Issues in Information Systems
Volume 23, Issue 2, pp. 119-131, 2022

DOI: https://doi.org/10.48009/2_iis_2022_110

Increasing cybersecurity interest and self-efficacy through experiential labs

Gelareh Towhidi, *University of West Georgia, gtowhidi@westga.edu*
Jeannie Pridmore, *University of West Georgia, jpridmor@westga.edu*

Abstract

Despite the high demand for cybersecurity professionals, there is a lack of student interest in pursuing a career in cybersecurity. It is vital to increase awareness and interest in cybersecurity among students to meet industry needs. Students need to have knowledge in the field of cybersecurity and confidence in their abilities to pursue a career in cybersecurity. This lack of awareness in cybersecurity occurs when students are unaware of their abilities, interests or how they relate to cybersecurity job opportunities. This paper presents an experiential lab designed to increase awareness and interest in the cybersecurity field. The developed experiential lab was well received by the students. After the lab, students expressed excitement and interest in future labs.

Keywords: cybersecurity, experiential learning, self-efficacy, lab

Introduction

The shortage of cybersecurity professionals is currently estimated at 465,000 in the United States and 956,000 worldwide (CyberSeek, 2021). Despite the high demand for cybersecurity professionals, there is a lack of awareness of cybersecurity as a career among students choosing majors and careers (Giboney et al., 2021). It is vital to increase awareness and interest in cybersecurity among students to meet industry demands.

According to Holland's (1997) theory of vocational choice, an individual needs to have knowledge in three crucial areas to correctly choose a career: accurate occupational knowledge, accurate self-knowledge, and accurate self-evaluation. Accurate knowledge of occupation or occupation awareness plays a critical role in students choosing a particular occupation (Crandall et al., 2019; Theresa, 2015). This lack of awareness in cybersecurity occurs when students are unaware of their abilities, interests or how they relate to cybersecurity job opportunities. Perceived self-efficacy also plays a critical role in career choice. Perceived self-efficacy refers to an individual's beliefs about their capabilities to accomplish a set of tasks (Bandura, 1997). If students believe they have the capabilities and skills for the field, they will consider it as a career. Otherwise, they will simply disregard that career path.

To increase cybersecurity awareness among students, it is critical to consider the following: students need to become aware of cybersecurity career needs and become aware of their abilities, i.e. cybersecurity self-efficacy (Crandall et al., 2019). Different initiatives have been offered and used to encourage students to pursue cybersecurity as a career, including instructional techniques such as competitions and camps

(Cheung et al., 2012; Katsantonis et al., 2017) and hands-on experiential learning (Hill et al., 2001; Straub, 2019). Recent research argues that while cybersecurity competitions and camps help raise cybersecurity awareness, they have fundamental problems as both recruitment and educational tools (Giboney et al., 2021). Both cybersecurity competitions and camps are most suitable for reinforcing the interest of students who are already interested in the cybersecurity field. They are usually sponsored by the government or industry, require considerable time, funding, and resources to run (Giboney et al., 2021), and are mostly considered extracurricular activities, limiting their potential for education settings (Cheung et al., 2012; Giboney et al., 2021).

How can we increase cybersecurity awareness and promote student capabilities with a broader and more diverse student body? Active learning methods such as experiential learning can effectively increase interest in the cybersecurity field (Giboney et al., 2021). Previous studies found that experiential labs not only equipped students with required hands-on skills but also motivated students to follow that field as a future career path (Abdulwahed & Nagy, 2009). Cybersecurity experiential learning enables students to build cybersecurity self-efficacy by developing technical skills through hands-on experiments and making it more interesting by providing a good learning experience (Konak, 2018). Experiential learning is effective through building confidence (i.e., self-efficacy) in students and encouraging them to pursue cybersecurity as their career. Furthermore, it requires less funding and resources and is more scalable while providing sufficient educational support to reach new potential students (Giboney et al., 2021).

This paper presents a practical way of using experiential learning to reach diverse students and increase student interest and self-efficacy in cybersecurity.

This study provides a better understanding of the following:

- How can we design experiential labs to improve student interest and self-efficacy in cybersecurity?
- How effective can experiential labs be in helping to increase students' interest in cybersecurity as a career path?

