ISSN: 2473-4901
v10 n6108

Cyber Palooza: Insights of a One-Day Cybersecurity Event

Joni Adkins
jadkins@nwmissouri.edu

Diana Linville
dianar@nwmissouri.edu

School of Computer Science and Information Systems
Northwest Missouri State University
Maryville, MO 64468, USA

Abstract

Cybersecurity is a highly sought after field and a critical need in industry. To increase awareness and interest through hands-on activities, a one-day event called Cyber Palooza was created for high school students. Cyber Palooza allowed students the opportunity to engage in cybersecurity topics that educated them on the different aspects of the field and issues within cybersecurity. Goals of the event were to expose students to safe cyber practices, generate interest in pursuing a cybersecurity career, and encourage students to attend our university. Students traveled to campus and attended sessions conducted by faculty from the School of Computer Science and Information Systems. Multiple events were held during the 2023-2024 academic year. This paper presents insights into planning and conducting Cyber Palooza, topics and activities presented, and the lessons learned from the event.

Keywords: Cybersecurity education, cybersecurity event, recruitment, high school

1. INTRODUCTION

Cybercrimes and threats continue to be an issue for industry. System attacks and data breaches are a significant financial burden on a company. In 2023, the annual cost of cybercrimes in the U.S. was 320 billion and is expected to grow to 1.82 trillion by 2028 (Petrosyan, 2023). A company's reputation can also be impacted by an attack which can negatively affect their profit margins. When consumers hear about a data breach, they become hesitant to do business with that company. These impacts lead to an increasing demand for cybersecurity skills within the workforce to keep businesses and consumers safe.

Several factors make cybersecurity an attractive employment area. The 2023 median pay was $120,360 annually and typically requires only a bachelor's degree (BLS, 2024). As of September 2023, there were 714,548 job openings in the U.S. in need of cybersecurity related skills, and openings are projected to grow to 3.5 million by 2025 (Madden, 2023). To meet this demand the cybersecurity workforce would need to grow at a rate of 12.6 percent per year; in 2023 it only grew by 8.7 percent (Poremba, 2024). This presents a considerable gap in fulfilling the needs for cybersecurity positions.

Filling this gap requires that students not only enter the field of cybersecurity, but also have the skillset that companies are looking for. Interviews conducted with cybersecurity professionals found that there is a high demand for cybersecurity graduates to have hands-on skills, to be continuous learners, and are excited to be in the cybersecurity field (Towhidi & Pridmore, 2023). Another study showed that higher education degrees were frequently required across different cybersecurity positions (Ramezan, 2023). Providing educational experiences in cybersecurity to students can help build the country's cybersecurity expertise (Locasto & Sinclair, 2009). Encouraging student interest in cybersecurity degree programs is essential for developing individuals equipped with the necessary skills and education to meet these demands.

In addition to the pressing demand for cybersecurity experts, foundational cybersecurity education plays a key role for all consumers as well. Studies have shown that 95% of cybersecurity issues can be contributed to human error (Mee & Brandenburg, 2020). This can be attributed to the increase in phishing scams and spam emails. By exposing students to cybersecurity topics, we can increase their awareness, minimize the impact of cybercrimes, and improve the safety of the nation. The increased need for both cybersecurity professionals and consumer cybersecurity safety measures show the importance of conducting events to showcase cybersecurity.

A recent test demonstrated there is a need to educate users on cybersecurity safety. Our university tested students with a typical phishing email that looked like it came from a Registrar's Office and told students their classes would be cancelled if they did not verify their student information using the link in the email. This email was sent the morning of the first day of fall classes. Preliminary results were 37% of university students clicked on the link. Of those clicking on the link, 66% entered their student details leading to 24% of students completely failing the phishing test. Even though today's students spend a lot of time online, many still could easily be a victim of cybercrime. This is further evidence of the importance of educating people on phishing and other types of cybercrime.

2. CYBER EVENT GOALS

We had three goals for our Cyber Palooza events. The first was to expose high school students to cybersecurity topics to reduce their chances of being a victim of cybercrime. The second goal was to generate interest in studying and working in the cybersecurity field. The third goal was to bring more potential undergraduate students to our campus. With the declining pool of traditional college students in rural areas, our university is always interested in getting prospective students to visit campus.

