Bridging the 'town and gown' divide: Experiential learning for students via a community cyberhygiene training program

Aunshul Rege, Gabrielle Spence, Rachel Bleiman, Sean Mitchell, and Jonathan Latko
Temple University, rege, gabrielle.spence0002, rachel.bleiman, smitchell, Jonathan.latko@temple.edu

2024 IEEE Integrated STEM Education Conference (ISEC) | 979-8-3503-5280-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISEC61299.2024.10664800

Abstract - **Cyberhygiene is a necessary tool for navigating today's ever-evolving tech-centric society. Unfortunately, discussion and development of this skillset rarely tends to go beyond the four walls of the classroom and into the wider community. This paper shares a pilot student course project conducted in Fall 2022 and Spring 2023 semesters that aimed to bridge academia and the community. Specifically, undergraduate and graduate students shared their knowledge on, and had conversations about, cyberhygiene and cybersecurity with the community. By combining academic resources, student learning, and key community partnerships, the authors created and facilitated a learning space for those who might not otherwise have access to cyberhygiene training. This paper shares student perspectives on how this project was valuable to themselves and the community; it also shares student recommendations for project improvement. The paper concludes with a discussion about fostering community-academia relationships, establishing trust, and suggestions for developing similar projects in the community.**

Index Terms – cybersecurity education, cyberhygiene, community engagement, STEM education

I. INTRODUCTION

The Internet Crime Complaint Center (IC3) is a central point for cybercrime victims to report their experiences. The 2021 IC3 Annual Report stated that it received 847,376 complaints that year, which resulted in financial losses of $6.9 billion [1]. The report also suggested that these monetary losses varied by victims' ages: those under 20 (N=14,919) reported losses of $101.4 million while those 60 and above (N=92,371) lost $1.68 billion [1]. These numbers suggest that older individuals are more likely to be targeted, which may coincide with their level of digital literacy. UNESCO defines digital literacy as the "ability to access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately through digital devices and networked technologies for participation in economic, social, and political life" [2]. Cyberhygiene is a key digital literacy skill that "encompasses practices and steps that individual users and organizations take to maintain their online security and strengthen the security of their computers or other digital devices" [2]. Thus, being digitally literate improves one's skills to use today's technology appropriately, effectively, and safely [3]. Lack of digital literacy could have dire consequences and result in victimization where individuals fall for scams, experience malware attacks, compromise sensitive data on open Wi-Fi networks, perpetuate mis/disinformation, or improperly dispose of old files [3].

This paper shares a pilot experiential learning project that serves as a case study for how the next generation workforce (current higher education students) can play a key role in raising cyberhygiene and security awareness by engaging with community partners and residents within their school's neighborhoods. The next section highlights the academic-community partnership, details of the course project, and the undergraduate and graduate students' topics. The third section shares both undergraduate and graduate students' experiences. The paper concludes with a discussion about the value of developing experiential learning projects where students, community partners, and local residents can all benefit. It also offers a brief discussion about the importance of building trustworthy, inclusive, and respect-centered relationships with members of the community.

II. COURSE PROJECT

This section shares information about the community partnership, project description, and specific projects designed by both undergraduate and graduate students.

A. Community Partner

According to the City of Philadelphia's Digital Equity Plan, there were approximately 96,000 households in the city that did not have broadband Internet access, and African American, Hispanic, and low-income residents were less likely to have access to a working device in 2022 [4]. One of the mechanisms through which this issue is being addressed is via the Digital Equity Center (DEC).

The DEC is a workforce development center for the North Philadelphia community, which opened in the summer of 2022. The Center provides North Philadelphia residents with access to technology, help desk support, and free education in the areas of digital navigation and digital literacy [5]. The DEC also helps "ensure that children can keep up with their schoolwork. We will be able to help their

parents receive free continuing education" (as cited in [5]). The DEC houses a computer lab and teaching space that is open to the public [5]. It also offers job training and career readiness programs. The DEC also works with existing nonprofits that already have connections and insights into the needs of the community [6]. The Center thus strives to build a digital inclusion solution for an underserved and underrepresented area in North Philadelphia [5].

