# Educating educators on social engineering: Experiences developing and implementing a social engineering workshop for all education levels

Katorah Williams, Rachel Bleiman, and Aunshul Rege
Temple University, Katorah.Williams, Rachel.Bleiman, Rege@temple.edu

*Abstract* - **There has been a noticeable increase in social engineering (SE) attack across the world, especially those that use phishing, vishing, and smshing. Despite the prevalence of cyberattacks that rely on these tactics and techniques, education about SE and how to defend against it is lacking. Instead, the focus of cybersecurity education has been heavily concentrated on technical skills. Recognizing that gap, this paper describes a case study of an attempt to improve SE education by hosting workshops for educators from diverse backgrounds. The workshop that was developed included education on the basics of SE and the psychology behind these attacks, the ethics around SE, and methods for implementing SE exercises in the classroom. Details are also provided on the experiences of those who attended the workshop. Lastly, challenges related to the implementation of the workshop are discussed as well as rationale for the continued use of workshops of this kind.**

*Index Terms* - Cybersecurity, Educators, Experiential learning and education, Social engineering

## INTRODUCTION

Social engineering (SE) can be defined as a form of psychological manipulation that influences someone to make an action or reveal information they otherwise would not have done and that may or may not be in their best interests [1]. While it is not always malicious, it is often used in the first steps of a cyberattack. It can be used to conduct reconnaissance (information gathering) on a target or, because humans are often and easily exploited in cyberattacks, to find a point of entry into a target's system. Some well-known forms of SE include phishing, in which someone tries to convince a target to click on a malicious link embedded in an email, or vishing, in which someone tries to convince their target to reveal personal information, such as their banking information, via a phone call. No person or organization is immune to SE. The Federal Bureau of Investigation's 2020 Internet Crime Report noted that the total financial loss from the SE tactics of business email compromise, phishing scams, and confidence fraud/romance scams totaled more than $2.52 billion [2]. While many companies have advanced technical defenses to thwart cyberattacks, awareness and training of SE is often absent or lacking, making it a common cause of successful attacks [3].

This paper details an effort to engage with educators about the relevance of SE and how to implement SE education into the classroom. The following section provides information on the importance of SE education and how those in non-technical fields can still engage in cybersecurity. The third section details how the authors developed and marketed the workshop, while the fourth section details participant attitudes and experiences regarding social engineering and completing the workshop. The paper concludes with a discussion of the challenges experienced and lessons learned during the development and implementation of this workshop.

## SE AWARENESS AND TRAINING

### *I. Importance of SE Training in Non-technical Fields*

As life, schools, and work have an increasing online presence, there exists a need for a holistic cybersecurity approach. Great strides have been made in technical cybersecurity efforts and cybercriminals have adapted to increasingly use non-technical attack vectors such as SE. SE awareness and training is instrumental as every online user is exposed to phishing, vishing, or other SE attacks. Furthermore, cybersecurity efforts can benefit from non-technical perspectives, such as psychology, business, or law, as they offer unique perspectives that can work in unison with existing technical cybersecurity practices.

People from all fields are exposed to SE, so people from all fields should be made aware and trained in it as well. However, people from non-technical backgrounds often feel as though they do not have the skills to be involved with cybersecurity, despite the relevance of SE for people from all backgrounds, both technical and non-technical [4]. This thought process needs to shift, so that students from non-technical fields graduate into the professional world with enough education and training to lower their (and others') susceptibility of falling for SE attacks. However, there exist relatively few programs that directly teach SE to technical students, let alone to non-technical or multidisciplinary students [5].

### *II. Importance of SE Training Across Education Levels*

While many organizations enforce SE awareness or training programs, such as phishing tests, it is not often taught in school curricula [5]. As the new generation of the cybersecurity workforce is being molded, all students need to learn about SE from both an offensive and defensive standpoint. Educational programs on SE are not currently commonplace, but SE should be emphasized in all education levels from middle/high school to higher education. While the extent of SE education is unclear, it can be logical to expect that SE is more common in higher education as it is a more specialized field. Even so, it is difficult to grow the field when students are not being introduced to it until they seek it out through higher education.