To answer these questions, we designed and conducted experiential labs open to all students. The design of the lab was critical. We designed the lab to be non-threatening, meaning that all students would be comfortable attending the lab to promote cybersecurity awareness and build self-confidence in even our youngest students. We designed the experiential labs following Kolb's (1984) experiential learning model principles to ensure we create an effective self-efficacy experience for students. Furthermore, we facilitate and evaluate our experiential labs using one of the highly successful frameworks for workshop and lab events by Brooks-Harris and Stock-Ward (1999).

We argue that experiential labs can be an effective tool to develop cybersecurity self-efficacy and interest in students. All four critical sources of self-efficacy (Bandura, 1997), including mastery experience, vicarious experience, social persuasion, and physiological state, are achieved by experiential learning, creating motivation and interest in cybersecurity as a career path. Cybersecurity experiential labs help to build students' cybersecurity self-efficacy by creating hands-on cybersecurity skills. In addition, implementing cybersecurity experiential labs are an easy and effective way for higher education to increase the interest in cybersecurity among the general student population. This paper details our lab design and provides students' responses and feedback. The results show that the cybersecurity lab motivated the students and increased their interest in cybersecurity as a future career.

Literature Review

Research in the career decision-making process has examined different factors impacting students' career choices (Spanjaard et al., 2018; Bridgstock, 2009). One of the main areas in this research stream centers on the role of self-efficacy. Self-efficacy refers to an individual's judgment of their ability to accomplish specific tasks needed to achieve particular performance outcomes (Bandura, 1997). Students must first become aware of their interests and abilities related to the work opportunities in a specific field to create interest and motivation for choosing a career (Bandura, 1997). Simply put this means students disregard careers they believe are beyond their capabilities.

Even though efforts have been made to increase awareness among students in cybersecurity, there is a continuous shortage of individuals interested in cybersecurity careers. (Crandall et al., 2019). Building cybersecurity self-efficacy in students has been suggested as an essential factor in encouraging students to pursue a career in cybersecurity (Konak, 2018). A recent study focused on understanding students' perceptions of cybersecurity and the barriers impacting their career choice in cybersecurity (Crandall et al., 2019). The results show that lack of occupational interest, awareness, and aspiration was among the top reasons students did not choose cybersecurity as a career. Students' perception of their abilities regarding cybersecurity careers (i.e. cybersecurity self-efficacy) and their awareness of cybersecurity opportunities are critical in building their interest or aspirations in cybersecurity as a career path.

Experiential Learning and Self-Efficacy

Experiential learning is considered one of the most effective learning tools for career readiness (Kolb & Kolb, 2005; Spanjaard et al., 2018). Experiential learning is defined as a teaching method that enables learners to learn from their own direct, hands-on experiences (Spanjaard et al., 2018; Kolb & Kolb, 2005). Experiential learning allows students to learn core theory and apply those concepts to a situation that replicates a real-world workplace.

Previous research found that experiential learning significantly increases students' self-efficacy (Peechapol et al., 2018). In a systematic review of factors influencing self-efficacy in learners by Peechapol et al. (2018), experiential learning and its hands-on experience were found to have significant direct and indirect effects on self-efficacy. For example, hands-on experience on computers directly affects computer self-efficacy for learners.

Self-efficacy is one of the most studied constructs for understanding academic performance and career decisions (Stewart et al., 2020). Perceived self-efficacy is found to be a strong influential decision-making factor, as it determines which actions the individual will undertake and which they will avoid (Bandura, 1997; Mozahem et al., 2021). Accordingly, perceived self-efficacy is one of the strong factors influencing career choice decision-making, even more, effective than income expectations (Mozahem et al., 2021). Furthermore, experiential learning enables students to build self-efficacy by developing hands-on experiment skills (Konak, 2018).

Based on Bandura's (1997) model of the sources of self-efficacy and the outcomes, perceived self-efficacy develops from information gathered from four sources: mastery experience, vicarious experience, social persuasion, and physiological state (Bandura, 1997).

