Securing Every Link: Expanding Cybersecurity Education to the General Public

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Michelle Nguyen
Spring 2024
Department of Computer Science

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Briana Morrison, Department of Computer Science

Securing Every Link: Expanding Cybersecurity Education to the General Public

CS4991 Capstone Report, 2024

Michelle Nguyen
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
mtn7vez@virginia.edu

ABSTRACT
As reliance on technology grows, cyberattacks become increasingly dangerous and costly. Although many technical measures can be put in place to prevent such attacks, human users themselves are often a major point of weakness. To address this, I propose that cybersecurity education be treated as an important facet of cyber defense by expanding it beyond schools and businesses to the public in various ways, with a focus on workshops helmed by qualified students. Workshops like these could be run by students under the supervision of a professor teaching the basics of personal cybersecurity. To determine the potential efficacy of such programs, I reviewed research on prior methods for teaching cybersecurity and similar computing-related subjects, such as public service announcements and games. I anticipate that a workshop program such as this could benefit both the attendees and the workshop students in that both would be honing their cybersecurity skills. In the future, this proposal could be properly tested by implementing it in a real-world setting, at UVa or at a community center.

1. INTRODUCTION

Due to the increasing importance of cybersecurity, engineers and security officials have placed much focus on creating advanced tools to aid in cyber defense, which alone may not be sufficient. These tools, including those using artificial intelligence, may provide substantial protection from some threats, but they cannot reinforce cybersecurity's weakest link—human users.

The 2013 Target data breach, in which up to 110 million customers' information was stolen, began as a simple phishing email (US Senate, 2014). Even outside the context of a large company, individuals in an increasingly online society are faced with cybersecurity threats daily. To address this, different parties have made efforts to raise awareness of cybersecurity knowledge in the public, with varying degrees of success.

2. RELATED WORKS

In gathering relevant information on the efficacy of cybersecurity training, Bada and colleagues' analysis (2019) of existing methods discusses features that are required for the public to embrace security measures. An initial step to any general cybersecurity program would be to raise awareness of the topic and introduce the public to common safety tools and methods they can employ. However, this alone is not effective. Bada, et al. found that, while an individual may correctly answer security-related questions, they may not be motivated to incorporate safe behaviors into their daily routine. They found that using fear as a motivator is unhelpful,

often deterring individuals from safe practices. The programs I propose will address this issue.

Analysis of established training programs also aids me in proposing a design. Kweon, et al. (2021) studied the effects of information security training and education (ISTE) on reported security incidents, finding that increased ISTE mitigated security risks. Training seminars, then, can be an effective method of teaching cybersecurity.

Certain public schools in Texas adopted a more distinct form of encouraging safe cybersecurity practices by adopting a mandatory gamified curriculum. In their study, Meadows and Sambasivam (2023) found that gamification, when done correctly, could encourage safe habits. Additionally, middle school aged children were receptive to the curricula, but only through repetition. These prior works provide a helpful framework for my program proposal and inform the features it may need.

3. PROPOSED DESIGN

I propose a series of hour-long workshops led by college students studying computer science under the guidance of a cybersecurity professor. Aside from a student's personal intrinsic motivation, a professor could incentivize students to participate if they implement the workshops as a project or as an extra credit activity. The curriculum would be developed by the professor with input from their students, which would ensure that the material is both accurate and relevant to a targeted audience. Having a group of students lead each session would create a smaller participant-teacher ratio, allowing the participants to get more individualized help than they would with a single professor. Each workshop series itself would comprise at least five sessions to enforce learning through repetition and encourage the building of safe personal security habits.

Each session would have two parts: a fifteen-to-twenty-minute lecture and an interactive segment. Students would act as lecturers during the first half of the session to raise awareness of personal cybersecurity issues. These lectures would emulate the ones given in a classroom setting and would give the audience the rationale behind certain secure behaviors.

Because awareness alone is not enough to encourage the formation of safe habits regarding cybersecurity (Bada, et al., 2019), the interactive segment that followed would serve to teach these habits in a personally engaging way. Student teachers would explain personal safety procedures as simply as possible to mitigate audience resistance to a new workflow. These segments would allow the audience to practice safe behaviors in small groups or on their own with aid from the student instructors. Additionally, they could incorporate elements of gamification. Meadows and Sambasivam (2023) describe card games, tabletop games, and online video games as being effective at teaching cybersecurity. Such games could be implemented in these segments on a small scale. By introducing participants to simple educational games, participants could be incentivized to continue learning personal security skills by engaging with the games outside of the workshops.