Instead, SE education should start as early as in K-12. Not only would this allow time for the material to be ingrained and become common knowledge but making SE accessible in early education would also introduce students to a field they otherwise may not have known even existed until they have already chosen a career path. The new generations of students entering the workforce are and will only continue to be more adept with and reliable on technology as compared to older generations, and it is important that they understand the risks associated with its use. This adeptness that new generations have with technology should only make this task less daunting, especially in comparison to training adults in non-technical domains. However, it is difficult to implement SE education programs when there is a deficit in educators who are properly trained to teach such information. Implementing SE education programs in schools must start with ensuring that educators are not only aware of SE, but that they are also properly trained in how to teach SE to their students. Educators in both K-12 and higher education lay the foundation for the future workforce, and they must be provided with adequate resources to properly train the next generation. While not every student will choose to become a cybersecurity professional, training educators to teach students about the basics of SE awareness offers the next generation knowledge of defensive cybersecurity measures, to protect themselves from being exploited in a SE cyberattack.

## SUMMER AND FALL EDUCATORS WORKSHOPS

While there are various opportunities to learn SE in different contexts, those opportunities often come with certain conditions, such as high costs from private education and technology vendors or being advertised to, or created for, those who are already working in cybersecurity and have large budgets; any and all of these caveats restrict educators' ability to access such workshops [6-7]. Recognizing this lack of access, the authors sought to develop a free, virtual SE workshop, which was held in the Summer of 2021 and again in the Fall of 2021. The workshops expanded the knowledge base by targeting the audience towards educators with a special focus on those in middle and high schools, as well as those in underserved communities.

### *I. Workshop Design and Development*

Given that the human factor is one of the most targeted yet overlooked components of cybersecurity, the authors wanted to develop a workshop that was both relevant and easy to adapt to different grade levels and education settings [8]. This was achieved by making sure to reference current events related to SE (vishing calls related to extended car warranties, smshing messages related to package deliveries or healthcare information) and providing hands-on activities where the educators had the opportunity to act as social engineers in a controlled setting that emphasized ethical behavior. Each workshop had 4 main components: Introduction to SE, SE case studies, Hands-on SE experience, and Ethics of SE, which are each described in greater detail below.

### *II. Intro to SE*

The workshops began with an introduction where participants were given a general overview of SE and its impact on society. Participants were also introduced to the psychology behind effective SE attacks, which highlighted the different personality types that are more or less susceptible to becoming victims of attacks and various principles of persuasion that are often used to sway a target into disclosing information or providing the access that cybercriminals seek. To demonstrate how these techniques look "in action," attendees were shown videos and examples of various course projects during which students tried their hand at SE and demonstrated the use of psychological persuasion techniques [9]. Lastly, attendees were shown examples of how various disciplines or subjects, such as art and psychology, can play a role in educating the public about the threat of and ways to protect oneself from SE.

### *III. SE Case Studies*

Next, attendees were shown a series of Institutional Review Board (IRB)-approved case studies based on class activities that had been previously implemented by one of the authors. During the Summer workshop, two case studies were presented. The first was a SE exercise, referred to as "shoulder surfing." Known as one of the oldest SE tactics, shoulder surfing refers to direct observations over someone else's shoulder to gather sensitive information [10]. Here, student teams targeted their classmates to capture photographs of each other using their devices. Each photo needed to have clear shots of the rival's screen [11]. During the presentation of this exercise, attendees were made aware of how this tactic can be used to steal pin numbers and passwords.

The second case study was a pretexting exercise. Pretexting is the act of credibly presenting oneself as someone else to obtain information [10]. In this exercise, student teams were tasked with creating a fake service or product to market to other students on campus. To provide a sense of legitimacy to their pretext and entice students to engage with them, teams were able to use props such as food or clipboards. During the marketing process, each team needed to convince unsuspecting students to sign a "terms and conditions" agreeing to the product; however, that document contained a "silly" embedded sentence in which student targets would unknowingly agree to perform certain tasks [12]. The objective was to demonstrate how easy it is to convince someone to sign a document and observe how often students read or do not read terms and conditions before signing them. During this exercise, workshop organizers stressed how easy it is to play on a person's beliefs or desire to help to manipulate them into giving an attacker vital information. With the terms and conditions exercise, emphasis was placed on how often we sign terms of conditions to use products and services, without knowing what is in these documents.