As a part of their programming, the DEC provides a digital onboarding course for community clients. This class is based around the essential computer skills laid out in the Northstar Digital Literacy Curriculum. As part of the curriculum, internet safety and cyberhygiene are discussed briefly, with a focus on phishing and digital footprints. However, during the time of this partnership, due to a sizable percentage of the DEC's clients being seniors and first-time computer users, more time was spent in the class focusing on the basics of using computers, so the Center was unable to expand their Cyberhygiene curriculum. The partnership between the authors created another outlet through event where they could spend the necessary time to teach meaningful cyberhygiene lessons.

B. Project Details

Developed in Fall 2022 and Spring 2023 for undergraduate and graduate classes, this pilot project aimed at working with the DEC to raise awareness about cyberhygiene in the North Philadelphia community. Students developed 10-minute cyberhygiene presentations on a cybersecurity topic of their choice. Specifically, the presentation had to cover three main components: (i) define the topic or issue, (ii) justify why it was relevant, and (iii) explain three clear ways to protect against/mitigate issues or practice good cyberhygiene. Students were given extra material on understanding how cybersecurity awareness and training programs were being offered, such as workshops, cyber clinics, games, and quizzes [7]. Students had to do 'dry runs' in class before presenting to the community. Representatives from the DEC provided feedback to the students during these practice rounds to ensure the accuracy of content and remove jargon/academic tone to cater to the general public.

C. Student Projects

The undergraduate classes across both semesters had 49 students and the Fall graduate class had 13 students. Students in each class worked in groups of two or three to develop and share a presentation. They presented during the regularly scheduled class time, which overlapped with the adult learning classes at the DEC. Topics across both undergraduate and graduate students included *malware, scams, deepfakes, digital footprints and privacy, social media hygiene, social engineering, and cyberbullying*.

In *malware* presentations, students covered definitions of malware and the various types of malware (e.g., viruses, trojans, worms, spyware, adware, bots, and ransomware), current malware prevalence trends, notable examples, and tactics used by cybercriminals to introduce malware into victims' devices (ex. phishing). Students shared the harms caused by malware (theft of sensitive information, computer performance, and spread/infection to other devices). Finally, students shared specific steps on how individuals could protect themselves from malware, such as keeping computers updated, using secure authorization methods, using safe browsing habits, thinking before clicking, and installing antivirus software.

Students covered the different platforms where *scams* occur, such as email, phone, and social media, and common types of scams, such as government scams (IRS, FBI, etc.) and romance scams via dating websites and apps. They discussed psychological persuasion techniques that explained why people fell for scams, such as playing on emotions, complying with authority figures, and responding to a sense of urgency. Students also shared tell-tale signs and scam detection tips, such as spelling and grammatical errors for emails and unknown numbers for vishing. Students shared tips on how to stay safe by limiting the information they shared online, not clicking on suspicious links, and not accepting follow requests from people they did not know. Finally, students shared tips on what individuals could do if they were victimized, such as contacting authorities, freezing credits, and auditing their social media accounts.

Students presenting on *deepfakes* shared the different types of frauds, such as textual deepfakes, deepfake videos and audios, deepfakes on social media, and real-time/live deepfakes. Students then shared the malicious uses of deepfakes with examples of how audio deepfakes had been used in financial crimes, intellectual property theft, and pornography. Students concluded with tips on spotting deepfakes, such as paying attention to side profiles, looking at the way mouths moved, and, in the case of live recordings, asking individuals/deepfakes to wave hands in front of their faces.