- Mastery experience refers to individual interpretation of their performance in a specific task based on their previous experience (Bandura, 1997; Mozahem et al., 2021).
- Vicarious experience refers to the social comparison between individual expectations of themselves and others' performance on the same task (Bandura, 1997; Mozahem et al., 2021).

- Social persuasion refers to feedback, support, and encouragement from important others, such as parents, teachers, and friends (Bandura, 1997; Mozahem et al., 2021).
- The physiological state refers to individual emotional arousal associated with the task (Bandura, 1997; Mozahem et al., 2021).

All four critical sources of self-efficacy are significantly impacted by experiential learning (Bandura, 1997; Stewart et al., 2020). Mastery experience happens when a student completes a hands-on task. As students successfully perform the tasks, it directly affects their perceived self-efficacy. Successful task completion increases self-efficacy beliefs. Thus, a successful experience in a cybersecurity experiential lab helps students build confidence in their cybersecurity efficacy. Vicarious experience happens while seeing similar students successfully perform the same task. This enhances the student's confidence in their own abilities in performing that task. Thus, when students see their peers succeed in cybersecurity lab tasks, they believe they can also succeed in cybersecurity tasks. Social persuasion occurs when a student successfully completes the task and is encouraged by the teacher and/or other students. Thus, during the cybersecurity labs, when students are persuaded that they have the capabilities to succeed, they are more confident in their cybersecurity self-efficacy and put more effort into resolving any problems while performing the task. And finally, when a student successfully achieves the task, their positive psychological arousal is interpreted as self-competence. Thus, students who experience positive feelings while performing cybersecurity experiential labs develop positive feelings about their cybersecurity abilities. The experiential labs must be designed based on solid and validated principles to achieve these self-efficacy outcomes. Kolb's Experiential Learning Model (Kolb, 1984) provides the base for developing successful experiential learning activities.

Kolb (1984) believes that learning is the process of creating knowledge through transformational experiences. Kolb's Experiential Learning Model (Kolb, 1984) consists of a four-stage learning cycle. Effective learning happens when a person progresses through a cycle of four stages: (1) having a concrete experience followed by (2) observation of and reflection on that experience which leads to (3) the formation of abstract concepts (analysis) and generalizations (conclusions) which are then (4) used to test a hypothesis in future situations, resulting in new experiences (Kolb, 1984; McLeod, 2017).

Thus, effective learning is achieved through an experiential learning environment that supports the four stages of learning. The learner must be able to have a concrete experience by involving themselves fully in new experiences, reflecting on and observing their experiences from many perspectives, creating concepts that integrate their observations into logically sound theories (analysis and conclusions), and using these theories to make decisions and solve future problems (Kolb, 1984).

Four stages of Kolb's Experiential Learning Model (Kolb, 1984):

1- Concrete experience: doing or having a new experience.
2- Reflective observation of the New Experience: reviewing or reflecting on the experience.
3- Abstract conceptualization: learning or concluding from the experience and creating new ideas.
4- Active experimentation: trying or applying what has been learned in a new situation.

The Experiential Lab Method

The idea for the lab came from collaborating with an Information Systems Cybersecurity industry advisor. The idea was to create and offer cybersecurity labs that would be open to all students using a Raspberry Pi device and PiHole software. Our goal was to create awareness in the field of cybersecurity and excite the students about the possibility of a career in cybersecurity.

Based upon Kolb's Experiential Learning Model (Kolb, 1984), we develop a hands-on experiential learning lab that supports all four stages of concrete experience, reflective observation, abstract conceptualization, and active experimentation. The designed hands-on activities fully support the four stages, summarized as the following:

- Concrete experience: Each hands-on activity includes step-by-step instructions for the tasks that lead to creating a new experience for the students.
- Reflective observation: At the end of each hands-on activity step, students participate in discussions and questions requiring them to reflect on their hands-on experience.
- Abstract conceptualization: After each section of the hands-on activity, questions are asked about what they performed in the activity that leads to the creation of generalized knowledge. Students connect the hands-on learning experience to their overall theoretical knowledge of cybersecurity.
- Active experimentation: Based on what they performed in the hands-on activity, students try a next-level hands-on experience that applies what they learned from the previous exercise.