In the Fall, educators were presented with three case studies: "shoulder surfing," pretexting terms and conditions (both the same as the summer workshop), and a laptop distraction project. The laptop distraction case study detailed an exercise in which student teams were tasked with developing a pretext or credible story that was convincing enough to separate a team of information technology professionals from a test laptop, so that they could install a flash drive and extract a file. Each attempt was timed, and students were judged on the effectiveness of their pretext, not how successful they were at extracting the file [13].

At the end of each workshop, attendees were provided with student feedback about their experiences participating in each exercise, strategies and defensive tactics used, suggested project modifications, and the lessons learned from implementing the activity. Lastly, they were provided with copies of published papers that explained both the project implementation and student experiences in more detail for reference, should they choose to try these projects in their classrooms.

### *IV. Hands-on SE Experience*

Following an hour-long lunch break, attendees were given the opportunity to "become social engineers." Each workshop engaged in a different hands-on open-source intelligence (OSINT) gathering activity. OSINT is information gathering using legal and ethical public sources [14]. Those who participated in the summer workshop were given an activity that involved technical OSINT. Participants were broken down into teams and given a series of clues that required them to complete technical OSINT using search engines and other data sources to find the answers. The answer to each clue was a set of numbers. After solving each clue, teams were required to put the numbers together, which created a set of coordinates. They then needed to use those coordinates to do a second, technical OSINT, where they needed to identify a building at said location [15].

Fall workshop attendees participated in a different OSINT activity. Their activity was broken down into three parts. First, teams of attendees were given twenty minutes to conduct OSINT on the workshop organizers. During this time, they were tasked with finding CVs, social media accounts, information about recreational activities, or any other information that was not too sensitive or personal. The first part ended with workshop attendees sharing their findings and thoughts. Next, those same teams were tasked with selecting one of the workshop organizers and using their OSINT findings to develop a target profile for their selected workshop organizer. Using the information they found, they needed to develop a believable pretext that would convince their chosen target to engage with them. Lastly, using all the information gathered and their developed pretext, teams were asked to craft a phishing email that they would send to their chosen/targeted organizer.

### *V. Ethics of SE*

The final module of the workshop explained the ethics of developing and implementing projects of this magnitude. Here, attendees learned of the steps that one of the workshop organizers took to craft these course projects, including ensuring that the projects aligned with the SE code of ethics, that all projects were approved by the IRB, that students completed ethics training, and that all the necessary waivers signed by participants. At the end, attendees were able to ask questions and were given resources to access the class activities detailed during the workshop.

### *VI. Advertisements and Participant Selection*

Advertising for the workshop was done primarily online via Twitter, LinkedIn, and various education- and cybersecurity-focused listservs. Using these platforms allowed the authors to reach educators across the country and on different academic levels. Advertisements for the workshop were posted approximately 6 weeks before the date of the event and interested participants were asked to register for the chance to participate. To be eligible to participate, potential attendees were required to be full-time educators in high school or higher education and over the age of 18. They were also asked to submit their CV or resume, a brief letter of support from a department chair or school principal, and to sign an audio-visual waiver. The workshop was capped at 20 attendees to ensure better engagement and create a closer connection between organizers and attendees. It should be noted that high school educators were compensated for their participation at a rate of $25 per hour as a means of increasing their engagement.

Once the registration period was over, all applications were evaluated for completeness and alignment with the intended objectives of the workshop. In keeping with the authors' dedication to increasing diversity and equity in cybersecurity across racial, ethnic, gender, and education level and subject domain, the authors made every effort to include educators who are underrepresented minorities or those who teach at the high school or community college level. Selected participants were notified approximately 10-14 days before the workshop.

## PARTICIPANT EXPERIENCES

Workshop participants were required to complete a post-event survey about how knowledgeable they were about SE, if the workshop improved their knowledgeability, and which parts of the workshop were most beneficial. This information along with demographic information about workshop attendees is shared in the following section.

