Journal of Cybersecurity Education, Research and Practice

Volume 2018 | Number 1 Article 3

July 2018

"Think Before You Click. Post. Type." Lessons learned from our University Cyber Security Awareness Campaign

Rachael L. Innocenzi
Eastern Michigan University, rinnocen@emich.edu

Kaylee Brown
Eastern Michigan University, browndk@umich.edu

Peggy Liggit
Eastern Michgian University, pliggit@emich.edu

Samir Tout
Eastern Michigan University, stout@emich.edu

Andrea Tanner
Eastern Michigan University, atanner1@emich.edu

See next page for additional authors

"Think Before You Click. Post. Type." Lessons learned from our University Cyber Security Awareness Campaign

Abstract
This article discusses the lessons learned after implementing a successful university-wide cyber security campaign. The Cyber Security Awareness Committee (CyberSAC), a group comprised of diverse units across campus, collaborated together on resources, talent, people, equipment, technology, and assessment practices to meet strategic goals for cyber safety and education. The project involves assessing student learning and behavior changes after participating in a Cyber Security Password Awareness event that was run as a year-long campaign targeting undergraduate students. The results have implications for planning and implementing university-wide initiatives in the field of cyber security, and more broadly, higher education at large.

Keywords
Cyber Security, Higher Education, Password, Learning Beyond the Classroom, Undergraduate Students, Interdisciplinary, Collaboration, Incentives

Authors
Rachael L. Innocenzi, Kaylee Brown, Peggy Liggit, Samir Tout, Andrea Tanner, Theodore Coutilish, and Rocky J. Jenkins

INTRODUCTION

"A password is the only thing that stands between a hacker and all of your personal information." "What action would you take if you found out your password could be hacked in a matter of hours, minutes or even milliseconds?" We made statements and asked questions like these as part of the Cyber Security Password Awareness event that was launched during the 2015-16 academic year targeting undergraduate students as part of a larger three-year, university-wide cyber security campaign. Cyber security is an important issue in today's computer-based society, yet there are relatively few studies that focus on cyber security and student behaviors and perceptions in higher education. This paper examines the effectiveness of the campaign, highlights the lessons learned, and offers recommendations for others who are interested in implementing university-wide initiatives.

The Cyber Security Password Awareness event was part of a larger collaborative initiative created by the Cyber Security Awareness Committee (CyberSAC). Founded in 2013, CyberSAC is an interdisciplinary committee with representatives from diverse units across campus consisting of the Director of the Faculty Development Center (FDC), a professor from the Information Assurance program, an administrator from the Division of Communications, and two administrators from the Division of Information Technology (DoIT). The goal of this committee is to "increase the awareness of cyber security at Eastern Michigan University and integrate security best practices into the culture of the institution" (Eastern Michigan University, 2013a). In October 2013, CyberSAC created a multi-year campaign called "E-Safe" and launched it during the National Cyber Security Awareness Month. The campaign promoted the following message: *Think before you click*, *Think before you post*, *Think before you type*, (http://www.emich.edu/it/security/initiatives/cybersac/cybersac.php).

Cyber Security in Higher Education

According to EDUCAUSE (2017), a non-profit association for Information Technology (IT) leaders in higher education, information security is the number one issue for information technology with regard to student success. The United States Department of Homeland Security reported that in 2010 "24% of all identity theft complaints made to the Federal Trade Commission [were] made by college students" (United States Department of Homeland Security [U.S. DHS], 2010), and in 2012, 31% of the complaints were filed by young adults (U.S. DHS, 2013). Although there have been many improvements in the cyber security world, information security seems to stay at the top of the higher education IT issues, and it continues to be a concern.

Figure 1: Think Before you Click. Post. Type. educational poster created by CyberSAC (Coverly, 2013).

Studies have found that new knowledge can greatly affect a user's behavior and actions. Huang, et.al. (2011) studied the information security knowledge of college students and found that the "lack of knowledge about the threats to information security is usually the main reason of underestimating or overestimating the security level of an information system" (p. 881). Students who are more aware of the advantages of using strong passwords are more likely to change their behavior

in order to increase the security of their passwords (Zhang & McDowell, 2009). We need to educate the students in order to improve the information security of the entire institution.

Password Strength

Passwords are a great way to measure users' perceptions and behaviors with respect to cyber security because passwords are widely used and easily assessed for viability. Hackers have used password cracking and guessing techniques for decades, yet many users report they do not utilize strong password practices to increase their security (McCrohan, Engel, & Harvey, 2010). This may be due to a lack of knowledge or apathy about the risks that a weak password could have to their overall cyber security.

