Teaching Tip

Let's Get Cracking – Teaching about cyber security and better password management by starting with cracking a safe

Jeff Strain
jeff.strain@byuh.edu
Faculty of Math and Computing
BYU Hawaii
Laie, Hawaii 96762

Abstract

It can be challenging to help learners understand the importance of keeping their cyber information safe with good password management. Cybersecurity concepts are abstract and vague concepts that many learners struggle to understand. This paper introduces an initial step in a scaffolded approach to help learners understand good password management. Introducing the concept of managing sensitive information in a cyber environment through a physical and effective pedagogical exercise. This early step has the learner crack into an older safe by creating a rainbow table with easy-to-obtain information, becoming more aware of the responsibility of managing sensitive information, and maintaining systems. This exercise provides an experiential learning experience that aids the learner on the path to better cyber awareness. Having the same experience in 2022, 2020, and 2019 at a small multi-cultural university, we can assess the perceived longevity of this teaching approach and the impact that it has had on their daily cyber usage.

Keywords: Keywords: Cybersecurity, Authentication, Passwords, Experiential Learning, Ethical Hacking, 2FA, MFA, Pedagogical Learning, Safe Cracking, Password Cracking, Rainbow Tables

1. INTRODUCTION

A safe is a great physical representation of security to a learner. Even when a learner has not used a safe before, everyone knows about them and understands that they are a security measure. Because of this, there is a sense of accomplishment after breaking into a safe. Using a safe in teaching cyber security has many synergistic qualities besides protecting backup tapes, thumb drives, and other vital data. The exercise in this paper is an example of how cracking into a safe is used at a small multi-cultural university to help learners better understand password best practices.

As with many systems, most safes are not well maintained. As time passes, people fail to change the mode of entry even though others may have seen them access it. Keypads used in safes, doors, and many other devices deteriorate, and frequently used inputs can become visible. When no degradation of the button exists, black lights can reveal the oil left by people's fingers.

People commonly use simple authentication methods such as PINs, patterns, combinations, and passwords. All these methods have similar flaws. Learning about those flaws can be used synergistically across most simple authentication methods. The knowledge gained can help one understand mitigation methods that can be applied.

Learners of Information Technology (IT) and related fields need a deeper understanding of cybersecurity and password management. "Two out of three people still reuse passwords across accounts, one in three share codes with others, and nearly 40 percent have been hacked"

ISSN: 2473-4901
v8 n5757

(Security.org Team, 2021). Password management issues continue, with 35% of people never changing passwords unless required (Moscaritolo, 2018). Learners studying IT and other technology fields should have better password management and not fall into these trends.

The safe used in this example is well suited for this exercise—the relative closeness to the classroom and the current condition of the safe. While a safe is one of the better choices, other options might be used for a similar exercise if a safe is unavailable. Additional options may entail an electronic key entry system on a door, garage, or lockbox.

The safe-cracking, with proper permission, is part of an optional cyber security capstone course taken by information technology majors or minors with prerequisites that help prepare learners for the ethical issues faced in the activity during the last year of study as an upper-level course.

1.1 The need to spark more interest in cyber security

Hacking is becoming more of a problem than it has been, skyrocketing in 2020 (Federal Trade Commission, 2022, p. 6) and continues to climb. With increased hacking, the usage of leaked data aids in stealing one's identity. The increased threat of hacking is due to many things, which include:

- Increased spare time
- Increased attack vectors with remote workforces
- Poverty
- Polarized views
- Tension between nation-states
- Commoditization of cybercrime

1.2 Credential management

Many password issues include reusing passwords, never changing passwords, and unintentionally giving the passwords to hackers. Cracking open a safe is a great way to familiarize oneself with many aspects of this issue. Code reuse, never changed, or inadvertently given to others are the main aspects of this exercise. Figure 1 shows the state of the number pad of the safe. One can see that specific numbers are no longer visible while others have not been affected, leading one to assume that the code is never changed. Understanding how to protect the combination to the safe can be applied to passwords.