In *digital footprints and privacy* presentations, students explained that these were traces of an individual's online activity (social media posts and online purchases), which could be traced by anyone (e.g., employers, schools, cybercriminals). Students then distinguished between active and passive footprints, with the former being those intentionally left by an individual (social media post) and the latter being those left behind without individuals realizing (i.e., data collection via websites and apps, such as location data and facial recognition data). Students then discussed why digital footprints were relevant to an individual's privacy, how this information could be used to make decisions that impact individuals now and in the future. Students also shared strategies on how to maintain a clean digital footprint, such as cleaning up their phones and computers of unnecessary textual, audio, and visual data, and familiarizing themselves with privacy settings.

Students covering the *social media hygiene* topic shared some of the dangers associated with using these platforms

(ease of spreading malicious content, unknowingly disclosing location data, agreeing to invasive privacy statements). Students then shared the types of scams typically seen via social media (adware, tracking and influencing behavior, etc.). Students concluded by sharing safety tips, such as limiting personal information shared online, checking privacy settings, and reading privacy statements before agreeing.

For the *social engineering (SE)* topic, students discussed phishing, pretexting, vishing, and baiting. Students shared psychological persuasion techniques, such as authority (complying with those in positions of power), likeability (agreeing or complying with those who are charismatic and charming), rapport (establishing trust and friendliness), and reciprocity (individuals tend to help those who have helped them), which are leveraged by cybercriminals. Students also shared tips on how to avoid SE, such as not trusting strange emails or phone calls, not sharing sensitive information, and always double-checking with friends, family, and colleagues when emails appeared to be coming from them.

Students who presented on *cyberbullying* discussed the many ways it can manifest via an assortment of platforms. Students shared the reasons individuals might engage in cyberbullying, such as anger, revenge, boredom, peer pressure, and jealousy. Finally, students shared tips on how to manage cyberbullying, such as not engaging with the individual(s) targeting them, talking to a trusted adult or friend about messages they received, and blocking and reporting the individual(s) targeting them.

III. Student Reflections

The course project required both undergraduate and graduate students to reflect on the project, the value they got out of it, how it benefited the community, and feedback for improvement.

A. Value to Students

Students found this community engagement project to be valuable for multiple reasons. Many students noted that they do not often participate in public speaking or have anxiety surrounding it. This project took place after the 2020 COVID-19 shutdowns, so students were used to presenting virtually or turning their cameras off when speaking. This project took them out of their comfort zone to practice speaking in front of an audience. Students revealed that the informal nature of the presentations and the level of engagement from the audience made the presentations more conversational, which made them more comfortable speaking. One student commented, “It can be intimidating to stand in front of a group of people and present information, but by doing so, I was able to build confidence in myself and my abilities.” Public speaking is an integral skill that students will need regardless of their future career path.

To give meaningful presentations, students first had to learn about their topics. The knowledge that they were going to be presenting and answering questions on their topics motivated students to research and explore the material more than what was learned in class. This project allowed students to realize that “[...]the true test of knowing whether or not you truly understand a topic is being able to explain it simply to someone else.” When preparing to present on their topics, students not only had to learn complex information, but they also had to learn how to convey it simply. A student agreed, noting that the project taught them “how to effectively communicate complex topics in a way accessible to a wide range of people [and that] this will undoubtedly serve [them] personally and professionally in the future.”

Students valued the opportunity to directly give back to the community, establishing a level of trust and care. They felt the community appreciated the exchange of knowledge and students enjoyed the high levels of interaction and engagement they displayed. One student noted, “this response from them was a relief because it did not feel like we were intruding.” Most students do not often engage with the community in which their school is based. One student noted “it is nice to get out of the classroom and actually do things that have an impact on something beyond getting credit for my degree.” Relatedly, students often do not realize that they do not have to wait until they have their degree to be able to share knowledge that they learn. One student said that they realized, “I could help people right now. With my classes, I have been focusing on graduation and trying to get a job. My brain was so occupied with trying to find a job that I did not realize I could help people with what I learned from my classes.”

