A social engineering awareness and training workshop for STEM students and practitioners

Aunshul Rege, Trinh Nguyen, and Rachel Bleiman
Temple University, rege, thuy-trinh.nguyen, rachel.bleiman@temple.edu

Abstract - **The human element is often regarded as the weakest link in cybersecurity, yet awareness and training efforts focus primarily on the technical aspects of cybersecurity and downplay the relevance of the human factor. One way to exploit this human vulnerability is through social engineering, in which cybercriminals utilize persuasion and manipulation of human behavior and psychology to convince individuals to reveal information, provide access or perform an action. This paper offers a case study on efforts to design and develop a social engineering awareness and training program that was implemented at the 2019 National Science Foundation Cybersecurity Summit using the National Institute of Standards and Technology framework for program development. This program was developed to enhance the ability for individuals in the future and current workforce to protect their organization against vulnerabilities to social engineering attacks, through corresponding awareness and training. The authors share the different stages that are involved in producing a successful program: designing the program, developing the awareness and training material, and implementing the program. In addition, this paper details the challenges and lessons the authors experienced and learned, which can be used as a guide for other practitioners to develop social engineering awareness and training programs.**

Index Terms - cybersecurity education, experiential learning, social engineering, STEM education

I. Introduction

In today's highly technologically interconnected work environment, organizations need to protect their data, assets, and services. The 'people' factor (not technology) is considered to be the weakest asset in attempting to keep an organization's systems and networks secure [1]. One way to exploit the human factor is via social engineering (SE), in which cybercriminals utilize persuasion and manipulation of human behavior and psychology to convince individuals to reveal information, provide access or perform an action that can then be used to initiate and/or maintain cyberattacks. Good awareness and training programs are instrumental in ensuring that people understand their organization's security policies and how to properly use and protect the organization's resources [1].

This paper shares one such effort to train the existing and future workforce across multiple disciplines on the relevance of the human factor in the area of cyberattacks and cybersecurity, through an awareness and training workshop. The next section provides a discussion on designing awareness and training programs and lists current social engineering awareness and training programs. In the third section, the authors detail the design, development, and implementation of the SE workshop. The next section details the experiences of the individuals who participated in the program. The authors end the paper by sharing the challenges the organizers experienced and the lessons learned in the development and implementation of this SE workshop.

II. Awareness and Training

According to the National Institute of Standards and Technology (NIST), awareness and training programs are crucial "vehicle[s] for disseminating information that [all] users need in order to do their jobs... [They are] *the* vehicles to communicate security requirements" across organizations [1, p.7].

NIST states that awareness efforts seek to change behavior and reinforce good practices [1]. Awareness programs focus attention on security where people are recipients of information [1]. Thus, awareness programs offer "basics and literacy material [which] is a core set of terms, topics, and concepts" [1, p. 9].

Training, according to NIST, aims to develop "relevant and needed security skills and competencies by practitioners of functional specialties" [1, p. 9]. In training, people have a more active role through which they develop skills and competencies that build on the basic knowledge acquired through awareness programs [1].

A. Designing Awareness and Training Programs

Developing a successful cybersecurity awareness and training program has three steps: (i) designing the program, (ii) developing the awareness and training material, and (iii) implementing the program [1]. Awareness and training programs should be designed to reflect the organization's mission and culture, and also provide people with relevant subject matter [1].

After the design process, the corresponding awareness and training material should be developed and address which skills organizations want their employees to learn and apply [1]. Also, materials should cater to *both* awareness and training. Awareness material should address a series of topics or a specific topic [1]. Awareness materials could include

978-1-7281-7520-1/20/$31.00 ©2020 IEEE

seminars and short courses that do not overwhelm the audience [1].

Training material is more in-depth and can build on the awareness material [1]. Organizations can use 'off-the-shelf' training materials developed by other agencies or develop their training materials in-house [1].

The last stage in designing the awareness and training program is its implementation. Techniques for implementation can include posters, videos, newsletters, and in-person instructor-led sessions to name a few [1]. The instructor-led sessions have the advantage of being interactive, and can also be blended with videos to effectively present material and retain the audience's attention [1].

After implementation, organizations should seek feedback and evaluation to determine whether the existing program is working and what improvements are necessary [1]. These feedback approaches should address quality, scope, level of difficulty, duration of session, relevancy, and suggestions for modification [1]. Evaluation and feedback can be obtained via questionnaires, focus groups, observations, and formal reports [1].