The Experiential Labs Process Model

Creating an effective cybersecurity experiential lab is a design problem. The first task is to design and develop the labs. Experiential lab design is an iterative process of defining a goal, testing solutions, evaluating their effectiveness, and improving ideas (Kerzner et al., 2018). To design the experiential lab and ensure its effectiveness, we used the highly regarded framework by Brooks-Harris and Stock-Ward (1999) and Kerzner et al. (2018). The framework is a thinking tool that enables us to navigate the process of planning, running, and analyzing the lab. We used the framework to design and facilitate the labs and apply Kolb's experiential learning principles. We applied the framework during the design process, including before the lab event, during the lab event, and after the lab event.
The process is summarized in the following:

- Before the labs
  Define and design: in this step, we defined the lab exercises, learning goals, methods, and materials and recruited a diverse group of students. The main goal was to provide an enjoyable hands-on cybersecurity experience while maintaining appropriate levels of interest and challenge. After setting the learning goals, we designed evaluation methods to ensure the materials were effective. In this step, we answered the questions such as: How many participants would be in the lab? Who will help to facilitate the lab? How long will the lab be? Where will the lab be run? What are additional lab constraints?
- During the labs
  Execute and adapt: during this step, we guided students through the exercises, limited the distractions, and were flexible and adapted to unforeseen events.
  Opening: we set the lab setup, started the lab and engaged and encouraged students to perform the labs. In the beginning, we communicated the goals and guidelines for participants. We also encouraged open communications among participants to promote interest in cybersecurity and make the lab experience valuable and enjoyable.
  Core: in this step, we performed the experiential labs focused on having active and engaged participation. We thoroughly explain the lab activities in the next section.
  Closing: at the end of the experiential labs, we asked students to analyze the results, encouraging reflection on their experience and promoting continued interest in cybersecurity. The closing provides the opportunity to encourage students to follow their interest in cybersecurity and plays an essential role in creating ongoing interest in cybersecurity.

- After the labs
  Analyze and act: in this step, we analyzed the results with an open mind to reflect on and revise the design of future labs.

The Experiential Labs Structure

To apply Kolb's (1984) experiential learning principles to the labs, Brooks-Harris and Stock-Ward (1999) suggest the following lab structure:

1- Introduction and overview
2- Reflecting on experience
3- Assimilating and conceptualizing
4- Experimenting and practicing
5- Planning for application
6- Conclusion

Learning activities in the labs should be sequenced in a meaningful and memorable way. Kolb's experiential learning model provides a logical approach to sequence the activities because it starts with past experience and ends by looking toward the future. The lab structure is designed in a way to sequence the lab activities according to the same order of Kolb's (1984) stages of experiential learning (concrete experience, reflective observations, abstract conceptualization, and active experimentation). Using this structure, we ensure that the experiential labs move participants through Kolb's experiential learning model. We begin the lab by reflecting on experience to encourage participants to show what they already know about cybersecurity. Based on this foundation, we add conceptualizing activities to introduce new information to their existing knowledge by experiencing it. Then, participants start to experiment and practice the new knowledge or skill in the lab. We then conclude the lab with activities that encourage using the lab experience and skill in participants' personal life or continue the experience by choosing cybersecurity as their future career.

The Cybersecurity Experiential Labs Activity

In this section, we explain the details of the experiential labs using a Raspberry Pi device and PiHole software. A Raspberry Pi is a small computing device that harnesses enough power to solve problems digitally and enable people to express themselves creatively. Students tend to shy away from cybersecurity because they do not think they are technical enough to work in that space. Designing a non-threatening cybersecurity lab using Raspberry Pi devices is an excellent way to increase student awareness, build confidence, and spark an interest in the cybersecurity industry. Thus, by combining a Raspberry Pi with PiHole software, students can create and build domain name servers (DNS) filtering servers in a couple of hours that will block over 100,000 ad-serving domains.

A DNS filtering server improves overall network performance while also securing the network, and using PiHole's statistics web interface allows students to view all of the domains being blocked. The agenda for the lab, the details of the information covered, and a description of the hands-on experience are next.
Lab Agenda

- What is DNS?
- Why filter DNS?
- How does this happen in the Enterprise?
- What is a Raspberry Pi?
- What is PiHole?
- Hands-On Workshop to Create a DNS Filtering Server

We designed the lab not to take any knowledge for granted. Therefore, we began the lab by introducing the students to the comic in Figure 1 created by Randall Munroe. We used the comic drawing to explain IP addressing and how addresses had been sold in blocks to companies and governments.