The United States Computer Emergency Readiness Team (US-CERT, 2009) offers techniques that help to develop strong passwords. These tips include:

1. Use different passwords for each of the person's accounts
2. Use mnemonics or passphrases
3. Avoid words that can be found in a dictionary
4. Use uppercase letters, lowercase letters, numbers, and special characters
5. Avoid using personal information to create a password

Other best practices with password safety include avoiding writing down passwords, not keeping an electronic password file that is unprotected, and refusing to share passwords with others (Hoonakker, Bornoe, & Carayon, 2009). DoIT at Eastern Michigan University (2013b) also suggests following all of the aforementioned techniques for strong passwords, along with using a 12, or greater number, character passphrase and intentionally using characters to create misspelled words.

Implementing Campus-Wide Campaigns

The purpose of this article is to share three global lessons learned about implementing a campus-wide campaign promoting cyber security: 1) Lesson 1 – highly valued incentives increase student participation and assessment response rates, 2) Lesson 2 – including students enrolled in information assurance related majors can help facilitate activities and provide valuable insights to the effectiveness of the event, 3) Lesson 3 – collaborating with diverse units across the university helps meet university strategic needs, is cost effective, is manageable, and is gratifying work. While this study focused on assessing undergraduate student knowledge and good practices for creating and sharing passwords, the lessons we learned by implementing this campus-wide campaign will be used for our next cyber security initiatives.

METHOD

Design

The Cyber Security Password Awareness event was held during the 2015-2016 academic year. For the event activity, a table display was set up in a high student traffic area around campus, such as the library, the student union, or large buildings with classrooms and residence halls. The event activity was repeated twenty-four times throughout the year.

The table set up for the activity included a laptop with password testing software and "E-Safe" swag, such as t-shirts, Frisbees, and water bottles. Student-participants who approached the tables could test their password strength using a program called "How Secure is my Password" (*http://hsimp.ihopeit.works/*) on secure laptops provided by DoIT. A DoIT security team tested the legitimacy and safety of this password testing website prior to the event. The "How Secure is my Password?" program produced an estimated time that it would take "to hack" the participant's current password, which could range from milliseconds to trillions of years. Participants were given handouts and flyers with tips about creating strong passwords/passphrases and tips about Cyber Security. To incentivize participation, CyberSAC offered students the opportunity to earn one credit of Learning Beyond the Classroom (LBC) https://www.emich.edu/gened/lbc/. Undergraduate students are required to attend eight cultural or academic LBC-approved events as partial fulfillment of their General Education program. The students who wanted to receive Learning Beyond the Classroom (LBC) Credit were asked to supply their contact information on a sign-in sheet. To receive the LBC credit, students were sent an electronic questionnaire asking about what they learned from participating in the event (see Appendix A for the electronic questionnaire).

During the Fall 2015 semester, the table activities were facilitated by DoIT staff, and in the Winter 2016 semester, the sessions were conducted by DoIT staff accompanied by student-facilitators. These student-facilitators were enrolled in a fully-online, 100-level Information Assurance (IA103) course. This course included an Academic Service-Learning (AS-L) component which is meant to engage students in community service activities while enhancing their academic understanding of course content. The AS-L assignment was worth 15% of the total course grade and it gave student-facilitators an opportunity to practice what they were learning in the course while engaging in a service activity to support the greater good of the campus student body. The assignment activities included the following:

A) *Training* (2 points). This was a mandatory activity whereby IA students had to undergo brief training, provided by DoIT personnel, on certain awareness activities that CyberSAC planned for that year. They also learned best cyber security practices, strategies for creating secure passwords, and how to facilitate the Password Awareness event sessions.

B) *Service Delivery* (4 points). After IA students were trained on the Cyber SAC awareness activities, they were placed in groups of two or three to actually implement what they had learned during that training. The service delivery was done in the form of facilitating an event and helping educate other students.

C) *Post-Delivery.* Journal and Reflection Paper:

   1) *Journal* (4 points): After IA students finished their service delivery in (B), they were asked to submit a journal that included the list of activities they performed throughout the AS-L activity. This included the date/time and details of their training and service delivery.

   2) *Reflection Paper* (5 points): IA student groups reflected on their AS-L experience. The reflection process gave students a chance to write about what they learned, how they have benefited, and how they think they have provided value to others about security awareness. See Appendix B for Reflection Assignment Directions.

Participants

Assessment data from two populations of students were analyzed during the Cyber Security Password Awareness event: the *student-participants* and the *student-facilitators*.

The student-participants were 705 undergraduate students who attended one of the sessions for the event and filled out the sign-in sheet for LBC credit.

The student-facilitators consisted of 30 undergraduate students enrolled in the IA103 course designated with the AS-L component during the Winter 2016 semester.