The purpose of this paper is to share the planning process, cybersecurity and technology topics covered, and lessons learned from the events.

3. CYBER PALOOZA PROGRAM PLANNING

There were several steps that took place leading up to the cybersecurity education and recruiting events. Our university was working to apply for the National Centers of Academic Excellence in Cybersecurity program for Cyber Defense (CAE-CD) designation. A core value of the program is sharing cybersecurity expertise with others. The Program Involvement, Outreach requirement for this distinction is to provide significant community involvement and academic programming in cybersecurity (CDWG, 2024). Educating prospective college students and high school teachers was one of our outreach efforts. Knowing that outreach would require resources, we determined that funds from an existing grant could pay for these events. Engaging students early is vital to attract students, especially females, into careers focused on technology (Amo, Liao, Frank, Rao, & Upadhyaya, 2018).

Grant Funding

In the fall of 2021, we applied for a MoExcels grant through the Missouri Department of Higher Education and Workforce Development. MoExcels funding is to help develop education and training programs specifically needed in the state (MDHEWD, 2024). The grant, "Protecting Missouri's Cybersecurity Future," requested $757,250 in state funds and offered $210,000 in internal matching funds to update two computer labs and to recruit more students to the cybersecurity program. In 2022, we learned the grant had been funded and began planning for the update of the labs and equipment. The labs were completed in summer of 2023. In addition to the remodel and new computing equipment, the matching funds allowed for faculty development and student cybersecurity recruiting and education.

Once the updated cybersecurity lab and the other lab with Apple computers were complete, planning for the recruitment and education events started. A team of faculty and staff from the School of Computer Science and Information Systems formed to develop ideas for recruitment events. The team included faculty with high school teaching experience or cybersecurity expertise along with the office manager, director, and assistant director.

Included in the grant were funds for faculty to travel to local high schools. We learned that heavy university faculty teaching loads and high school visitor/admissions restrictions would limit the travel faculty could do to high schools. Therefore, a one-day event on campus was developed.

Working with Campus Partners
Our group met with admissions early in the process to discuss the best ways to communicate the day with high schools. The Admissions office provided names and addresses for the top 100 feeder high schools. The Marketing area developed brochures and postcards to be mailed to the high schools.

We developed two different programs for campus visits, a Cyber Palooza and a Cybersecurity Showcase Visit Day. The Cyber Palooza activities were modeled like Computing Palooza events done in the past where teachers bring groups of students to campus to participate in activities. We changed the activities to be related to cybersecurity. The Cybersecurity Showcase Visit Days were modeled after a typical Computer Science Visit Day with a shortened version of the admissions presentation and campus tour. The showcase day also had two cybersecurity sessions and panels with faculty and students.

4. CYBER EDUCATION EVENTS

We selected three dates in November, one for Cyber Palooza and two for Cybersecurity Showcase Visit Days. We elected to do paper mailings to high schools to advertise these events along with utilizing the Missouri Business Educator listserv. Postcards and brochures were developed and mailed to the top 100 feeder high schools. The materials to the school advertised free registration, lunch, t-shirt, technology for classroom, and bus reimbursement. We had heard from admissions that fewer schools were coming to campus for visits due to the cost and availability of buses so we hoped the bus reimbursement would make the event more appealing to administration.

The registration for our Cyber Palooza date soared quickly, and we had to cut off registrations when we reached approximately 200 students. Since one of our Cybersecurity Showcase Days did not have any sign ups, we switched that date to a second Cyber Palooza. In the spring, we did another Cyber Palooza event on one date in March. Our attendance numbers are displayed in Table 1.

Event	Schools	Teachers	Students
First Fall Cyber Palooza	16	26	180
Second Fall Cyber Palooza	11	17	159
Spring Cyber Palooza	4	5	35
Fall Showcase Day	1	2	11
Totals	32	50	385

Table 1: Attendance numbers

Expenses for the one-day events were covered by internal matching funds from a MoExcels grant. There was no fee for students to attend, and each student received a free meal voucher for campus dining as well as promotional swag items from the School of Computer Science. Each teacher who attended received 10 micro:bits to use in their classrooms along with swag items from the School.

Table 2 shows the breakdown of grade levels for students who attended the cyber events. We opened it up to all high school students, and one school requested to bring some eighth graders. We also had one local community college participate.