### *I. Attendee Demographic Information*

Thirty-five people registered to participate in the Summer workshop; 30 participants were accepted and 22 attended the workshop. Fifty-five percent of the participants self-identified as male, 36% as female, and 9% did not report their gender. Most of the attendees (32%) identified as White, 18% identified as Black, 18% identified as Asian, 14% identified Asian-American or Pacific Islander (AAPI), and 9% did not report their racial identity. Most attendees identified as either high school (36%) or undergraduate (36%) level educators, while 14% identified as community college educators, and 14% identified their educator level as "other." Included in the "other" category was a self-reported librarian and a K-12 educator.

Sixteen educators registered for the Fall workshop, and all 16 were accepted; however, only 9 educators attended the workshop. A majority of the attendees (78%) self-identified as male, while 22% self-identified as female. Most of the attendees identified as either Asian American-Pacific Islander or White (33% respectively), with a smaller percentage of attendees identifying themselves as Black (22%) or mixed (11%). Lastly, most of the educators in the workshop reported being college level educators (56%); however, there were some (44%) who reported being high school educators.

### *II. Participant Experiences*

Participant experiences with the workshop are based primarily on 17 post-event survey responses from the Summer workshop and 9 post-event survey responses from the Fall workshop. First, analysis was conducted on how the attendees felt about the structure of the workshop. Broadly, all attendees, regardless of which session they attended, had positive reviews and experiences with the workshop. All attendees (100%) from both workshops strongly agreed that the content of the workshop was relevant and that the presenters of the workshop were knowledgeable about the content they were discussing. Additionally, all attendees either strongly agreed (Summer: 88%; Fall: 100%) or somewhat agreed (Summer:12%) that the content was valuable to their teaching. When asked to rate the presenters, almost all attendees (Summer: 94%; Fall:100%) strongly agreed that the presenters were well prepared, and that the material was presented in a clear and concise manner (Summer: 94%; Fall: 89%).

When asked specifically about the modules presented during the workshop, attendees had varying responses. For example, all workshop attendees were asked to rate how beneficial each component of the workshop was. As compared to the Fall workshop, more attendees of the Summer workshop rated the Introduction to SE (82%), case studies (71%), and OSINT hands-on-activity (71%) as "extremely beneficial." In comparison, when the same question was posed to Fall workshop attendees, they rated the OSINT hands-on-activity (78%) and ethics in SE (56%) components "extremely beneficial." Given the popularity of the hands-on OSINT activities, it was no surprise that when asked what exercise(s) they were mostly likely to implement in their classrooms, educators in both workshops reported that the OSINT exercise was selected as the most likely to be implemented (Summer: 65%; Fall: 78%).

Lastly, participants were asked to rate their knowledge level and confidence in SE techniques, ethics surrounding SE, integrating SE in the classroom, and implementing experiential learning exercises. Figure I shows the reported differences in feeling very or extremely knowledgeable before and after attending the Summer workshop in each of