Measures

Data about the student-participants were collected only for those who signed-up for LBC credit by providing their student ID number, last name and University email address. After each Cyber Security Password Awareness event, the Faculty Development Center emailed student-participants with the learning questionnaire and directions on how to receive LBC credit. Final reminders to complete the questionnaire were sent out before the end of the semester. See Appendix A for a

copy of the questionnaire. Consent agreements were collected from student-participants for permission to use quotes from their responses in the questionnaire.

Data about student-facilitators included a thematic analysis of journal entries and reflection papers describing observations and experiences during the training and facilitation of the service activity for the Password Awareness event.

Limitations

Several limitations of this study are summarized. The data collected did not include demographic information about the students. Future studies would benefit from gathering information about the students' backgrounds to see if there is a difference between the cyber security awareness of various age groups, genders, cultures, or intended majors. This study was only conducted over the period of two semesters, only providing a snapshot in time where a longitudinal study would monitor changes in learning and behavior over a period of several years.

Delivery of the event was inconsistent depending on the facilitation team. Although all facilitators were trained, the DoIT facilitators who manned the table exclusively in during the fall 2015 semester were employees of the IT Help Desk and they had multiple chances to refine their presentations. Each of the student-facilitators from the IA major only facilitated the event once.

From the student-facilitators' reflections, it was discovered that many student-participants were hesitant to type their password into the password checker website. Although this may be a positive sign that these students have high cyber security awareness (i.e. not giving another person one's password), it may have had an impact on the number of students who attended the event. We recommend in the future to have facilitators suggest that participants input a fake password that follows the same general structure as their real password. For example, instead of entering the password *Jd0g1*, have the student enter the password *Td0g2*. Cyber Security Awareness initiatives are only as effective as the number or people that they can reach and educate.

The password checker website that we used during the study is no longer available. We had the University DoIT security team verify the website checker for authenticity and safety to ensure it was not a phishing website. Although this specific website is no longer active, there are other similar sites on the Internet that check password strength, such as http://lastpass.com/howsecure.php.

RESULTS

Student-Participant Questionnaire Results

In this study, a total of 705 student-participants who attended the Password Awareness event also signed up for LBC credit. Each participant was emailed an online assessment questionnaire to complete and return in order to fulfill the requirements for LBC credit; 455 student-participants out of the original 705 completed the assessment, generating a response rate of 64.5%.

The student-participants' open-ended responses to the questionnaire were analyzed for statements claiming: 1) they had either a strong or weak password when they tested the strength of their password during the event, and 2) whether they changed their password, or not, if it was determined they initially had a weak password. Seventy-five percent (n=342) of the student-participants reported they already had a strong password, and of the twenty-five percent (n=113) who reported having a weak password, seventy-five percent of those students (n=85) changed their password after attending the event. (See Figure 2).