Engaging directly with the community also gave students a perspective outside of academia to understand how cyberhygiene and cybersecurity topics realistically impact people. Community members shared their personal stories related to these topics, which changed students’ perspectives on who may fall victim, how, and why. One student noted, “I used to think people who fell for romance scams are silly but from this project I've realized that scammers target the most vulnerable populations and use scary tactics to make themselves believable.” Even though this information is learned in class and from their research, hearing stories from people directly impacted by scams had a more profound impact than reading it in a book. Overall, students found this project to be a two-way interaction with the community. As one student reflects, adults in the community “opened their hearts to me and [gave] me their time so that I as a student can teach them a little bit of what I am learning.”

B. Value to Community

All students felt that the community benefited from learning about different aspects of cyberhygiene and cybersecurity. One student noted, “I think it is important for older people to understand the topics we were presenting because [many] scammers will go for their age group.”

Students also felt that generating a hearty discussion, where community members could ask questions or seek clarification, was important. Students were also mindful of the community's access to good information on cyberhygiene: "Since some people don't have access to things like classes on how to be safe online, especially in today's era. I think they benefitted a lot since they were filled with so many questions and were truly engaged in what we were presenting." Another student echoed this sentiment: "I personally desire that this initiative could reach more parts of [our community] in order to give information to more people who need it."

Students agreed that the presentations and corresponding discussions would make attendees think more about keeping not only themselves, but also their loved ones safe online. In short, attendees would take on the role of cybersecurity ambassadors and spread cyberhygiene awareness in their communities. One student stated, "I believe they took what we were teaching and they'll be able to take that new knowledge back into their homes and teach their friends and families these new things. In my case in particular – vishing – they'll tell their loved ones what makes up a vishing call, how they sound and how to avoid that interaction all together."

Students felt that attendees appreciated them sharing knowledge, interacting, and giving back to the community. One student said, "the relationships between [the] University and the surrounding… residents has not always been positive. This project has the potential for allowing the residents to see that we can be very respectful and of service to them." Another student felt similarly and said, "I felt that the members of the community were grateful to have [conversations about topics that are not] as common to learn about and make them feel like [university] students care about them because we do."

C. Feedback for Improvement

Both undergraduate and graduate students had several thoughts on improving this project. First, they wanted to be more knowledgeable about their own topics. While students could research their chosen topic independently, it would have made them feel more confident in answering any audience questions that did not come up in their own research. Some of the presentation topics were taught in class lessons, however not every group's topic was discussed in class. The former groups appeared to feel more confident in their presentations.

Students also wanted to spend more time learning how to improve the quality of their presentations, such as learning how to be more interactive with the audience, getting fellow students to ask questions during practice runs in class, seeing past student submissions to learn how to frame their own presentations effectively, and avoiding repeated topics between groups to give attendees a broader portfolio of cyberhygiene and cybersecurity topics.

Regarding time, students would like to see the time structure of the presentations reconfigured. A couple of students did not get the chance to share their work during the originally allotted presentation period. This was primarily due to the audience being exceedingly more engaged than expected, which led to many discussions. The discussions were fruitful and the engagement encouraging, so perhaps the program would benefit from two different presentation periods so that students can have time to thoroughly present their topics, and the audience can ask questions and engage in discussions without worrying about affecting the schedule.

Students would also like to see cultural literacy training for the students to learn how to better connect with the audience. These students go to school or even live in this community yet are detached from the local community members. Some students are culturally different than many audience members or have had few interactions with community members in the past. Some students (and subsequently the community) would benefit if they better understood how to speak and relate to the audience.

A final recommendation, which came specifically from the graduate students, was to have audience members submit requests for specific topics to be covered and for any specific questions they would like to be addressed beforehand so that the students can adequately prepare and meet the needs/requests of the audience. Not overlooking the fact that new questions will arise during the presentations, submitting even just some beforehand can help ensure adequate responses and could have the potential to solve some of the logistical time issues. This would also assist in selecting presentation topics.

IV. CONCLUSION

This paper shared a pilot cyberhygiene course project that was designed to expose students to experiential learning that encouraged community outreach and engagement in partnership with the DEC. It shared the reasoning behind the design and implementation of the project, the cyberhygiene projects developed by undergraduate and graduate students, and students' experiences. A logical question that follows is "was this beneficial to the community?"