Figure 1: State of the safe

1.3 Effective Pedagogy

Too often, cybersecurity courses fall into the rut of understanding terms and definitions. The regurgitation of course materials is not equivalent to critical engagement and meaning. Teaching through conversation is a part of the five pedagogy standards. The five standards of effective pedagogy shown in Figure 2 include

1. Joint productive activities
2. Developing language competency
3. Making it meaningful by connecting it to the student's life
4. Teaching complex thinking
5. Engaging through dialogue

(Dalton, 1998, p. 10). Suitable activities relating to something learners already know can spark better conversations and complex thinking.

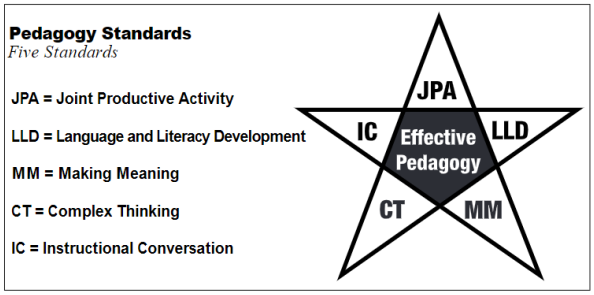

Figure 2: Pedagogy Standards (Dalton, 1998, p. 10)

1.4 Experiential Learning

Experiential learning is about helping learners understand better and retain longer "since they are finding out something that is important and useful for themselves, using their powers of observation and interpersonal skill" (McKeachie & Svincki, 2006, p. 278). By providing an experiential learning example of breaking into a safe, learners can experience the connection between life and learning. Activities with real-life synergies, achieving benefits in and outside the

classroom, should be the goal for any instructor who aims to create motivated learners. "Coursework should include real hands-on application and deep instructor-led group discussions of cyber security methods, techniques, challenges and difficulties." (Erickson & Kim, 2021)

1.5 uCertify Certified Ethical Hacker Online Courseware

In 2022 we adopted an online course from uCertify Certified Ethical Hacker - CEHv10 for the first time. An online course helped with terms, lessons, and virtual labs. Other hands-on labs are kept and help with consistency with changing instruction materials. Some labs are almost identical to in-class engagements. For example, uCertify has password cracking using Linux and Windows. The Linux virtual lab is similar to one of the engagements with "Cracking passwords with John." Students understand some of the minor differences between virtual labs and real-world experiences by cracking passwords in the virtual lab and the classroom.

1.6 Scaffolded approach based on 2022

Scaffolding is the breaking up of learning so that it is smaller and more manageable for learners to build upon what they know. Scaffolding is done with a tool or structure to help incorporate these smaller layers into the learning process (Alber, 2011). A side effect of scaffolding is that one is teaching small portions over a longer time. Teaching small portions over a long time has been shown to enhance long-term knowledge retention (Raman, Mclaughlin, Violato, Rostom, Allard, & Coderre, 2010). Below is a list of the assignments part of the scaffolded process.

1. Course Prerequisites
2. Crack Open a Safe Engagement
3. Social Engineering
4. Gather Passwords
5. Password Cracking
6. Encrypting and Hashing
7. Cracking passwords with John
8. Wi-Fi Cracking

1.6.1 Course prerequisites

An introduction to information security is required, as is computer networking and systems administration—this help to give the foundational knowledge to get started in ethical hacking.

1.6.2 Crack open a safe engagement

Cracking open the safe is an in-class engagement that all learners participate in and is the main topic of this paper. Some foundational information is needed, and hands-on learning and discussion are key. These foundations continue to be reinforced and extended in later lessons.

1.6.3 Social engineering

The core aspects of social engineering that tie back into this scaffolded assignment series include more in-depth on shoulder surfing and phishing and its many similar forms.

1.6.4 Gathering passwords

The many ways one can obtain passwords and password files. The gathering passwords exercise is new to 2022 and are a virtual lab added with the adoption of the uCertify ebook.