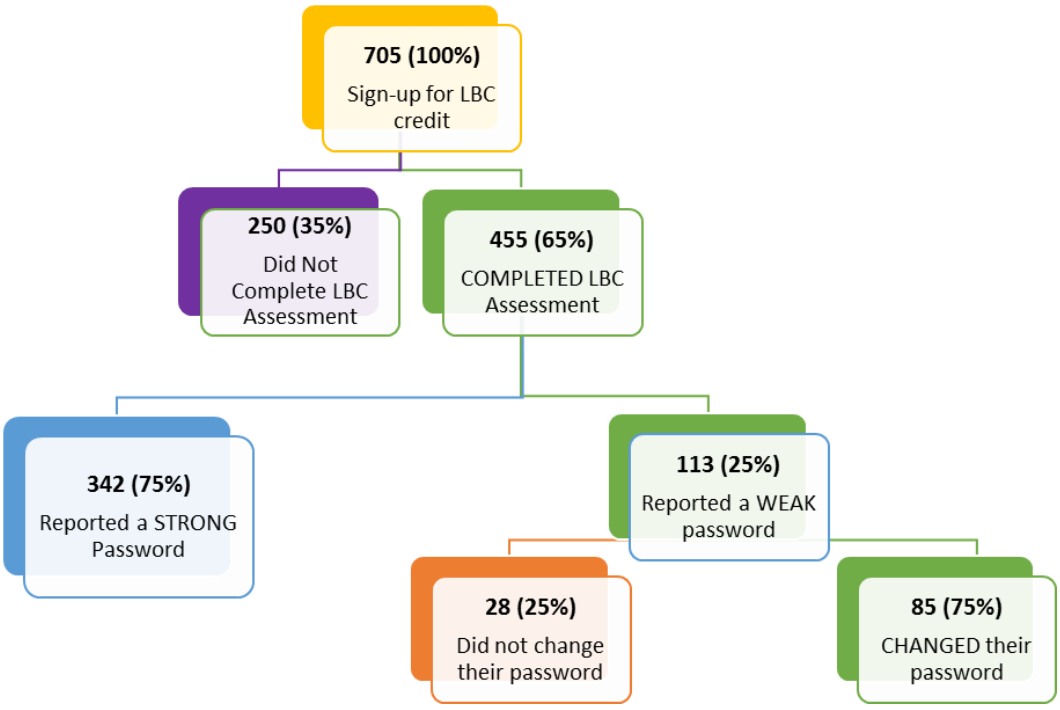


Figure 2: Number and percentage of students who changed their password behavior as a result of determining they had a weak password while attending the Cyber Security Password Awareness Event.

In the LBC assessment questionnaire, we also asked student-participants, "How has your understanding of password strength changed since this event?" The responses were analyzed from the 455 students who completed the questionnaire, and their statements could be categorized into three common themes: *No Change*, *Increase in Awareness*, and *Learned New Strategies* (see Table 1).

Response Themes (n=455)	**Percentage of Students' Responses in Each Category**
Increase in Awareness	44.6%
Learned New Strategies	27.0%
No Change	28.4%

Table 1: Response themes to the question, "How has your understanding of password strength changed since this event?" and percentage of students who stated no change in understanding, learned new strategies, and the event increased my awareness with regard understanding password strength.

Some examples of student responses that fell into the "Increase in Awareness" theme include:

> *"It was a wake-up call because my other passwords could be cracked in 3 hours. It persuaded me to change my other passwords."*
>
> *"Knowing the period would take my password to get hacked gave a stronger idea regarding the importance of having a stronger password. Seeing the period helped in feeling the importance of password and cyber security."*
>
> *"My understanding of password strength has changed because I used to pick easy password just because I was too lazy to pick difficult ones, but what I didn't think about were the consequences that can occur when picking easy ones. I even have a lot of passwords that are the same, which would give a hacker a lot of open opportunities to go through my things. So it is important to pick passwords that is difficult to guess."*
>
> *"It made me realize that my other passwords probably aren't sufficient enough, but that I have the potential to make strong passwords."*
>
> *"I understand that it is a major problem since this event rose awareness. I never had a problem with cyber security so I never thought too much about the consequences."*

Some examples of student responses that were categorized as "Learned New Strategies" include:

> *"I've learned that it doesn't matter if the password isn't significant to you in any way, the hacker/hackers can still find out your password easily. I learned that it's best to have many letters and numbers in your password, and not obvious number sequences like 1, 2, 3, 4."*
>
> *"I learned that it takes a lot of variety and unpredictability to make a password a good one (i.e. uppercase, lowercase, characters, numbers)."*
>
> *"Now I make sure that my password is very long with a mixture of numbers, capital letter, and spaces."*
>
> *"From this event, my understanding of password strength changed by making sure I use really specific passwords that may include two words with a number and/or symbol. For example, EastMichU2$."*
>
> *"I learned that having numbers and also a password varying in capital and lowercase letters an make a big difference in the strength of a password."*
>
> *"I thought I had a very strongly password, but I quickly learned otherwise. I learned that a smart way to do passwords is to choose a sentence and use the first letter of every word as a password."*
>
> *"My understanding of password strength has improved. I know now how important it is to have a very strong password that includes uppercase, lowercase letters, and includes numbers too."*

The most common reason that students did not experience a change in their understanding of password strength was due to the claim that they had previous knowledge of the importance, so the information was not new. Most of these student-participants already had strong passwords before coming to this event. Some examples of their comments include:

> *"My understanding of password strength hasn't really changed that much only because I was already taught the importance of ensuring your privacy and security online."*
>
> *"My understanding of password strength didn't change much since I already knew how to make a strong password."*
>
> *"No, not really, as an IA major I already am aware of the necessity for a strong Password"*

"Not really, before college I went to a cyber security lecture, but it was a good reminder to make your passwords difficult for others to access."

"My understanding of password strength has not changed much since the event since my passwords were strong."

"In all honesty, it hasn't. But I was also pretty well informed about the importance of password strength."

Course Assignment Results

Thirty students enrolled in the IA103 course participated as student-facilitators in the Cyber Security Password Awareness event. Participation in the event was designed as an AS-L project and worth 15% of the final course grade. At the conclusion of the AS-L project, IA student-facilitators were required to write a reflection paper (see Appendix B for the assignment details).