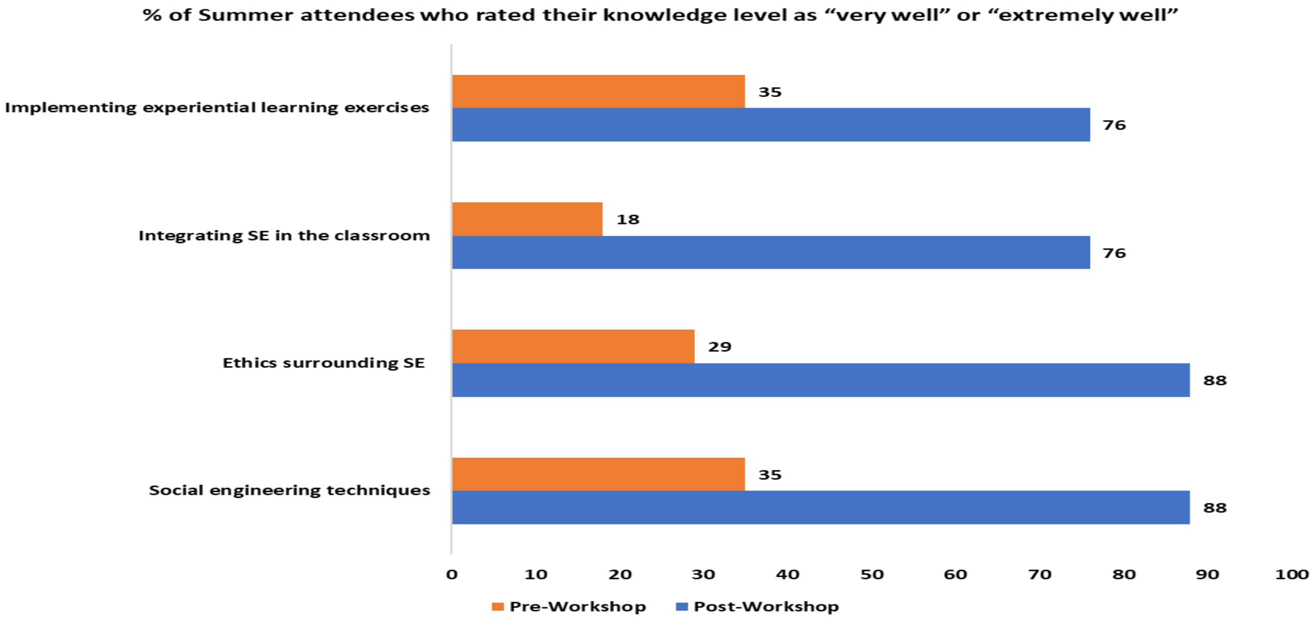

Figure I. Percent change in knowledgeability between pre-survey and post-survey for the Summer workshop.

the aforementioned categories. Looking at each component shows a marked improvement in knowledge and confidence across all categories. For example, when asked to rate how knowledgeable they were of SE techniques before the workshop, 12% of Summer workshop attendees reported being not well knowledgeable at all, 29% reported being slightly well knowledgeable, 24% reported being moderately well knowledgeable, 6% reported being very well knowledgeable, and 29% reported being extremely well knowledgeable. However, after completing the workshop, all of the Summer attendees reported an increase in knowledgeability, with 12% reporting being moderately well knowledgeable, 47% being very well knowledgeable, and 41% reporting being extremely well knowledgeable. This trend not only extended across all categories in the Summer workshop, but it was also evident in the consistent change of knowledgeability reported by Fall workshop attendees.

Figure II shows a similar increase in knowledgeability and confidence before and after the Fall workshop. For example, looking specifically at the category of integrating SE into the classroom, there was a dramatic increase in knowledgeability. Before the workshop, 22% considered themselves not well knowledgeable in how to integrate SE education into their classroom, another 22% considered themselves slightly well knowledgeable, 22% considered themselves moderately well knowledgeable, 22% considered themselves very well knowledgeable, and 11% considered themselves extremely well knowledgeable in this area. However, after the workshop, 11% reported being moderately well knowledgeable in how to integrate SE education into their classroom, 44% reported being very well knowledgeable, and another 44% reported being extremely well knowledgeable. Similar improvements are seen in the other three areas as well. These findings confirm that the workshops are beneficial in improving knowledge of and comfort with educating others about social engineering.

## CONCLUSIONS AND IMPLICATIONS

SE exposes the role that human behavior and interaction play in cyberattacks. Despite its importance, it is often given less attention than the more technical components of cyberattacks. Even less attention is given to SE in cybersecurity education [8]. Recognizing this gap, the authors sought to develop a workshop that exposes more educators to SE. This paper presents a detailed account of the development and implementation of the workshop and the experiences of the educators who attended. Overall, the workshops were effective at exposing educators to SE and providing resources for integrating SE exercises into the classroom. Results show a significant increase in knowledgeability about SE and interest in integrating SE activities into the classroom. Moreover, these findings not only signal that the authors have identified a gap in cybersecurity education, but also that educators are interested in learning about new ways to *teach* cybersecurity education.