1.6.5 Password cracking

How to crack a password in Linux and Windows engagements are new to 2022 and are virtual labs added with the adoption of the uCertify ebook.

1.6.6 Encrypting and hashing

Ways to protect data and make them more secure. What are the issues, and how to make it harder for hackers if they can obtain a password file?

1.6.7 Cracking passwords with John

We start by having students create passwords and try to crack them using a rainbow table password cracker of John the Ripper. We then use business as an example and easy and medium-difficulty passwords for student groups to crack.

1.6.8 Wi-Fi Cracking

We show how to obtain the hashed shared secret of a Wi-Fi connection. Once it has been obtained wirelessly, the cracking can begin. There are varying levels of difficulties in the shared key. In the second part of this exercise, each time has a Wi-Fi access point they set up. Another group captures their connection wirelessly, grabs the password hash, and cracks it. This exercise uses a little of almost everything that came before it and is an excellent capstone to these scaffolded learning assignments.

2. CRACK OPEN A SAFE ENGAGEMENT

The cracking open of a safe engagement occurs in the first week of class and usually on the second day. It was first introduced in 2019 and was by chance. The safe was publicly accessible and in poor condition. The stewards of the safe agreed to the usage of the safe for an ethical hacking exercise. Safe access and usage are acceptable. In 2022 the safe was donated for exclusive use in the class. This exercise helps set expectations for the class and understand what follows.

The safe engagement introduces several essential principles to cybersecurity. Such as avoiding password sharing and reuse. It emphasizes the issues that appear over time without password changes. This engagement also shows how systems age and regularly need maintenance or replacing. When an issue cannot be taken care of immediately, we discuss alternatives that help make something less terrible.

2.1 People are People

The first thing a learner must know is that people are predictable. By looking at pins people use, one can see how predictable they are. Looking at dumps from hackers, we see that over 20% of a 4-digit PIN in China is among ten numbers. (Wang, Gu, Huang, & Wang, 2017). Learners learn to look for dates and patterns. Patterns can start anywhere but usually start and follow how someone would read a page or write a letter The great thing is that when students list the numbers missing from the number pad due to repetitive use, they usually list them in the correct order for safe access. Listing the numbers in the correct order is because people like to do things a certain way. Listing the rubbed-off numbers is the beginning of our rainbow table.

2.2 Do reconnaissance

For the activity, students have limited information and time. In real-life hacking techniques like shoulder surfing. Shoulder surfing is where someone casually watches someone else uses their password or enter a pin to see what the person enters. Shoulder surfing can help by adding additional information that could be useful. In the crack a safe engagement, shoulder surfing helps understand the flow or pattern used. As part of the exercise, to help students benefit from this in their experience but save on time, information such as the safe requires a five-digit code, per the user's manual, and some basic information on the pattern that would be easy to obtain with shoulder surfing is discussed. This discussion is an excellent substitute to speed up the process. With shoulder surfing, one could quickly identify, in general, if the code is likely a pattern or a date.

A multitude of security measures follows a pin that includes a certain number of digits. The same patterns used on a number pad exist on Android. These patterns are easy to observe (Zezschwitz, De Luca, Janssen, & Hußmann. 2015). Shoulder surfing for phone passwords is a standard tool to collect information on users. This common information-gathering technique is not well researched. A study discovered "168 of our 174 participants (97 %), claimed to know of a shoulder-surfing situation in everyday life. Moreover, 21 % of the participants mentioned that shoulder surfing occurs regularly" (Eiband, Khamis, Zezschwitz, Hussmann, & Florian, 2017)