These papers provided valuable insights to new learning and thinking that IA students gained from facilitating the sessions for the Cyber Security Awareness event. The reflection assignment directed students to summarize what they hoped to gain from the experience and how they planned on accomplishing that; describe skills that were enhanced as a result of the experience, such as: communication, critical thinking, social responsibility, or personal responsibility; discuss insights, feelings, change in perceptions and key observations; and explain how the service-learning experience connects to the current course and/or the IA major. Fifteen group reflection papers were submitted representing the thirty students enrolled in the class. We analyzed the papers for common themes and listed the findings in Table 2, which can be found on the next two pages.

Theme 1: Preparation for the event:

- Some groups made informational posters, such as: a graph showing the analysis of password length vs. time (the longer and more complicated the password the greater and exponentially longer it takes to hack), or showing examples of worse possible choices vs better password strategies.
- Some groups wrote out possible scripts explaining cyber security issues and how to address them.

Theme 2: Observations and change in perceptions after the event:

- All groups commented that they observed student-participants with password strengths that showed a huge range from "1 milliseconds," minutes, or days to trillions or "13 sextillion" years before they could be hacked.
- Almost every reflection paper commented that they expected (perceived) student-participants to have weak passwords and were "shocked" or "surprised" when they observed there were more students with stronger passwords than weaker ones.
- Many groups commented that going into the event they thought student-participants would be interested in the activity and willing to test their passwords. They observed that at the beginning of the event many students just walked by the table. The student-facilitators had to be more engaging, change their strategy, level of enthusiasm, and messaging to get people to participate. Facilitators were also "stunned" by the number of participants who were skeptical to type their password into the software program to test the password strength – wondering if this was a "gimmick" to steal their password.
- Most groups discussed the importance of having incentives to get people to participate, such as: the LBC credit and cyber security swag – e.g. E-Safe t-shirts, USB chargers, and water bottles.

Table 2: Common themes from the comments IA student groups made in their reflection papers.

Theme 3: Skills developed through the Academic Service-Learning experience:

- The majority of papers indicated that the skill developed most was improvement in communication, primarily in how to talk to a general audience about technical information. Some facilitators identified themselves as "introverts" and this experience helped build their confidence in speaking with strangers. Others commented on how important it was to be "sensitive" to the audience and gauge their "technological aptitude" before discussing the idiosyncrasies of cyber security issues.
- Some papers focused on critical thinking skills stating that as facilitators they had to figure out clever ways to entice the audience to come to their table. For example, one group mentioned walking over to students manning a table for a different service project and convincing them to direct students who visited their table to go to the cyber security table next.

Theme 4: How the service-learning activity relates to the course and IA major:

- Many papers discussed the idea that "people are the weakest link" when it comes to security. This experience provided a "real world experience" for IA student-facilitators to see how that played out in the general public.
- Several groups commented that this experience helped solidify their passion for information assurance and supported why they selected this as a major and future career.
- Other groups commented that they were pleased to see the Cyber Security initiative as evidence that the University cares about safety and security of the students, faculty, and staff.
- Many groups mentioned that they enjoyed working with a diverse group of people across campus with different backgrounds and perceptions about cyber security. In general, the class felt good about participating in a service activity and having a positive impact on others.

Table 2: Continued from previous page.

DISCUSSION

The Cyber Security Password Awareness event, created by CyberSAC, was aimed at increasing awareness about security breaches involving weak passwords and promoting positive change in student behavior by encouraging students to change weak passwords to stronger ones. Through the assessment of the event, we gathered information about the students' cyber security perceptions and their thoughts and behaviors towards password safety and strength. For example, many participants expressed surprise when they realized how weak or strong their password was in accordance with the "How Secure is my Password" program. From the LBC assessment questionnaire, if respondents testing their password were informed that it was weak, then the majority of those students (75%) changed their password using the suggested tips to increase its strength. We were pleasantly surprised to find that the majority of students who attended the event already had strong passwords (Figure 2). IA-103 student-facilitators confirmed these results when we analyzed their journals and reflection papers.

CyberSAC also analyzed the password change frequency after each event to see if there were spikes in the number of password changes to the University's email system around the day and times the events were scheduled. No correlation could be made between upticks in password changes happening during or after the Password Awareness events, however we did learn that most people change their passwords on Mondays, Tuesdays, or Wednesdays. Examples of these data are found in Appendix C. The columns range from the least number of password changes (red) to the most number of password changes (green). We do not have any hard evidence for the reason why students are more likely to change their password Monday through Wednesday. After conducting informal interviews with students, we learned that these students access their accounts more frequently during the beginning of the week. According to these students, they are working over the weekend and the phrase "out of sight, out of mind" may be one explanation for why less passwords are changed at the end of the week and during the weekend. We will use this information for scheduling future cyber security awareness initiatives – planning more events around Monday-Wednesday dates and avoiding Thursdays-Sundays.