3.1 Audience Variations

Because the needs of children and adults differ, the workshops could be formatted for each of them as two different audiences. Meadows and Sambasivam (2023) found that, because children begin to expand their technological horizons in middle school, it is a promising time to teach them safe online skills. Children have fewer habits to unlearn, which allows them to learn healthy behaviors from the beginning. Schools interested in this

program could implement workshops targeted toward children into their curriculum, which would ensure that there are repeated sessions each student is expected to attend. With the guarantee that most students will be attending each session, the professor can write the curriculum to be continuous and build on prior knowledge.

Workshops for adults could be held in community centers such as libraries or universities and advertised as a series on the internet. Because attendance cannot be compelled, the professor must take care to create workshops that are not so interconnected that they alienate new participants, but not so similar that each workshop is the same for returning participants. These workshops would not only aim to teach participants to protect themselves, but could train parents to teach their children and other family members safe security habits.

3.2 Curriculum

Organizers could derive the curriculum for these workshops from certain portions of introductory cybersecurity courses at UVa, such as CS 3710: Introduction to Cybersecurity. Professors and students could identify the most relevant portions of the course for general audiences and add current best practices in personal cybersecurity, including the creation of strong passwords, phishing, and common internet scams.

4 ANTICIPATED RESULTS

I anticipate that such a workshop program could moderately improve the cybersecurity habits of its audiences, which could be measured by comparing the results of a survey or questionnaire taken during the first workshop with one taken a few weeks to months after the conclusion of the program. Such a survey would include questions regarding best practices to assess general awareness and questions regarding individuals' personal cybersecurity practices to assess the participants' habits as a group. Due to the middle school audience's mandatory attendance and the lack of unsafe habits for children to unlearn, I suspect that the middle school workshops will be more effective than adult workshops.

The results of an evaluation completed after the program ended could also inform organizers about what skills were more difficult to teach and less likely to be retained by the participants once the workshops concluded. Such a questionnaire could then inform future research on the topic, to encourage safe cybersecurity habits more comprehensively and via different methods.

I also anticipate positive results for the students who lead the workshops, which guiding professors could measure qualitatively. Students teaching common personal security skills to participants would have heightened awareness of the rationale behind such skills and be encouraged by repetition to adopt these habits themselves. Students teaching personal security skills to the public would better their own cybersecurity knowledge alongside the participants.

5 CONCLUSION

Given the prevalence of personal technology and thus the increased risk of online threats, it is paramount that the public is educated on best practices regarding cyber safety. Raising awareness of safe behaviors would not only benefit individuals, but would also aid in preventing large-scale cyberattacks where a single employee is exploited to damage a large organization. Implementing a free workshop system targeted at different audiences would create accessible areas to learn safe practices for populations who may be vulnerable or easily targeted, including children and older adults. By drawing curricula from existing

cybersecurity classes, my workshop proposal would ensure that participants receive accurate, updated information. Participants could build lasting healthy habits through gamification and repetition within the workshops. Finally, by allowing student volunteers to lead the workshops, participating professors would encourage their own students' mastery over introductory cybersecurity topics and best personal practices. While the creation of safeguards in technology is important for cybersecurity, education and human actions also play a significant role in determining how safe the online world is.

6 FUTURE WORK

The next step in following through with this proposal is to formalize separate curricula for children and different audiences of adults. The bases for these curricula could stem from simplifying material from introductory cybersecurity classes and include elements of gamification. After formally proposing the workshops and acquiring student volunteers, a professor could pilot the workshops in university classrooms or community centers.

These pilot workshops would provide feedback in the form of evaluations completed by participants after the workshops. Researchers could use evaluation results to compare the efficacy of the workshop proposal with traditional cybersecurity education efforts such as online campaigns and current technology curricula. The program could then be revised as needed.

REFERENCES

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*.

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. *Information Systems Frontiers*, 23(2), 361–373. https://doi.org/10.1007/s10796-019-09977-z

Meadows, J. J., & Sambasivam, S. (2023). Mandatory Gamified Security Awareness Training Impacts on Texas Public Middle School Students: A Qualitative Study. *Issues in Informing Science & Information Technology*, *20*, 67–94. https://doi.org/10.28945/5129

United States Senate Committee on Commerce, Science, and Transportation. (2014). *A "Kill Chain" Analysis of the 2013 Target Data Breach.* https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883