Grade Level	Number Attended
Community college	3
12th	139
11th	93
10th	75
9th	61
8th	14

Table 2: Attendance by Grade Level

Since our goals were to expose students to both cybersecurity and our university, we were pleased with the number of schools who participated in the event. A total of 31 schools participated with 28 in state and 3 out of state. Table 3 shows a summary of the size of schools attending. Since we are in a rural area, it was not surprising that most schools attending were small. The community college is not included in the table below.

9-12 Enrollment	Number of Schools
1-200	16
201-500	8
500+	6

Table 3: Attendance by school size

Table 4 shows how far the participants traveled to get to our university. School districts were also reimbursed for transportation. The average cost for transportation per school was $170.00.

Number of Miles	Number of Schools
1-50 miles	14
51-100	12
100+	5

Table 4: Miles Travelled

5. CYBER PALOOZA ACTIVITIES

During the one-day Cyber Palooza event, students were assigned to groups. There were approximately 30 students in each group which was determined by classroom size. The groups consisted of students from different schools so that they could meet and network with other students. Each group was assigned an attending teacher and rotated between four different sessions. The schedule for the event is shown in Appendix A.

Cyber Palooza was designed around six different areas that were implemented across five different sessions. Each session was conducted by faculty within the School of Computer Science and Information Systems and provided hands-on activities. Due to the number of groups, students did not participate in every session, except for the "Hands-On Coding", "Cracking Passwords", and "Phishing/Internet Safety" sessions, each of which had two sections.

Hands-On Coding

The Hands-On Coding activity consisted of students first becoming familiar with using block-based programming and sending messages to their micro:bits. Then they paired up and sent messages to each other. The teacher then demonstrated how easy it was to intercept their messages and discussed the importance of security and encryption (See Appendix B). Students then set up a key exchange to show how to encrypt a secret number.

Cracking Passwords

In this session, students learned the importance of the password, how to make a strong password, how the password is stored, how to crack a password, and two factor authentication. Students used John the Ripper software to demonstrate cracking a password and evaluated password strength online. Using their own examples, they verified the properties of the hash.

Phishing and Internet Safety

During the Phishing and Internet Safety activity, students received information on the risks of phishing and other internet safety issues such as secure passwords. The students were then put into 5-6 groups and given a breakout box. Each breakout box had 5 different locks and all the clues to find the codes to unlock them were scattered on the table. Students had to use critical thinking, perseverance, and teamwork to figure out what clues went together to find the correct code for each lock. The clues included information about internet security, phishing, binary code, and basic technology concepts. At the conclusion of the session, the session leader wrapped up by stating that the skills that they needed to complete this activity were the same skills needed to be successful in the field of cybersecurity: critical thinking, perseverance, and teamwork.

Cryptography Unplugged

Cryptography Unplugged included information about ancient cryptography (Caesar Cipher) and modern ciphers (DES, AESRSA, ECC). Students were divided into groups to encrypt a message with a shift cipher and then challenged to break a simple cipher without a key (See Appendix C).

Other Sessions

Additional sessions included Robotics, Virtual Reality, and 3D Printing. The Virtual Reality and 3D Printing sessions allowed the high school students to interact in the maker space and see cool technology. University students led this session. The Robotics session used scribbler robots and did some basic coding. Students attended one of these sessions to see another side of technology and to hear about the importance of cybersecurity to protect devices.

6. RESULTS OF EVENTS

Since the students were attending from multiple high schools and were mostly under 18, we did not gain permission from parents to use student feedback data for publication. We did not want the teachers to have extra hurdles or roadblocks that might discourage them from attending. This means that we cannot report on the data gathered through student surveys.

Our university admissions team coded all students who attended so we can track them in future years to see if they attend our university and/or enroll in the cybersecurity major. In the first academic year following these events, 16 students who attended a cyber event enrolled as a full-time student at our university. Of these students, one is a cybersecurity major and four are majors in other computer science/information systems disciplines. Deckard, Quarfoot, & Csanadi (2014) found that a one-day session to expose middle school females to STEM had an impact on reshaping attitudes toward engineering. In another study, a 1-hour session on computer networking did not show any statistically significant effects (Amo, et al, 2018). The impact of this event on future enrollment in a cybersecurity major does not appear to be significant for the first year but could influence future students.