In addition to our findings about student learning and the ability to influence change in student behavior for creating safe passwords, CyberSAC also gleaned valuable insights about the strategies we used to implement the event over the course of the academic year. We are taking away three major lessons from this experience that will aid in planning future cyber security initiatives.

Lesson 1: Use high-value incentives. By offering LBC credit, we incentivized undergraduate students to participate in the Password Awareness event. To receive

their LBC credit, student-participants had to complete the assessment questionnaire explaining what they learned by attending the event. We are satisfied with the total attendance number of over 700 student-participants with a response rate of 65% for the assessment questionnaire. Embedding the AS-L service project into the IA-103 class and making it worth 15% of the course grade motivated students in a fully online course to engage in a service activity that brought them on campus and involved them in a face-to-face experience.

Lesson 2: Include students enrolled in cyber security-related majors. Including student-facilitators to help implement the event provided the people-power to host more sessions over the academic year (we implemented 24 Password Awareness sessions in one academic year). The reflection papers written by the IA-103 student-facilitators discussed the passion they have for the information assurance discipline and the emerging knowledge they have about cyber security issues. Helping to facilitate the Password Awareness event gave these students valuable experience in developing communication and critical thinking skills as well as reflect on why they chose this major and how they see themselves as emerging professionals in the field of information assurance. Not only was this a great retention exercise for the IA program, having the IA student-facilitators interact with the general student body provided a good opportunity to recruit new students into the program.

Lesson 3: Collaborate with diverse groups across campus. The goal of the project was to support safety and educational awareness for cyber security. This is a strategic initiative for the University. The members of CyberSAC brought unique qualities to the project. The DoIT team provided the technological training, staff-facilitators, and computer hardware and software used for the event sessions. The professor in the IA program provided the student-facilitators and the reflection paper as one of the assessment tools for the event. The Division of Communication provided the professional quality marketing tools, E-Safe swag (T-shirts, water bottles, flyers), and promotional materials for the slogan *Think Before You Click. Post. Type.* The Faculty Development Center set-up the LBC credit approval and the human subject's protocol, created the assessment questionnaire for LBC credit, and analyzed all the data for the event. By working together and sharing resources and talents (with people, equipment, and funds to run the events), the CyberSAC group was able to implement a successful large-scale, campus-wide event while staying within a small budget.

Although our university continues to promote good practices for password safety and strength, we are now promoting using Two Factor Authentication through Duo Security, as well as electronic password vaults that allow you to safely store all of your passwords, such as LastPass. DoIT also utilizes forced password changes once a year to help avoid security breaches on student, faculty, and staff accounts. It is important to recognize that institutions must try to design and build effective

security measures, but as Huang et al. (2011) pointed out, “No matter how well designed, security methods rely on individuals to implement and use them” (p. 882). Cyber security will improve if all users are following safe cyber practices. The next event that CyberSAC implements for cyber security awareness will include the lessons learned from this research project.

REFERENCES

Coverly, D. (2013). *Think before you click, post, type* [cartoon graphic]. Retrieved from http://www.emich.edu/it/security/initiatives/cybersac/type.php

Eastern Michigan University (2013a). About the cyber security awareness committee. *Division of Information Technology*. Retrieved from http://www.emich.edu/it/security/initiatives/cybersac/aboutcybersac.php

Eastern Michigan University (2013b). Think before you type! Protect your passwords. Division of Information Technology. Retrieved from http://www.emich.edu/it/security/initiatives/cybersac/type.php

EDUCAUSE (2017). *Top 10 IT issues, 2017: Foundations for student success*. Retrieved from http://er.educause.edu/articles/2017/1/top-10-it-issues-2017-foundations-for-student-success

Hoonakker, P., Bornoe, N., & Carayon, P. (2009). Password authentication from a human factors perspective: Results of a survey among end-users. Proceedings from the *Human Factors and Ergonomics Society 53rd Annual Meeting*. San Antonio, Texas.