B. Existing Social Engineering (SE) Awareness and Training Programs

As noted above, the human factor is often considered to be the weakest link in cyberattacks. One way this human factor is exploited is through a process called social engineering (SE). SE is defined as "any act that influences a person to take an action that may or may not be in his or her best interests" [2, pp. 23]. SE involves employing "human skills and persuasion techniques to obtain unauthorized information" [3, pp. 29]. Thus, educating humans about SE via effective awareness and training programs is crucial. There are various sources of SE awareness and training in the United States.

The SE Village at DefCon offers a combination of conference style SE talks and a hands-on SE competition, where participants try vishing (SE via the phone) [4]. The Layer8 conference is the first conference that is solely focused on SE and intelligence gathering [5]. This event offers SE talks, hands-on workshops, and small-scale competitions [5].

Specialized SE courses and training are also available through Social Engineer Inc. and the SANS Institute. These courses cover topics such as Open Source Intelligence (OSINT), introduction to communication styles, psychological manipulation techniques, reconnaissance, and phishing [6, 7].

SE video podcasts have emerged more recently and serve as excellent awareness programs. Layer8's podcast series shares the experiences and stories of professional social engineers [8]. OSINTCurio.us offers weekly videos and podcasts on an assortment of tools that can be used to conduct OSINT and several case studies where these tools have been used successfully [9].

Each of the SE awareness and training programs/events listed above is an excellent source that provides participants with awareness (podcasts, conferences) and hands-on experiences (conferences and training) in SE. These programs/events provided inspiration for a SE awareness and training program that was developed and implemented at the 2019 National Science Foundation Cybersecurity Summit.

III. SE AWARENESS AND TRAINING AT THE 2019 NSF CYBERSECURITY SUMMIT

A goal of the National Science Foundation (NSF) is to support trustworthy science through cyberinfrastructure. Trusted Cyber Infrastructure (CI), the NSF Cybersecurity Center of Excellence is comprised of a team of cybersecurity experts whose goal is to train and disseminate experiences on cyberinfrastructure using the best practices [10]. The 2019 NSF Cybersecurity Summit provided a space for organizers to carry out these goals by inviting submissions for talks and workshop proposals.

In response to this call for workshop proposals, the authors developed a SE awareness and training workshop and used the aforementioned NIST framework to develop a successful cybersecurity awareness and training program. The first stage of the process, designing the program, considered Trusted CI's 2018 report on the lack of emphasis on the human factor in security events [11]. In completing stage two of developing the awareness and training material, the workshop emphasized disseminating awareness information on styles of SE attacks, principles of persuasion, and target personality types, as well as developing hands-on SE training material. Lastly, stage three, implementing the program, involved an instructor-led session with group-based activities that kept the participants engaged with the use of their knowledge on the awareness material.

A. Designing the Program

Trusted CI's report from the 2018 NSF Cybersecurity Summit had several key observations, one of which was about the human factor. The report stated that the "human factor in security events is continually overlooked. The community needs to better understand the interaction between humans and security" [11, p. 4]. More specifically, the report indicated that awareness and training programs should move beyond simply educating the user; programs should be evaluated to determine how "awareness is disseminated and what is included within the disseminated information" [11, p. 12]. One of Trusted CI's specific missions was to focus on the human factor, and as such, the authors designed a SE workshop that spoke to this specific mission.

B. Developing Awareness Material

The workshop organizers developed awareness and training material as part of step two in the NIST framework, with the aim for participants to gain basic knowledge and skills.

The authors developed materials on SE attack styles, principles of persuasion, and target personality types, and showcased two case studies to demonstrate the application of

SE. The methods of attack included baiting, phishing, spear phishing, vishing, quid pro quo, pretexting, and shoulder surfing. *Baiting* exploits human curiosity by baiting people with infected devices, such as a flash drive, to be injected into and infect their own devices [12]. *Phishing* is a SE method that attempts to trick users into revealing sensitive information, such as usernames and passwords [12]. *Spear phishing* is similar, yet it is more complex and targets a specific person within an organization [12]. *Vishing* is an attack style during which attackers pose as representatives from companies and attempt to gain the targets' information through phone calls [12]. *Quid pro quo* features attackers offering something desirable in exchange for users' information; these data are collected and then used for identity theft [12]. *Pretexting* requires attackers to present themselves as someone else in a specific situation to obtain information from targets [12]. Lastly, *shoulder surfing* is a method through which sensitive information can be gathered about people by looking over their shoulders at their personal devices without their knowledge and consent [12].