7. LESSONS LEARNED

The cybersecurity events went very well, and the students and teachers seemed to enjoy and appreciate their time on campus. We wanted students from various schools to network and meet other students, but that did not work as we had hoped. Students did not interact and were more reserved when participating in the activities. It also required teachers to regroup with their students at lunch. We adjusted for our second planned day and did not mix up the students, and they appeared more engaged and animated when with their classmates. Another option in the future could be to add icebreaker activities or some kind of structured networking to encourage students to engage more with students from other schools.

As explained above, we held two Cyber Palooza days in the fall and one day in the spring. The two fall days had better attendance than the one held in the spring. We attributed this to the large number of events and end-of-school-year activities that take place in the spring in high schools. Future Cyber Palooza events will take place in the fall to avoid these conflicts.

We found that Cyber Palooza was more popular than the Cybersecurity Showcase Day (Schedule in Appendix D). The hands-on activities that were presented appealed to the high school teachers and students more than listening to faculty and student panels and observing projects. We will not offer a Cybersecurity Showcase Visit Day but will continue with our general Computer Visit Days which are held two times a year.

Overall, observations were made that indicated students enjoyed the hands-on activities such as virtual reality, hands-on coding, and internet safety. Conversations with teachers indicated they appreciated the day and were excited to use their micro:bits in their classrooms. Students completed admissions information cards when they attended and are now all coded within the admissions system so they can be contacted for future events. In the future, we will be able to see how many Cyber Palooza attendees attend the university and/or major in cybersecurity.

8. MOVING FORWARD

Holding the Cyber Palooza events allowed us to demonstrate cybersecurity practices to teachers and students who were not within the university structure, helping us to meet the Program Involvement requirement for the CAE-CD designation. Matching funds are still available so two more Cyber Paloozas will be offered in the fall of 2024. We will invite the same schools for this fall and make sure to have different activities for students who may be attending a second time. A similar schedule will be used, and sessions will be updated to include more interactive material. Students seemed to enjoy the hands-on learning sessions more than those with more lecture. Developing cybersecurity education materials requires both technical knowledge and creativity to engage students (Locasto & Sinclair, 2009) so some cybersecurity experts may be teamed with instructors who excel at creativity in their courses. In addition, we will use more materials from sites such as cyber.org and CLARK.

Future events could include guest speakers. Locasto & Sinclair (2009) included NSA employees, IT staff, a PhD student, and independent information consultants in their educational program. Other universities have developed programs that focus on training teachers on integrating cybersecurity into the curriculum (Ivy, Lee, Franz, & Crumpton, 2019). We will continue to explore ways to expose K-12 students to solid cybersecurity practices and cybersecurity post-secondary options. By providing these events, we hope students will consider cybersecurity as an area of study in the future to help meet the growing need for cybersecurity professionals.

9. REFERENCES

Amo, L. C., Liao, R., Frank, E., Rao, H. R., & Upadhyaya, S. (2018). Cybersecurity interventions for teens: Two time-based approaches. *IEEE Transactions on Education 62*(2), 134-140. doi: 10.1109/TE.2018.2877182.

Cyber Defense Working Group (CDWG). National Centers of Academic Excellence in Cybersecurity NEAE-C 2024 Designation Requirements and Application Process for CAE-Cyber Defense.

https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_designation_requirements.pdf

Deckard, C. & Quarfoot, D., & Csanadi, K. C. (2014). Analysis of a short-term STEM intervention targeting middle school girls and their parents. *121 ASEE Annual Conference & Exposition.* Retrieved from https://monolith.asee.org/public/conferences/32/papers/9747/view

Locasto, M. E. & Sinclair, S. (2009). An experience report on undergraduate cyber-security education and outreach. *Annual Conference on Education in Information Security (ACEIS)*. ACM. Retrieved from https://cs.gmu.edu/~mlocasto/papers/sismat.ACEIS.pdf

Ivy, J., Lee, S. B., Franz, D., & Crompton, J. (2019). Seeding cybersecurity workforce pathways with secondary education. *Computer (52)*, 67-75. Doi: 10.1109/MC.2018.2884671

Madden, J. (2023). *CompTIA Partners: Meeting the Rising Demand for Cybersecurity Skills.* Retrieved from: https://www.comptia.org/blog/meeting-the-rising-demand-for-cybersecurity-skills

Mee, P., & Brandenburg, R. (2020). *After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk.* Retrieved from: https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education/

.