Huang, D., Rau, P. P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, *69*(12), 870-883. https://doi.org/10.1016/j.ijhcs.2011.07.007

McCrohan, K., Engel, K., & Harvey, J. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23-41. https://doi.org/10.1080/15332861.2010.487415

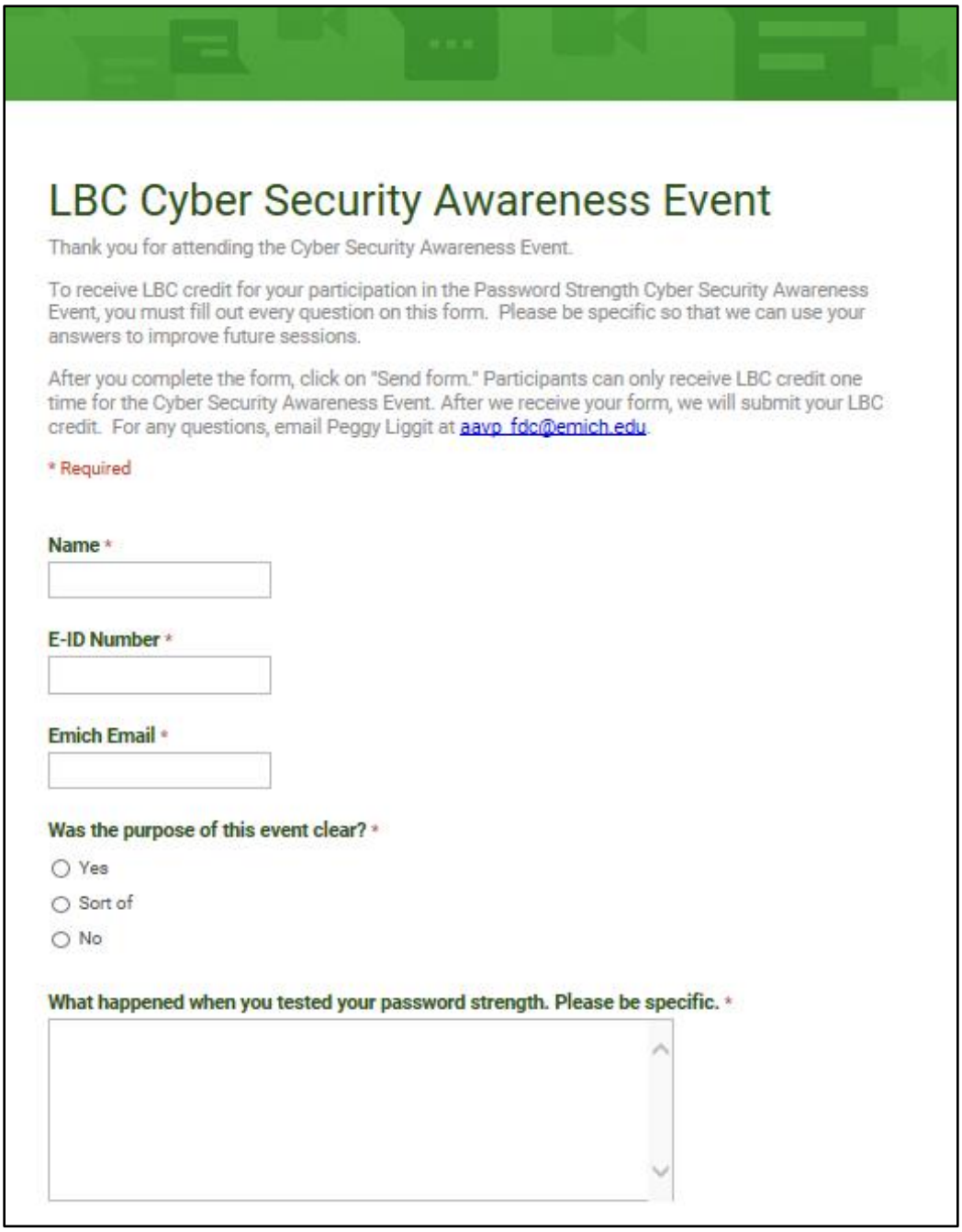
United States Computer Emergency Readiness Team [US-CERT] (2009). Choosing and protecting passwords. *National Cyber Alert System Security Tip ST04-002*. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-002

United States Department of Homeland Security (2010). Undergraduate students tip card. Retrieved from: https://www.dhs.gov/sites/default/files/publications/Undergraduate%20Student%20Tip%20Card_0.pdf

United States Department of Homeland Security (2013). Undergraduate students tip card. Retrieved from: https://www.dhs.gov/sites/default/files/publications/Undergraduate%20Student%20Tip%20Card.pdf

Zhang, L., & McDowell, W. C. (2009) Am I really at risk? Determinants of online users' intentions to use strong passwords, Journal of Internet Commerce, *8*(3-4), 180-197, doi: 10.1080/15332860903467508

Appendix A



LBC Cyber Security Awareness Event

Thank you for attending the Cyber Security Awareness Event.

To receive LBC credit for your participation in the Password Strength Cyber Security Awareness Event, you must fill out every question on this form. Please be specific so that we can use your answers to improve future sessions.