The workshops provided four key benefits to attendees. First, they were able to learn basic information about SE and how it affects society. Beyond that, they were educated on the various types of SE, the tactics that are often used to convince unsuspecting targets to give up their private information, and how to connect those tactics to current events or scams. Second, attendees were provided with examples of what SE education could look like in a classroom setting. These examples demonstrated that SE education can be implemented in a classroom with few resources, and it does not require technical skills or expertise to teach. Third, by engaging in one of these exercises, attendees were able to make connections between the exercise objective and the material they teach.
Furthermore, the experiential-learning component reinforced the concepts that SE is relevant, transcends academic

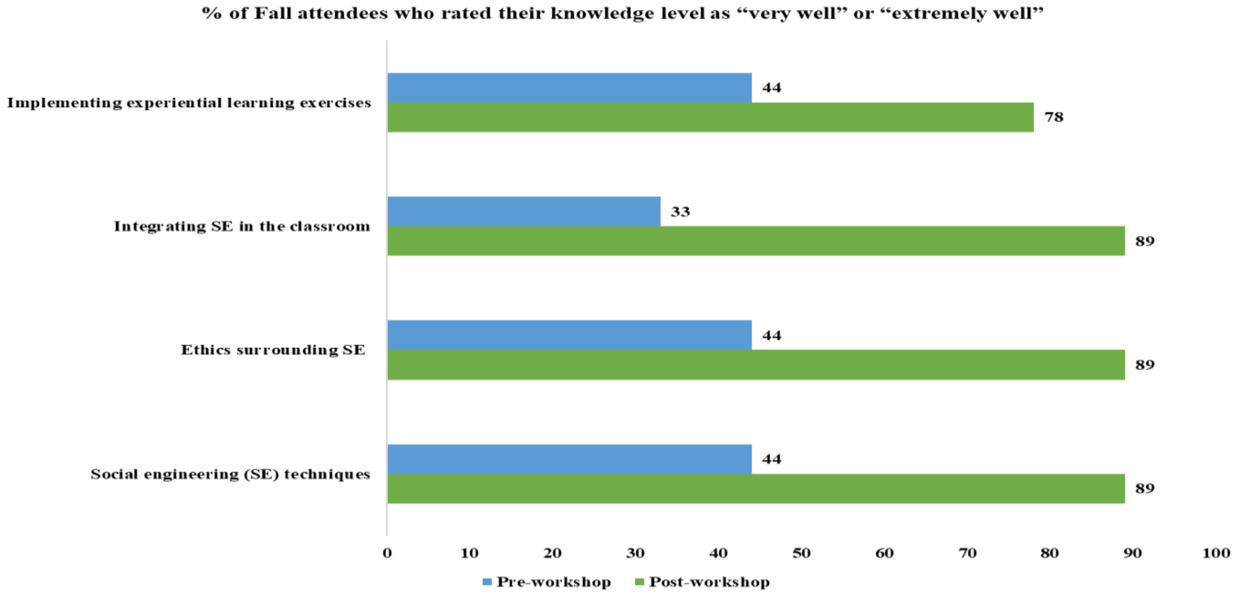

Figure II. Percent change in knowledgeability between pre-survey and post-survey for the Fall workshop.

subjects, and can be easily integrated into current curricula and lessons. Lastly, by learning the ethics of SE, the educators were given the resources to obtain all the necessary permissions needed to implement these exercises in a safe manner. Furthermore, as these educators become more well-versed in SE and its ethics, they can begin to develop their own experiential learning exercises where they expose their students to the different SE tactics.

Despite the success of the workshops, there were some challenges that the organizers faced regarding the survey instruments and recruitment strategies. Although important information was able to be gleaned from the data collected, there was still some data that the organizers wished they had collected and had questions they wished they had asked differently. For example, data was collected about how beneficial the case studies were as a whole, but no data was collected about each individual case study. Without this information, there is no way of knowing exactly which case studies were the most beneficial or most relevant and which should be removed for future workshops.

The challenges encountered during the recruitment process for this workshop related primarily to ensuring there was significant diversity among attendees. Despite having advertised on a diverse network of listservs and emailing lists, the racial and gender identity makeup of workshop attendees still skewed heavily towards those who identify as white and male. Furthermore, most of the participants reported they were educators at 4-year universities and almost all participants had taught subjects directly related to STEM or cybersecurity. Although the organizers are extremely grateful for all attendees and their interest in cybersecurity, the relatively homogenous makeup of the workshop signals that the developers need to create more innovative ways of reaching those in minority communities that are underrepresented in cybersecurity. Additional work is also needed to encourage educators of different educational backgrounds and disciplines to participate in this workshop.