Missouri Department of Higher Education and Workforce Development (MDHEWD). *MoExcels Workforce Initiative*. (2024). https://dhewd.mo.gov/initiatives/moexcels.php

Petrosyan, A. (2023). *Estimated annual cost of cybercrime in the United States from 2017 to 2028.* https://www.statista.com/forecasts/1399040/us-cybercrime-cost-annual

Poremba, S. (2024). *What the cybersecurity workforce can expect in 2024.* https://securityintelligence.com/articles/cybersecurity-workforce-trends-2024/

Ramezan, C. (2023). *Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field*. Journal of Information Systems Education, 34(1), 94-105

Towhidi, G. & Pridmore, J. (2023). *Aligning Cybersecurity in Higher Education with Industry Needs*. Journal of Information Systems Education, 34(1), 70-83. https://jise.org/Volume34/n1/JISE2023v34n1pp70-83.html

U.S Bureau of Labor Statistics (2024). *Occupational Outlook Handbook*. Retrieved June 15, 2024, from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

APPENDIX A
Cyber Palooza Event Schedule

9:00 – 9:15 am	REGISTRATION
9:15 – 9:30 am	WELCOME & ADMISSIONS
9:35 – 10:15 am	SESSION 1 (refer to assigned schedule)
10:20 – 11:00 am	SESSION 2 (refer to assigned schedule)
11:00 am - 12:00 pm	LUNCH
12:05 – 12:45 pm	SESSION 3 (refer to assigned schedule)
12:50 – 1:30 pm	SESSION 4 (refer to assigned schedule)
1:35 – 2:00 pm	WRAP UP SESSON/CLOSING
2:00 pm	DEPART

APPENDIX B
Hands-On Coding

1. Programming Steps:
    a. Create New Project – Call it MicroChat – 1, 2, 3, or 4 Depending on group #
    b. Explain Interface pieces – blocks, simulator, etc.
    c. Drag and Drop Forever block onto blocks area to delete
    d. Set radio channel (have students use the number on their card). This makes sure that only the microbits set to the same channel (ideally, their neighbor)
    When the button is pushed send a message; have them choose one of the secret words on their card. When a message is received, display that message

2. After the code is written, students can investigate what the Python would look like (Blocks/Python selector at top).
3. Download the code to the microbits using Chrome and the big purple Download button

Securing transmissions – Important

1. Have them send another word, show them the teachers that was listening.

APPENDIX C
Cryptography Unplugged

Cipher

QIJ XIHCJ KTHVCJZ XBQI QIJ XHTCS BA QIGQ LHHCA GNS LGNGQBPA GTJ
GCXGWA AH PJTQGBN HL QIJZAJCDJA, GNS XBAJT KJHKCJ AH LMCC HL
SHMVQA.

Hint

1) E was replaced by J

Encodings

The substitutions: (H⇒I indicates that H was replaced by I)

1) [H⇒I, X⇒O, D⇒S, J⇒R, I⇒B, M⇒Z, Z⇒F, S⇒A, A⇒G, C⇒P, N⇒N, Y⇒W, R⇒T, G⇒E, E⇒J, V⇒D, U⇒M, L⇒C, B⇒V, K⇒Y, F⇒L, O⇒H, W⇒X, T⇒Q, P⇒K, Q⇒U]

Solution

1) THE WHOLE PROBLEM WITH THE WORLD IS THAT FOOLS AND FANATICS ARE ALWAYS SO CERTAIN OF THEMSELVES, AND WISER PEOPLE SO FULL OF DOUBTS.

APPENDIX D
Cybersecurity Showcase Visit Day Schedule

9 – 9:15 a.m.	Check-In
9:15 – 9:30 a.m.	Welcome and Admissions Presentation
9:30—10:15 a.m.	Cybersecurity Class Demonstrations
10:15—11:00 a.m.	Student Projects & Activities
11:00—12:00 p.m.	Lunch
12:00—12:45 p.m.	Student Panel & Faculty Information
12:45—1:50 p.m.	Campus Tour
1:50 p.m.	Visit Day Wrap Up