After you complete the form, click on "Send form." Participants can only receive LBC credit one time for the Cyber Security Awareness Event. After we receive your form, we will submit your LBC credit. For any questions, email Peggy Liggit at aavp_fdc@emich.edu.

* Required

Name *

E-ID Number *

Emich Email *

Was the purpose of this event clear? *

- ○ Yes
- ○ Sort of
- ○ No

What happened when you tested your password strength. Please be specific. *

If you learned that your password strength is strong, where do you think you learned to make strong passwords? *

If your password was not strong, just answer N/A

Did this event prompt you to change your my.emich password? *

- ○ Yes
- ○ No

Did this event prompt you to change any other passwords? *

- ○ Yes
- ○ No

What does cyber security mean to you? *

How has your understanding of password strength changed since this event? *

Please be specific.

What suggestions do you have to make Cyber Security Awareness Tables better? *

Appendix B

Academic Service-Learning: Reflection Paper

Instructions:

Please write this paper in essay format. It should be approximately 1-2 pages (single space – 12 point font). Below is a list of key components that you should address in your reflection but please do not respond to each separately, but rather create a coherent summary that is structured around your experience and includes this components. A drop box will be available for this paper on the course shell by the deadline.

Key Reflection Components:

1. List the names of the organizations(s) and their role in the community you served
2. Describe the community need(s) that your service learning experience addressed
3. Describe the "what" and "how" of your experience. In other words, describe what you had hoped to gain from this experience and how you planned on accomplishing it.
4. Describe how this experience enhanced "one" of the following skills:
    a. Communication Skills - This describes the ability to effectively express and exchange ideas through listening, speaking, reading, writing, and other modes of interpersonal expression
    b. Critical Thinking Skills - This describes the ability to gather and synthesize relevant information, evaluate alternatives, and implement creative and effective solutions
    c. Social Responsibility Skills - This is the ability to practice community engagement that addresses social justice, environmental responsibility, personal/national security, cultural diversity, etc.
    d. Personal Responsibility Skills - This is the ability to become an independent learner who understands and expresses the lifelong skills that are necessary for physical, social, economic, mental, and emotional health
5. Describe how your service learning experience may be connected to your current course work and/or major
6. Describe what you learned about yourself and any insights you gained as a results of this service learning experience. In what ways did your perceptions change? Include impressions, feelings, and key observations.

Appendix C

October 2015 Password Changes

Date	Day of the Week	Number of Password Changes
10/1/2015	Thursday	96
10/2/2015	Friday	48
10/3/2015	Saturday	34
10/4/2015	Sunday	29
10/5/2015	Monday	92
10/6/2015	Tuesday	118
10/7/2015	Wednesday	103
10/8/2015	Thursday	93
10/9/2015	Friday	64
10/10/2015	Saturday	36
10/11/2015	Sunday	51
10/12/2015	Monday	98
10/13/2015	Tuesday	106
10/14/2015	Wednesday	97
10/15/2015	Thursday	94
10/16/2015	Friday	82
10/17/2015	Saturday	45
10/18/2015	Sunday	54
10/19/2015	Monday	115
10/20/2015	Tuesday	107
10/21/2015	Wednesday	108
10/22/2015	Thursday	76
10/23/2015	Friday	59
10/24/2015	Saturday	29
10/25/2015	Sunday	36
10/26/2015	Monday	126
10/27/2015	Tuesday	114
10/28/2015	Wednesday	106
10/29/2015	Thursday	93
10/30/2015	Friday	71
10/31/2015	Saturday	41

March 2016 Password Changes

Date	Day of the Week	Number of Password Changes
3/1/2016	Tuesday	338
3/2/2016	Wednesday	260
3/3/2016	Thursday	217
3/4/2016	Friday	136
3/5/2016	Saturday	134
3/6/2016	Sunday	142
3/7/2016	Monday	293
3/8/2016	Tuesday	250
3/9/2016	Wednesday	208
3/10/2016	Thursday	203
3/11/2016	Friday	168
3/12/2016	Saturday	124
3/13/2016	Sunday	148
3/14/2016	Monday	282
3/15/2016	Tuesday	275
3/16/2016	Wednesday	282
3/17/2016	Thursday	225
3/18/2016	Friday	264
3/19/2016	Saturday	146
3/20/2016	Sunday	149
3/21/2016	Monday	286
3/22/2016	Tuesday	254
3/23/2016	Wednesday	203
3/24/2016	Thursday	187
3/25/2016	Friday	109
3/26/2016	Saturday	90
3/27/2016	Sunday	95
3/28/2016	Monday	242
3/29/2016	Tuesday	240
3/30/2016	Wednesday	232
3/31/2016	Thursday	192