to 10 participants per group.

Groups were made based on gender identification. For participants that registered and indicated non-binary or other, we reached out to them to determine what group they would prefer to be in for the camp. Many of them responded to this email thanking us for asking them about their preference. The main reason for dividing camp participants based on gender was to ensure a welcoming environment for all, including those that identified as female given the propensity for those that identify as male to at times dominate discussions in mixed gender computing-based settings [8]. We wanted to ensure that everyone felt empowered in the camp.

6.2 Icebreakers

An in-person camp experience is inherently quite different than a virtual camp experience. With in-person camps you can engage the students with physical-based icebreakers, see their expressions, and feel their energy in a sense. Virtual camps do not provide those same opportunities; however, there are ways to emulate the experience as much as possible. We employed a variety of icebreakers throughout the entirety of the camp.

This included large-scale icebreakers when we were all together, such as the use of polls with "would you rather" type questions and a Tablet, which is an online platform that collects and displays data in real-time, to assess the similarities and differences between everyone. Individuals would often speak up by unmuting their microphones and/or putting their thoughts into the chat. During small group time, the student leader would engage them in another icebreaker aimed at building trust and rapport within their small group. This would generally occur one to two times per day.

6.3 Schedule

The typical schedule each day consisted of a morning icebreaker and mini-lecture (9-9:30) followed by a lab/activity (9:30 – 10:30), a 15-minute break, and then another mini-lecture and lab activity, which would conclude at noon for a 45-minute lunch. After lunch, we had one-hour allocated to a guest speaker with a 15-minute break afterward. We then engaged in another mini-lecture, lab/activity, 15-minute break, and then a short mini-lecture and lab/activity to end the day. Camp concluded by 4:30 each day. It is difficult to overstate the importance of multiple breaks and a day that is not too long.

7 TECHNOLOGICAL CONSIDERATIONS

Participants were provided with a Raspberry Pi 400 kit to use during camp and keep upon its conclusion. We were able to obtain additional funding outside of the GenCyber funds to also purchase small monitors for each participant so that they could use it with their Raspberry Pi. This resulted in each participant having a complete computer for free. We also flashed onto a microSD card Kali Linux for the Raspberry Pi.

And similar to an in-person environment in which technological problems do occur, the same was true for a virtual environment. Technological problems in a virtual environment provided unique challenges in troubleshooting. Simple side conversations that may occur in-person to workout a problem were not possible in the same manner in a virtual environment. Therefore, we created two breakout rooms dedicated to technical support. When an individual was having technical difficulties, the student leader would place them in one of the breakout rooms dedicated to technical support. This proved to be a very efficient method of handling such challenges.

Another technical consideration is the use of Ethernet instead of WiFi for camp staff, when possible. This helps ensure that their bandwidth is as high as possible and provides a greater level of connection stability [5].

8 PROGRAM OUTCOMES

The camp had three primary intended outcomes: 1) Increased cybersecurity knowledge, skills, and abilities among program participants related to the GenCyber Cybersecurity Concepts; 2) Improved cybersecurity hygiene of program participants, both within and outside of their educational institutions, and 3) Dissemination of information on advantages of pursuing cybersecurity careers for program participants, including the variety of opportunities available within cybersecurity.

Based on the comments received, we believe we were successful in achieving our three intended outcomes.

- "The camp clearly explained cybersecurity topics in a fun and engaging manner and really helped increase my interest in cybersecurity."
- "the exposure...all the information was all new to me and it made me so much more aware like your files are not actually deleted just because you delete them...it's awesome."
- "I learned a lot of new things about Cyber Security and all the activities went really smoothly."
- "Getting to know what cyber security is and the basic concepts surrounding it."
- "Expanding my knowledge and interests in cybersecurity."
- "I also really enjoyed learning new terms like the 'Black Swan' and thinking like your adversary, which I found really important to note if I were to join the cybersecurity field. And the people I met like the guest speakers and student leaders were amazing in what they did."

- "Guest speakers were all absolutely great in sharing their advice and tips on the industry."

The use of the Raspberry Pi also appeared to resonate well with camp participants:

- "The activities involving the Raspberry Pi really made me love coding more and the capabilities of this new computer I've never heard of. "
- "I liked that we got the electronics because it made the camp more engaging by having hands-on activities."
- "I liked using the pi and actually doing things with the command line."

Out of 71 responses in an end-of-camp questionnaire, we asked them to rate how well we did at several different activities on a seven-point Likert scale (Excellent; Great; Very Good; Good; Somewhat Good; Okay, and Poor). Some of the results from those questions include:

- 97.2% of the respondents indicated that we did a very good job or better at increasing their interest in cybersecurity
- 87.3% of the respondents indicated that we did a great or excellent job in explaining cybersecurity concepts
- 90.1% of the respondents indicated that the labs were great or excellent
- 95.8% of the respondents indicated that the instruction was great or excellent
- 91.5% of the respondents believed that we were great or excellent at providing a supportive environment to learn about cybersecurity
- 97.1% of the respondents indicated that we did great or excellent at providing a positive environment

Overall, all respondents indicated that they were glad that they participated in the camp with 46.5% indicating they were extremely glad and another 43.7% indicating they were very glad.

9 CONCLUSION

Transitioning from an in-person camp to a virtual camp introduced several unique challenges, such as logistical issues with shipping packages to each participant and lack of in-person engagement and immediate feedback since most participants did not consistently have their cameras on (or did not have cameras to begin with). However, it also allowed us to reach participants for whom such opportunities are generally not available, such as those that live in more rural parts of the state or are geographically distant from larger population centers that often hold such camps.

REFERENCES

[1] Marc Dupuis. 2017. Cyber Security for Everyone: An Introductory Course for Non-Technical Majors. *Journal of Cybersecurity Education, Research, and Practice* 2017, 1, Article 3 (2017), 17.

[2] Marc Dupuis and Faisal Khan. 2018. Effects of peer feedback on password strength. In *2018 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, San Diego, CA, 1–9. https://doi.org/10.1109/ECRIME.2018.8376210

[3] Marc Dupuis and Karen Renaud. 2020. Scoping the ethical principles of cybersecurity fear appeals. *Ethics and Information Technology* (Oct 2020). https://doi.org/10.1007/s10676-020-09560-0

[4] Marc Dupuis, Karen Renaud, and Anna Jennings. 2022. Fear might motivate secure password choices in the short term, but at what cost?. In *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS) 2022*. Virtual, 4796–4805. https://doi.org/10.24251/HICSS.2022.585

[5] Marc J. Dupuis and Karen Renaud. 2020. Conducting "In-Person" Research During a Pandemic. In *Proceedings of the 21st Annual Conference on Information Technology Education*. ACM, Virtual Event USA, 320–323. https://doi.org/10.1145/3368308.3415420

[6] Marc J. Dupuis, Jaynie Shorb, James Walker, Fred B. Holt, and Michael McIntosh. 2020. Do You See What I See? The Use of Visual Passwords for Authentication. In *Proceedings of the 21st Annual Conference on Information Technology Education*. ACM, 58–61.

[7] John Knight, Jack Davidson, Anh Nguyen-Tuong, and Jason Hiser. 2016. Diversity in cybersecurity. *Computer* 4 (2016), 94–98.

[8] Ming-Te Wang and Jessica L. Degol. 2017. Gender gap in science, technology, engineering, and mathematics (STEM): Current knowledge, implications for practice, policy, and future directions. *Educational psychology review* 29, 1 (2017), 119–140.