A. Community responses to class project

One of the biggest hurdles in the community education space is that of mistrust, which can break down potential partnerships even before they are forged. Researchers should hold "themselves accountable for building trust" and move beyond addressing "theoretical questions that are not directly linked to problems of practice" [8, p.1]. The authors were intentional not to turn this community engagement project into a research project. As such, no formal evaluations for community members' experiences were done as they would be potentially considered 'research subjects;' the authors wanted to treat their community partners and members with respect and dignity, build trust, and use this pilot as a steppingstone to build trust and continue engagement. In

addition to the student experiences outlined above, the highly interactive nature of the discussions between students and community members could be taken as a good sign that the students' presentations were being appreciated. An informal chat with the community members revealed that they would like to continue this engagement with the students in the future. Community members should have an equal voice and shape the direction of the project if it is to truly benefit them [9].

B. Designing programs for students and communities

Developing a successful cyberhygiene awareness and training program has three steps: program design, awareness and training material development, and program implementation [10].

Awareness and training programs should be designed to reflect the organization's mission and culture and provide people with relevant subject matter [10]. In this case, the lead author wanted to create a course project at her home university that would not only benefit undergraduate and graduate students by allowing them to apply their knowledge and share with others, but also benefit the community where the general public would learn about cyberhygiene. Thus, the organizations whose missions and cultures had to be considered were higher education and community partners. The lead author then approached the Digital Equity Center (DEC) as their community partner (section II.A) to understand how this course project should be developed, who the audience was, and what topics might be of interest to community partners. The preliminary conversations with the DEC aligned nicely with the typical list of cyberhygiene topics found in research and through security websites, as noted in section II.B.

Typically, cyberhygiene awareness strategies include posters, videos, infographics, newsletters, guides, and tips, which help explain concepts and ideas while also teaching the ability to recall this information [10, 11]. More interactive aspects include workshops, in-person instructor-led sessions, phishing simulations, and computer games, which help individuals understand the concepts, develop their practical skills, and evaluate cyberhygiene actions [10, 11]. Instructor-led sessions can be interactive and use videos to effectively relay material, engage the audience, and retain their attention [10]. The authors chose a combination of awareness and interaction to serve as the mechanism through which cyberhygiene topics would be relayed.

The authors have also used this approach successfully in a myriad of contexts to offer awareness and training programs for educators [12], students and practitioners [13], and in after-school workshops for high school students [14].

III. Building on the DEC experience

The Fall 2022 and Spring 2023 pilot projects revealed that community members had specific questions about certain topics and devices, which might suggest the need for something more tailored to the community's needs rather than a generic set of topics.

One potential solution is the introduction of cyber clinics, which are designed using the model of mobile medical clinics that take public health approaches to 'treat' community members [7]. Community members would go through a triage-treat-and-train process in the cyber clinics. Members are first assessed for their baseline knowledge and cyberhygiene practices (triage) and then they receive custom-tailored guidance (treat and train) based on their triage findings [7]. These cyber clinics could be led by students (cyber medics) who are trained themselves at the start of the semester.

More importantly, these cyber clinics could be established at multiple venues in the community, such as senior citizens' residences, nonprofits and small businesses, and high schools. They should be designed also to serve underrepresented communities. Research suggests that American adults who are not digitally literate are typically less educated, older, and more likely to be Black, Hispanic, or foreign born [15]. By going out into communities and serving different demographics (age, race/ethnicity, education levels), higher education institutions, faculty, and students can start to build trust with the public, while simultaneously serving their specific needs.

IV. Conclusion

This paper highlighted one pilot project that sought to develop experiential learning projects for undergraduate and graduate students, while simultaneously benefiting the wider community via a cyberhygiene awareness training project. A strong student-faculty-community partnership is needed for such projects to take flight, have value, and build trust – this is an effort that extends well beyond the confines of traditional and higher education institutions. Cybersecurity is a *shared responsibility*; more work needs to be done to engage with the wider community if we are to bridge the 'town and gown' divide.