The principles of persuasion discussed in the awareness training included authority, commitment, consistency, reciprocity, likeness or commonality, scarcity, social proof, and a natural inclination to help. Attackers who utilize *authority* as a principle of persuasion rely on the victim's willingness to comply to authorities, despite their own personal ethics [13]. *Commitment* is used to persuade victims by targeting their beliefs and commitments, and *consistency* relies on the fact that people act and behave in a manner consistent with their beliefs [13]. *Reciprocity* relies on the fact that people are likely to return favors when one is given to them [13]. *Likeness or commonality* is used when perceived similarities between the attacker and victim enhances the victim's compliance [13]. *Scarcity* persuades people through offering opportunities or objects that are seen as less available or highly valuable [13]. *Social proof* exploits the tendency that people are more likely to comply to a request if others have already done the same [13]. Lastly, attackers can persuade their targets to help them execute their attack by posing as someone in need of assistance, as people have a *natural inclination to help* others who are in need [13].

The types of personalities that affect how a person is targeted include individuals who are conscientious, extroverted, agreeable, and neurotic [13]. Attackers target people who are *conscientious* and tend to follow rules by exploiting social norms [13]. *Extroverted* people are targeted with SE attacks that leverage social relationships, as they are more likely to cooperate than introverts [13]. People who are *agreeable* and more trusting are targeted because they have a higher likelihood of disclosing personal information [13]. The last personality trait, *neuroticism*, serves as a protective factor from SE attacks because these potential victims are more cautious [13].

The authors also decided to include two case studies that would demonstrate the application of SE. These case studies were from prior training exercises led by one of the authors that involved participants working in teams to complete hands-on SE activities.

The first case study focused on social engineering. Each team was to target rival team members by capturing photographs of them using their devices, with the screen clearly shown in the picture. Each team shared its successes, failures, challenges, strategies, and lessons learned. Specific strategies used by teams were offensive and defensive in nature. Offensive strategies that students used included 'light stalking' as well as 'honey pots', which is a type of baiting. Defensively, students decreased their screen use or hid against walls to prevent from becoming targets [12].

The second case study focused on pretexting. Each group created a fake product that required targets to agree to a bogus terms and conditions document to receive that product. The document embedded a funny or silly statement within it. Each group convinced targets to sign the document and observed whether they read (and caught) the embedded sentence.

Both case studies were chosen to demonstrate the applications of SE techniques (shoulder surfing and pretexting) and also to give workshop participants an idea of what the hands-on projects would entail.

This introduction provided the participants with an overview of SE; it served as a source of informational awareness material yet was brief enough to not overwhelm the audience. Building on this introductory awareness material was training material that covered the SE topics in more depth.

C. Developing Training Material

The training material was developed into hands-on projects for the audience to complete, using what they had previously learned from the awareness material.

The trainers developed five hands-on SE group projects, each requiring the use of at least one SE strategy that was discussed in the introductory awareness material. The objective of each project was to complete a task through the use of pretexting. The *first* task was for a team to send the workshop developer an email from someone else's phone but using one of their own email addresses. The *second* task was for a team to convince a rival team member to use a predetermined prop. As part of the task, the team also had to capture a photograph of their success. The *third* task required a team to identify the real identities of rival team members, as everyone used an alias throughout the duration of the workshop. The *fourth* task was for a team to convince rival team members to disclose a specific piece of sensitive information, and capture a voice recording of the disclosure. The *fifth* and final task was for a team to determine where the other rival team members lived and identify who lived furthest away from the location of the conference. All the projects were approved by the university's ethics board.

After the completion of the hands-on training projects, the audience collectively generated prevention measures through an interactive portion at the end of the workshop that served as an additional training mechanism.

At the end of the workshop, each group completed a report detailing their experience, successes, and failures from the hands-on portion, which were later scored by the workshop developers. The group that was most successful in completing the hands-on portion of the training and who received the highest score on the report was awarded portable chargers as a prize. This served to encourage attendees to stay and participate for the entire duration of the workshop, and it also brought about a healthy competitive spirit.

D. Implementing the Program

The format of the SE awareness and training workshop was multifaceted to provide an experiential learning environment, which catered to the varied backgrounds of the attendees. A total of 14 individuals attended the awareness and training session, and the attendees were comprised of a mixture of working professionals and students across various STEM fields (engineering, computer science, law and policy, and social science). The workshop was presented in-person for a total duration of 3.5 hours. The structure of the workshop consisted of several presentations, open-focus group style discussions, and a hands-on project. Additionally, video content was weaved into the powerpoint topics to keep the audience engaged. Prior to the commencement of the workshop, the facilitators informed the attendees that the activities included in the training were approved by the university's ethics board. As each attendee entered the workshop, they were instructed to create an alias and had to remain in character until after the debriefing of the hands-on project.