Not only is shoulder surfing an everyday occurrence, but it is also effective. One justification for this in-class discussion that helps speed things along is how easy it is to shoulder surf and get the correct pattern. Cornell University did a study where they asked people to shoulder surf from different angles. They then asked them to open the device as if they were attackers. "64.2% of them were successful after seeing the phone being unlocked with a pattern once. This number went up to 79.9% if the 'attacker' got to see the phone being unlocked multiple times. Successful attacks were much lower when using a PIN. Only 10.6% of attacks were successful after a single observation of a PIN unlock, and that number increased to 26.5% with multiple observations." (Alber, 2011)

The learner can take what they learn from the reconnaissance and apply that to the rainbow table. A hacker may learn about people through public sources or social media to help create a rainbow table. Experienced hackers may have access to prior data breaches that may contain past passwords. The information gained from reconnaissance helps to create a better rainbow table.

2.3 Class discussion

First, discuss the locking device and how specific numbers are not visible. One should provide a hint when discussing a standard PIN versus patterns due to the shoulder surfing expectation. The hint given is that the code is a pattern. The class discusses common patterns they think may be used with the locations rubbed off before giving the next shoulder surfing hint, and by default, most want to start in the top left since that is how they read—informing the learners that the order they provided the missing number is the correct starting position of the numbers in the pattern, helps to reinforce that people tend to do things in a certain way.

The last item in the class discussion is the number of items in the code per safe make and model. As Figure #1 showed, four numbers are missing, leaving one needing to be duplicated or used twice. Discussing how five numbers are needed but only four are missing leads to the possibility that one number is used more than once. The three options the class usually chooses are the first, the last, and the middle. Understanding the middle of a list of four numbers can be difficult

but looking at the locations on the pad is helpful.

Finally, list the three agreed-upon numbers on the board that the class has guessed and mention that the correct number is in their list. With good shoulder surfing, one would likely be able to identify the correct numbers and patterns, but the previous shoulder surfing hints are sufficient.

Due to the age and condition of the safe, some additional instructions, with our specific safe, are required. The beeps for a correct pattern differ from the incorrect one. Opening the safe can be tricky because the internal workings are old. One may need to hold up the handle slightly before opening. There is a taped-over button that should not be used. This button changes the safe from a combo to a key, and the location of the key is unknown.

2.4 Cracking the Safe

While the class works on other engagements, groups of learners will take turns going to the lab where the safe resides. The instructor or a tutor watches the first learner. After that, the last learner to open the safe stays and watches the next learner. The observer leaves when the next learner succeeds, and a new learner comes in to try cracking the safe. There are always two people at the safe at any time. One learner attempts to open the safe at a time while someone who has successfully opened it observes. The observer's purpose is to verify success and help the learner with the safe if there is an issue. All learners should be successful.

Once a group completes the engagement, we show other methods to gain access to the safe, including how to use a pen to unlock the safe. Alternative methods show that other ways of getting into a system exist, and all should be understood and secured.

2.5 Cracking a safe debrief

When possible, the learners drive the debriefing by asking questions and understanding how to make things better. Using comparisons to passwords and how one would do things in the cyber world, the learners can better understand. This "debriefing" scenario would help the learners see the process of making security more secure in real life. Debriefing is to help gain a better understanding of how to solve the issues and deter hackers. "With strong passwords and multifactor authentication, the hackers are deterred from these systems and will move on to more easily attainable targets." (Hemann, 2021)

2.5.1 Limit physical access by moving it behind a locked door

The placement of the safe is not ideal. The safe is currently by an unlocked door in a public space lacking supervision. Some security cameras inside and outside would record nefarious activities, but this would not prevent the crime. Moving the safe behind a locked door is comparable to adding multi-factored authentication. It does not fix the security issues, but it does improve the security of the safe's contents by requiring door access to attempt to use the code. The proposed locked door is also the office space of the lab manager. This office space is a small room. The small private room would prevent most shoulder surfing opportunities as the safe would no longer be in a "public open" space.

2.5.2 Change the code to avoid using all the rubbed-off numbers

If the code were changed, it should use some numbers other than the ones already in use. Changing the code is like requiring a password change and not allowing it to be the same or similar to the prior passwords and password complexity requirements. Changing the code would render the rubbed-off keys less valid. The rubbed-off keys are similar to hackers getting a user's password from prior breaches.