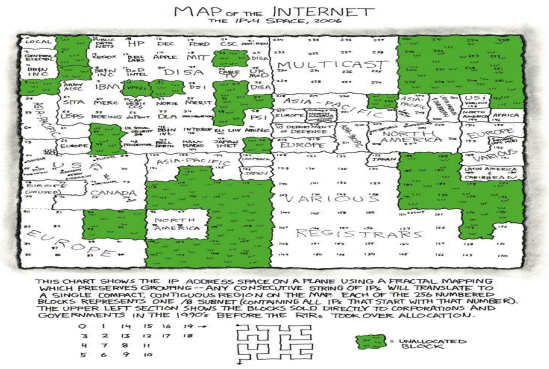

Figure 1: Map of the Internet (https://xkcd.com/195/)

Next, we discussed domain name servers (DNS). DNS is a system in which a domain name is converted to an IP address. We described it as a phonebook for IP addresses. When a user types a domain name into the browser address bar, the browser sends a request to the DNS server to find the correct IP address. For example, a user types in www.google.com. The DNS server finds its IP address of 74.125.68.102 and returns it to the browser. Figure 2 displays an example of a DNS server in action.

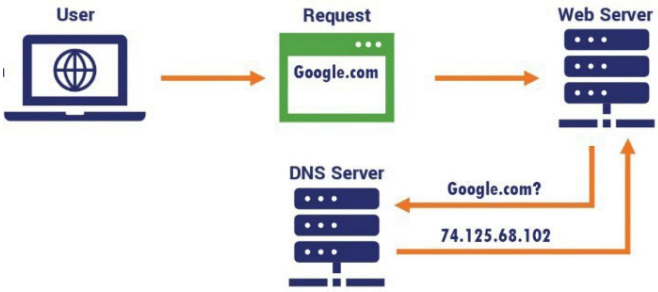

Figure 2: DNS Example
(https://www.itrelease.com/2021/11/what-is-domain-name-server-dns-with-example/)

Then we discussed why someone would want to filter DNS. DNS filtering uses the DNS to block malicious websites and filter out harmful or inappropriate content. Using a DNS filter increases performance, improves security, and helps to block inappropriate content. We discussed this at a personal level and at an enterprise level. Next, we introduced the students to their Raspberry PI devices. Figure 3 is a drawing of a Raspberry Pi.

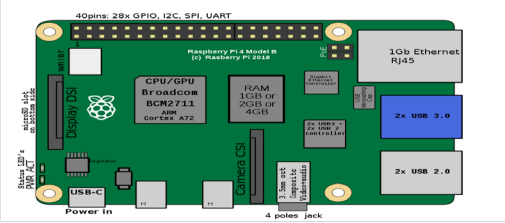

Figure 3: Raspberry PI
(https://commons.wikimedia.org/wiki/File:Drawing_of_Raspberry_Pi_model_B_rev2.svg)

Raspberry Pi devices are small, single-board computers (SBC) created by the Raspberry Pi Foundation. They were first released in February 2012 and generally cost $35 to buy. They were designed to promote computer education in developing countries and have been embraced by the hobbyist communities. They can run on many operating systems, from Windows 10 to Linux.

Then we introduced the students to PiHole. PiHole is a network-level DNS filtering application that is Linux-based. It was released in June 2015 and includes a query list for investigation and troubleshooting. Using PiHole's statistics web interface, the students can view all of the blocked domains. Since Pi-Hole blocks and not just hides these domains, the created DNS filtering server improves overall network performance while also securing the network. Figure 4 shows an example of a PiHole dashboard.

Figure 4: PiHole Dashboard Example from the Lab

After introducing the students to the theory, devices, and software used in the lab, we began the hands-on experience. The instructions for creating the DNS Filtering Server are below.