The hands-on SE project was group-based and concluded with deliverables in the format of a formal report. All attendees who remained for the hands-on project were randomly divided into five groups. Envelopes with specific instructions outlining the different tasks for the hands-on activity were given to each group. The groups were also required to complete a formal report; they had to document their successes and failures, SE strategies, division of labor, and obstacles and adaptations while completing their assigned task. Additionally, they had to conclude their reports with recommendations for prevention measures against SE attacks and provide general feedback on their experience. The attendees had a total of 50 minutes to complete the SE project; the allotted time was organized into 10 minutes for preparation, 30 minutes to execute the tasks, and 20 minutes to debrief and begin filling out their report.

The last component of the workshop included a collective training opportunity on preventative measures against SE attacks. The organizers generated a live documentation of the audience's suggestions on preventative strategies and put it on display. Some of the preventative measures generated by the audience included the following: acting out scenarios to show the consequences of becoming a victim to SE, confirming origins of requests, avoiding using email to send private information, being wary of posting information on online platforms, spreading awareness of how basic information can be used maliciously, and prioritizing and identifying the threats that are not commonly known.

An important element in the last stage of implementing an awareness and training program is feedback; therefore, the hands-on project was concluded with an open discussion on the attendees' overall experiences and suggestions for improving the workshop. The groups were given time to submit their final reports the following day for the facilitators to assess final group scores.

IV. Participant Experiences

Overall, the attendees indicated in their formal reports that they had a positive experience and found the SE workshop to be interactive and informative. All the attendees enjoyed the hands-on projects and reported their successes and failures, SE strategies, division of labor, and specific challenges they experienced individually and in each of their groups. While the attendees reported they had a valuable experience, a minor suggestion for future iterations of the workshop was to allow more time for the hands-on project.

The teams provided their successes and failures in their formal reports, detailed in Table I below.

TABLE I
SUCCESSES AND FAILURES

Task	# Successes	# Failures
1. Send email	1	3
2. Prop picture	2	2
3. Find real identities	2	2
4. Record sensitive info	3	5
5. Who lives furthest away	10	0

The teams also reported on strategies they used. Two of the five teams did not use any strategies. The other three teams used pretexting and at least one additional strategy such as quid pro quo or shoulder surfing. Team five, who had to determine who lived the furthest away, used the strategy of quid pro quo to determine who lived furthest away. They allowed another team to use them as a target and in return, were able to target that team. They reported "the first person targeted wanted to log in to their email address. Their email address revealed their city".

The division of labor for each team varied for each group, but each group worked together to overcome obstacles during the hands-on project. The participants reported experiencing several challenges, but some groups were able to develop strategies to overcome them. A primary obstacle the attendees experienced was the atmosphere of the workshop. The nature of implementing a SE-based program created an environment where participants had the knowledge that someone was actively trying to make them the target of a SE attack. Therefore, attendees had a lack of trust among one another; potential targets lied or avoided engaging in conversations entirely. For instance, team two reported "the biggest obstacle was that we were in a seminar on social engineering, and so even basic requests and conversations were met [with]

extreme skepticism." Additionally, another challenge the participants expressed was effectively implementing a pretext, such as developing a convincing backstory, remaining in character, and retrieving information in a subtle manner. Team one, who had to send an email from another attendee's phone, provided an example of the difficulties it had with its pretexts. One of its targets asked, "You have your own phone, why [do] you need mine?". Team one realized its approach "[l]acked credibility… [and that it needed] a better back-story." While the groups each experienced challenges, some adapted additional strategies to complete their tasks. For example, team three, who had to uncover the real identifies of other attendees, quickly realized the pretexts they developed were not sufficient and instead utilized shoulder surfing, a strategy they learned through the awareness segment of the workshop. In addition, team two reported a broad range of additional strategies stating, "we defaulted towards stonewalling any form of questioning, feigning ignorance, answering with jokes, or otherwise deflecting responses to be as unhelpful as possible." Thus the workshop participants used an interesting mix of offensive and defensive strategies to engage in the hands-on SE activities.

V. Conclusion

This paper presents a detailed approach to designing awareness and training programs focused on the importance of the human factor in cyberattacks and describes the dissemination process of information to the future workforce in cybersecurity. While there were some challenges to designing, developing, and implementing the program, the overall workshop was successful and provided a beneficial experience for individuals who attended. Therefore, organizations must be proactive in adopting awareness and training programs that effectively enhance the knowledge and behaviors surrounding security measures, specifically on the relevancy of the human factor.