Considering the role of the human factor in cyberattacks, efforts must be made to educate the public about ways to protect themselves [8]. These workshops were the authors' attempts to demonstrate how education about SE can be useful in preventing cyberattacks. Given that these were pilot workshops, the authors of this paper are encouraged by how beneficial the workshops were to the attendees. They are even more encouraged by the enthusiasm shown by attendees about implementing some of the SE exercises in the future. It is frequently stated that the best cybersecurity defense is an effective offense; by priming educators to integrate SE into their classrooms, students and eventually the general public not only become more aware of cyberattacks, but they eventually become better defenders against them.

## ACKNOWLEDGMENT

This work was supported by the National Science Foundation Award # 2032292. The authors thank their university's ethics board for guiding us to ensure that this workshop was be safe, ethical, and fun for all those involved. The authors also thank their university's Risk Management Unit for preparing all the forms necessary for this workshop. Finally, the authors thank their College's Marketing Unit for developing promotional materials that helped with advertising the workshop.

## REFERENCES

[1] Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Wiley.

[2] Federal Bureau of Investigation. (2020). 2020 Internet Crime Report. Retrieved January 21, 2022. Online at https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[3] Mitnick, K., & Simon, W. L. (2002). The art of deception. Indianapolis, IN: Wiley.

[4] Rege, A.& Bleiman, R. (forthcoming). Collegiate Social Engineering Capture the Flag Competition. Proceedings of the 2021 IEEE eCrime Researchers Summit.

[5] Twitchell, D. P. (2006). Social engineering in information assurance curricula. Proceedings of the ACM 3rd Annual Conference on Information Security Curriculum Development, 191-193. Retrieved from EBSCO database.

[6] Fruhlinger, J. (2021, October 26). *Cheap and free cybersecurity training: 8 ways to build skills without breaking the bank*. CSO Online. Retrieved January 21, 2022, from https://www.csoonline.com/article/3340819/cheap-or-free-cybersecurity-training-resources.html

[7] Marks, J. (2020, June 25). The cybersecurity 202: Few students are getting serious cybersecurity training. That's bad news for the U.S. workforce. The Washington Post. Retrieved January 21, 2022, from https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/06/25/the-cybersecurity-202-few-students-are-getting-serious-cybersecurity-training-that-s-bad-news-for-the-u-s-workforce/5ef3ec5f88e0fa7b44f67191/

[8] 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

[9] Rege, A., Williams, K., & Mendlein, A. (2019). "An experiential learning cybersecurity project for multiple STEM undergraduates". Proceedings of the 9th IEEE Integrated STEM Education Conference (ISEC).

[10] Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. *Information Resources Management Journal (IRMJ)*, 24(3), 1-8.

[11] Rege, A., Mendlein, A., & Williams, K. (2019). "Security and Privacy Education for STEM Undergraduates: A Shoulder Surfing Course Project". Proceedings of the IEEE Frontiers in Education.

[12] Williams, K., Ducoste, M., & Rege, A. (2020). "Educating multidisciplinary undergraduates on security and privacy". Proceedings of the IEEE Cyber Science Conference.

[13] Rege, A., Williams, K., & Mendlein, A. (2019). "A Social Engineering Course Project for Undergraduate Students Across Multiple Disciplines". Proceedings of the IEEE Cyber Science Conference.

[14] Steele, R.D. (1995) The importance of open source intelligence to the military. *International Journal of Intelligence and Counter Intelligence*, *8*(4), 457-470.

[15] Mendlein, A., Nguyen, T., & Rege, A. (2020). "Cybersecurity Awareness and Training Through a Multidisciplinary OSINT Course Project". Proceedings from the 2020 ASEE Annual Conference & Exposition.

## AUTHOR INFORMATION

**Katorah Williams,** PhD Student, Department of Criminal Justice, Temple University.

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

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