1) Download Raspberry Pi OS Lite
2) Write it to the SD Card
3) Enable SSH
4) Start-Up the Raspberry Pi
5) Connecting with SSH
6) Install Pi-Hole
7) Setting Up Pi-Hole
8) Configuring your DNS to use Pi-Hole
9) Test Pi-Hole

We walked the students through each of the steps in the lab. At the end of each step in the lab, we intentionally discussed the "why" for each step. Once the lab was complete, we asked the students questions to help them reflect on the process, the purpose, and the technology used. We had two graduate assistants (GA) to help when students encountered issues. The GA's were instrumental in running the lab successfully. The students were engaged and asked many questions. The lab lasted two hours. Figure 5 shows pictures from the first experiential lab held and our GA's.

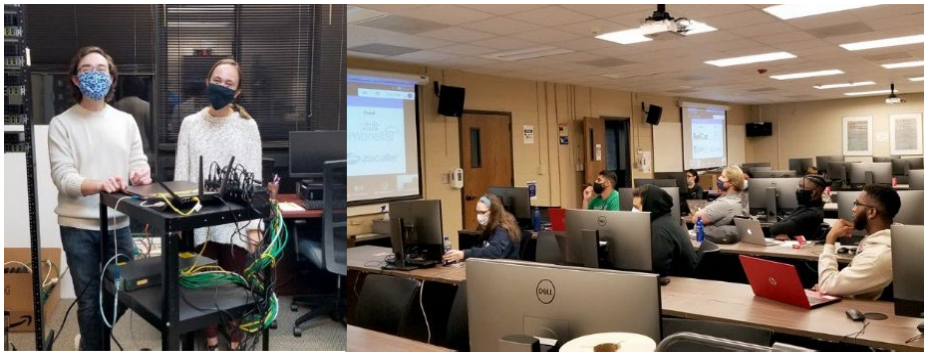

Figure 5: Graduate Assistants and Lab Event

Discussion

There are three primary tasks in the successful development of experiential labs (Brooks-Harris and Stock-Ward, 1999). The first task is to understand the lab participants. The second task is to develop the lab based on the desired goals. Our main goal was to provide an opportunity for students to have an enjoyable hands-on cybersecurity learning experience that promotes their self-efficacy and interest in cybersecurity. The third task is to facilitate the labs. Our key focus was to lead the lab in a way that promotes active learning. To ensure that, we applied Kolb's (1984) experiential learning model to develop our experiential labs. Kolb's experiential learning model provides guidelines for all three tasks (Brooks-Harris and Stock-Ward, 1999). First, by using Kolb's experiential learning principles, we identified our students' learning needs and preferences to achieve the first task. Second, when designing the experiential labs, we used Kolb's four learning processes to identify lab learning activities to promote all four types of learning. Third, we set facilitation skills that correspond to the four types of the learning process.

We designed lab learning activities to enable all four of Kolb's learning processes. Participants were asked to recall their past experiences, which increased their motivation and prepared them for learning by reminding them of what they already knew. Then we led participants to move from reflection and observation to abstract conceptualization by instructing them through the labs' basics and demonstrating the common mistakes. In the third learning process, participants were moved from abstract conceptualization to active experimentation by performing the labs. And fourth, participants were moved from active experiments to concrete experience by encouraging them to apply what they have learned in their personal or professional life.

Experiential Labs Evaluation

We analyzed our lab using the Brooks-Harris and Stock-Ward (1999) evaluation model that is according to the definitional characteristic of Kolb's experiential learning model. The characteristics of a lab that promotes experiential learning are defined as the following:

- Short-term intensive learning
- Small group interaction (interactive learning)
- Active involvement (hands-on practice)
- Development of competence (or self-efficacy)
- Problem-solving, skill-building, increasing knowledge, systemic change, personal awareness/ self-improvement
- Application on new learning

Our experiential labs followed all the characteristics. It was a short-term intensive hands-on learning experience with a small group of students. Our experiential labs provided students with cybersecurity skill-building, cybersecurity problem solving, increasing cybersecurity knowledge, and personal cybersecurity awareness. Our experiential labs equipped students with specific cybersecurity skills through hands-on practices. It allowed students to share the learning experience with one another to find new insights and solutions to the problem. Students had the opportunity to use and apply their new knowledge. Finally, it promoted cybersecurity self-efficacy by applying their new cybersecurity learning.