The awareness and training workshop provided three key benefits for the attendees. The program familiarized individuals on crucial SE topics to enhance awareness, such as SE attack methods and common characteristics of targets. Participants were then immediately able to utilize this information and directly apply it in a hands-on training activity. Additionally, the open-discussion format of the program provided an opportunity for participants to reflect on their experience with other working professionals and students in the field of cybersecurity.

While the NIST framework offers an efficient approach to creating a successful cybersecurity awareness and training program, the authors experienced three challenges and learned valuable lessons. First, the authors had to carefully compose a hands-on activity based on SE tactics that would be approved by their home institution's ethics board. Second, the organizers had to design projects that were logical in a conference setting and adaptable to unanticipated events. The relationship between the participants, either as strangers or acquaintances, would directly impact the implementation of the hands-on SE project. With those factors considered in the designing stage of the program, the organizers were able to quickly divide the participants into groups after determining which working professionals and students were acquaintances on the day of the workshop. This would also ensure that none of the teams had an unfair advantage in completing their tasks. Finally, although many participants indicated they had a positive experience, the organizers had hoped for more detailed feedback that could be used to improve future iterations of the program. The NSF coordinators administered a survey at the end of the summit, but the response rate for feedback directed at the SE workshop was low. A post-survey had not been developed for the program to avoid saturating the conference's survey and overwhelming the workshop participants. In the future, the organizers suggest placing more emphasis on the feedback aspect of the project deliverables.

The authors want to encourage the development of more awareness and training programs for cybersecurity that emphasize the human factor because it is the weakest link in cyberattacks [1]. Additionally, these programs should be periodically reinforced as participants may forget or revert to old habits after training completion. The security of organizations and all individuals are vulnerable to SE attacks. Therefore, these programs are critical tools that will enable individuals in the current and future workforce across multiple disciplines to be more equipped to protect their organization's resources. Moreover, the NIST framework for designing awareness and training programs lays the necessary foundation to creating programs that will produce effectual changes in cybersecurity.

Acknowledgments

This material is based upon work supported by the National Science Foundation CAREER Award, Grant No. 1453040. The authors thank the University's ethics board for guiding us to ensure that this project would be safe, ethical and fun for all those involved. Finally, the authors thank the NSF Cybersecurity Summit Program Committee for granting us permission to use our social engineering workshop as a case study for this paper.

References

[1] 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

[2] Hadnagy, C. (2018). Social engineering: The art of human hacking. Indianapolis, Indiana: Wiley Publishing Inc.

[3] Jakobsson, M. (2016). Understanding social engineering based scams. New York, New York: Springer.

[4] Social-Engineer.org (2020). "SEVillage at DefCon". Online at https://www.social-engineer.org/sevillage-def-con/

[5] Layer8.com (2020). "Layer8 Conference: About Us". Online at "https://layer8conference.com/about-us/"

[6] Social-Engineer.org (2020). “Social Engineering Training”. Online at https://www.social-engineer.com/social-engineering-training/

[7] SANS (2020). “SEC567: Social Engineering for Penetration Testers”. Online at https://www.sans.org/course/social-engineering-for-penetration-testers

[8] Layer8.com (2020). “The Layer 8 Podcast”. Online at https://layer8conference.com/the-layer-8-podcast/

[9] OSINTCurio.us (2020). “OSINT Videos and Podcasts”. Online at https://osintcurio.us/osintvideosandpodcasts/

[10] Adams, A., Avila, K., Basney, J., Brunson, D., Cowles, R., Dopheide, J., Fleury, T., Heymann, E., Hudson, F., Jackson, C., Kiser, R., Krenz, M., Marsteller, J., Miller, B.P., Piesert, S., Russell, S., Sons, S., Welch, V., & Zage, J. (2019). "Trusted CI Experiences in Cybersecurity and Service to Open Science". In PEARC'19: Practice and Experience in Advanced Research Computing, July 28-August 1, 2019, Chicago, IL, USA. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3332186.3340601

[11] Trusted CI. (2018). “The Report of the 2018 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure”. Trusted CI: The National Cybersecurity Center of Excellence. Online at https://scholarworks.iu.edu/dspace/handle/2022/22588

[12] 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.

[13] Uebelacker, S. & Quiel, S. (2014). The Social Engineering Personality Framework. Online at https://www.researchgate.net/publication/271135217_The_Social_Engineering_Personality_Framework

AUTHOR INFORMATION

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

Trinh Nguyen, PhD Student, Department of Criminal Justice, Temple University.

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