REFERENCES

[1] IC3 (2021). "2021 Internet Crime Report". Online at https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf. Retrieved February 2, 2023.

[2] USAID (2022). "Digital Literacy Primer". Online at https://www.usaid.gov/sites/default/files/2022-05/USAID_Digital_Literacy_Primer.pdf. Retrieved August 14, 2022.

[3] Ailoaiei, A. (2023). "What Is Digital Literacy and Why It's Crucial to Us Now". Online at https://www.cyberghostvpn.com/en_US/privacyhub/what-is-digital-literacy-and-why-its-crucial-to-us-now/. Retrieved February 2, 2023.

[4] Jones, A. (2022). "Temple University unveils Digital Equity Center". Online at https://www.phillytrib.com/news/local_news/temple-university-unveils-digital-equity-center/article_dfbd8767-ce7f-50fe-ab13-1f7d77d192d3.html. Retrieved August 14, 2022.

[5] Orbanek, S. (2022). "Temple University unveils new Digital Equity Center during first-ever Digital Equity Day as part of Technical.ly Philly's Philly Tech Week". Online at https://news.temple.edu/news/2022-06-21/we-are-committed-bridging-digital-divide. Retrieved September 1, 2023.

[6] Huffman, S. (2022). "Temple's new Digital Equity Center brings boosted computer access to surrounding neighborhoods". Online at https://technical.ly/diversity-equity-inclusion/temple-digital-equity-center/. Retrieved February 1, 2023.

[7] Croasdell, D., Elste, J., & Hill, A. (2018). Cyber clinics: Re-imagining cyber security awareness.
[8] Heath, D. (2017). "Mistrust: An Obstacle Standing Between Research and Practice". Online at http://www.research4schools.org/blog-post/mistrust-obstacle-standing-research-practice/. Retrieved February 2, 2023.
[9] Christopher, S., Watts, V., McCormick, A. K. H. G., & Young, S. (2008). Building and maintaining trust in a community-based participatory research partnership. American journal of public health, 98(8), 1398-1406.
[10] Wilson, M. & Hash, J. (2003). National Institute of Standards and Technology (NIST) Special Publication 800-50: Building an Information Technology Security Awareness and Training Program. Online at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf. Retrieved January 13, 2020.
[11] Stavrou, E. (2020). Back to Basics: Towards Building Societal Resilience Against a Cyber Pandemic. Journal on Systems, Cybernetics and Informatics, 18(7), pp. 73-80.
[12] Williams, K., Bleiman, R., & Rege, A. (2022). "Educating educators on social engineering: Experiences developing and implementing a social engineering workshop for all education levels". Proceedings from the 11th IEEE Integrated STEM Education Conference (ISEC).
[13] Rege, A., Nguyen, T., & Bleiman, R. (2020). "A social engineering awareness and training workshop for STEM students and practitioners". Proceedings from the 10th IEEE Integrated STEM Education Conference (ISEC).
[14] The CARE Lab (2021). "Social Engineering High School After-School Training Program". Online at https://sites.temple.edu/care/social-engineering/high-school/. Retrieved February 2, 2023.
[16] Mamedova, S., Pawlowski, E., & Hudson, L. (2018). "A Description of U.S. Adults Who Are Not Digitally Literate". Online at https://nces.ed.gov/pubs2018/2018161.pdf. Retrieved February 2, 2023.

ACKNOWLEDGEMENT

This work was supported by the National Science Foundation Award # 2032292.

AUTHOR INFORMATION

Aunshul Rege, Associate Professor, Department of Criminal Justice, Temple University.

Gabrielle Spence, PhD Student, Department of Criminal Justice, Temple University.

Rachel Bleiman, PhD Student, Department of Criminal Justice, Temple University.

Sean Mitchell, Technical Support Specialist, Temple University.

Jonathan Latko, Assistant Vice President, Business Operations, Temple University.