Students Feedback

We adapted Brooks-Harris and Stock-Ward's (1999) qualitative evaluation questions to analyze the students' feedback.

- What did you like the most about the lab? Why?
- What did you like the least? Why?
- Which lab activity did you find most beneficial? Why?
- Which activity was least helpful? Why?
- What did the facilitator do to increase your ability or motivation to learn?
- What did the facilitator do that may have decreased your ability or motivation to learn?
- How could the lab have been improved to meet your needs better?

The students' response was incredible. We had a set of 10 Raspberry Pi devices and designed the lab for the students to work in pairs with each device. We had 52 students register for the lab and could only include the first 20 who registered. Based on the demand, we ran a second lab session that following Spring semester, and we plan to offer this lab at least once a semester. The students who attended the labs during both sessions were engaged and excited to learn. Even though they needed help along the way, the students were visibly proud of themselves once their DNS filtering server was up and running. Several students reported back that they bought a Raspberry Pi device for further exploration after the lab. A few of the students said they had redone the lab on their own and created a DNS filtering server using their own Raspberry Pi device for their apartments. Furthermore, we evaluated our lab design and lab directing skills.

Evaluating Experiential Labs Design Skills

We evaluated our experiential lab design skills using Brooks-Harris and Stock-Ward's (1999) design skills evaluation criteria, summarized in Table 1.

Table 1: Lab Design Skills

Skill	Rating
Choosing an effective design strategy	A
Collecting helpful information before the lab	A
Setting appropriate goals and objectives	A
Identifying a consistent theme	A
Sequencing activities appropriately	B
Designing activities from all Kolb's learning dimensions	A
Balancing activities according to perceptual styles	C
Balancing activities according to personality types	C
A- strong skill; no improvement needed B- pretty good; could use some refinement C- definitely needs improvements	

Based on the evaluations, we intend to better develop lab activities to balance activities according to students' perceptual styles and personality types and make sure to have steps in place for the more advanced ones in the lab. Some students needed more help than we anticipated. This extra help slowed the lab down. Next time, we will try to predict better what support could be required.

Evaluating Experiential Labs Directing Skills

We evaluated our experiential lab directing skills by Brooks-Harris and Stock-Ward's (1999) set of directing skills evaluation criteria, summarized in Table 2.

Table 2: Lab Directing Skills

Skill Group	Skill	Rating
Creating a positive learning environment	Arranging the physical environment	A
	Creating relationships	B
	Facilitating multidirectional communication	B
	Building trust and acceptance	A
	Providing encouragement	B
Beginning the lab	Introductions and welcome	A
	Overview	A
	Goals and objectives	A
	Setting ground rules	B
	Clarifying assumption	A
	Maintaining a coherent message	A
	Pacing and timing	B
Concluding the lab	Reviewing contents	A
	Planning for the future	B
	Feedback/Evaluations	A
	Follow-up	B
A- strong skill; no improvement needed B- pretty good; could use some refinement C- definitely needs improvements		

Overall, we plan to improve our directing skills by focusing more on our communication skills, providing more encouragement, setting the rules, pacing and timing, and future planning and follow-ups.

Conclusion

By creating this experiential lab based on Kolb's Experiential Learning Model, we developed a hands-on learning experience in cybersecurity. This lab supported the students in gaining concrete experience, reflective observation, abstract conceptualization, and active experimentation. The lab goals were to increase awareness and excitement of cybersecurity as a career and increase student confidence in cybersecurity (i.e., cybersecurity self-efficacy). This lab provided students with hands-on skills and helped build their self-confidence to consider a career in cybersecurity. It supported all four critical sources of self-efficacy, including mastery experience, vicarious experience, social persuasion, and physiological state. Students gained mastery experience through completing the hands-on labs, vicarious experience through seeing their peers successfully completing the same labs, and social persuasion while successfully completing one task and moving to the next task. Finally, they all showed their positive psychological state as more self-confidence in cybersecurity. We were enthused by the students' responses to the lab. In the future, we will continue to offer this lab and other potentially usual labs, such as an introduction to python lab using the Raspberry Pi devices. Factors that may also play important roles in students' interest in cybersecurity need to be examined in future research, such as age, gender, and culture.

References

Abdulwahed, M., & Nagy, Z. K. (2009). Applying Kolb's experiential learning cycle for laboratory education. *Journal of Engineering Education*, 98(3), 283-294.

Bandura, A. (1997). *Self-efficacy: the exercise of control*. New York: Freeman.

Bridgstock, R. (2009). The graduate attributes we've overlooked: enhancing graduate employability through career management skills. *Higher Education Research & Development*, 28(1), 31-44.

Brooks-Harris, J. E., & Stock-Ward, S. R. (1999). *Workshops: Designing and facilitating experiential learning*. Sage Publications.

Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., & Carrillo-Marquez, V. (2012). Effectiveness of cybersecurity competitions. *In Proceedings of the International Conference on Security and Management (SAM)*, (p.1).

Crandall, K. S., Noteboom, C., El-Gayar, O. F., & Crandall, K. (2019). High school students' perceptions of cybersecurity: an explanatory case study. *Issues in Information Systems*, 20(3), 74-82.

CyberSeek (2021, September), Cybersecurity supply/demand heat map. https://www.cyberseek.org/heatmap.html.

Giboney, J. S., McDonald, J. K., Balzotti, J., Hansen, D. L., Winters, D. M., & Bonsignore, E. (2021). Increasing cybersecurity career interest through playable case studies. *TechTrends*, 65(4), 496-510.

Hill, J. M., Carver Jr, C. A., Humphries, J. W., & Pooch, U. W. (2001). Using an isolated network laboratory to teach advanced networks and security. *ACM SIGcSe Bulletin*, 33(1), 36-40.

Holland, J. L. (1997). *Making vocational choices: A theory of vocational personalities and work environments*. Psychological Assessment Resources.

Katsantonis, M., Fouliras, P., & Mavridis, I. (2017). Conceptual analysis of cyber security education based on live competitions. *In 2017 IEEE Global Engineering Education Conference (EDUCON)* (pp. 771-779).

Kerzner, E., Goodwin, S., Dykes, J., Jones, S., & Meyer, M. (2018). A framework for creative visualization-opportunities workshops. *IEEE transactions on visualization and computer graphics*, 25(1), 748-758.

Kolb, D.A. (1984). *Experiential learning: experience as the source of learning and development*. Prentice-Hall, Inc. Englewood Cliffs, NJ.

Kolb, A. Y., & Kolb, D. A. (2005). Learning styles and learning spaces: enhancing experiential learning in higher education. *Academy of Management Learning & Education*, 4(2), 193-212.

Konak, A. (2018). Experiential learning builds cybersecurity self-efficacy in K-12 students. Journal of Cybersecurity Education, *Research and Practice*, 2018(1), 6.

McLeod, S. (2017). Kolb's learning styles and experiential learning cycle. *Simply psychology*, 5.

Mozahem, N. A., Boulad, F. M., & Ghanem, C. M. (2021). Secondary school students and self-efficacy in mathematics: Gender and age differences. *International Journal of School & Educational Psychology*, 9(1), S142-S152.

Peechapol, C., Na-Songkhla, J., Sujiva, S., & Luangsodsai, A. (2018). An exploration of factors influencing self-efficacy in online learning: a systematic review. *International Journal of Emerging Technologies in Learning*, 13(9).

Spanjaard, D., Hall, T., & Stegemann, N. (2018). Experiential learning: helping students to become 'career-ready'. *Australasian Marketing Journal (AMJ),* 26(2), 163-171.

Stewart, J., Henderson, R., Michaluk, L., Deshler, J., Fuller, E., & Rambo-Hernandez, K. (2020). Using the social cognitive theory framework to chart gender differences in the developmental trajectory of STEM self-efficacy in science and engineering students. *Journal of Science Education and Technology*, 29(6), 758-773.

Straub, J. (2019). Experiential research education: a report on the first year of a NSF-sponsored cyber-physical system cybersecurity research experience for undergraduates program. *In ASEE Annual Conference Proceedings.*

Theresa, L. D. (2015). Factors that inform students' choice of study and career. *Journal of Education and Practice*, 6(27), 43-49.