2.5.3 Get a new safe

This safe is old and, in some ways, more of a liability to the enclosed items. If someone pusses the button, items inside would be unreachable, and locksmiths are expensive. At first, the cost of the items in the safe was less than the locksmith to open the safe. Since the calculators were updated, that was no longer the case. Getting a new safe is like updating one's identity management system. Ideally, one would use the features to require a code to be more secure, not reused, and changed regularly.

2.5.4 The code is shared

Due to sharing a single code, the pattern entered is always the same. Code sharing makes it easy to learn the pattern by shoulder surfing. Consider giving everyone a unique code. Sharing a code is similar to sharing accounts and passwords. Many organizations still share specific passwords. Ideally, this should never be the case.

2.5.5 The code is easy

Making the code easy helps to open it and not forget it, but it comes at the expense of how

ISSN: 2473-4901
v8 n5757

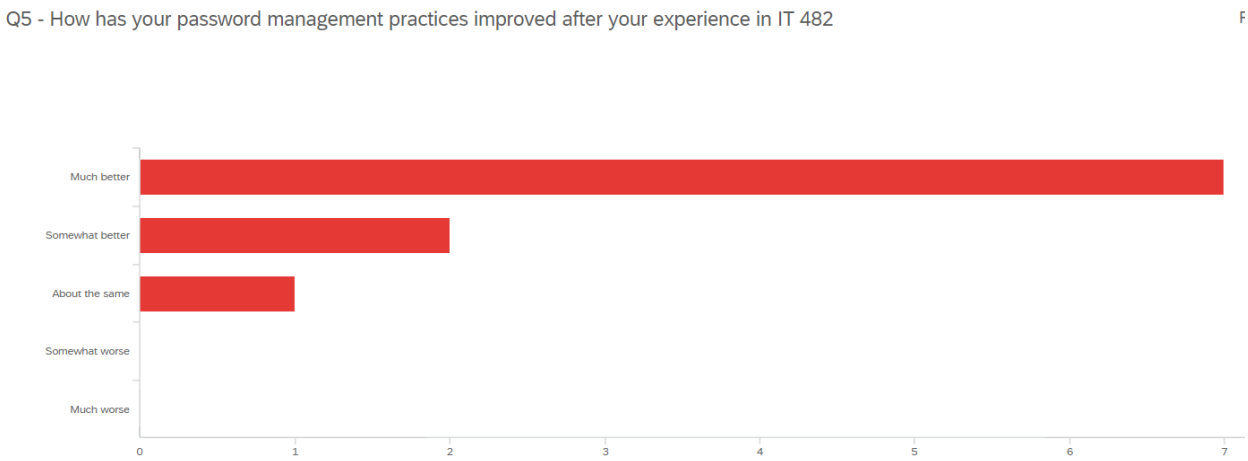

Figure 3 How has your password management practices improved

secure it is. We see this often with passwords, and it is incredible how many people still use "password" as their password. Making a pin or password easy makes it easier to crack.

2.6 Reinforce through the semester when doing the other scaffolded assignments

More significant synergies come into play when it is brought back into memory. Planned exercises in the scaffolded group are places where the safe cracking exercise is frequently mentioned.

3. Survey

We invited students from 2019, 2020, and 2022 to take a survey. Due to the inability to contact graduates successfully, all responses (n=10) out of 16 were from 2022. All 16 consented to the study, but only 10 answered questions other than the informed consent. The relevant questions and responses are below.

3.1 In IT 482 did you do something that you will never forget? If so, what was it?

This question was to see what stuck without leading them to what we wanted and is before any of the other questions referenced by this survey.

Relevant student responses include:

"I will never forget when we went through students password, we were scanning through the network for peoples username and password"
"Getting wifi passwords from other group's wifi router"

3.2 What do you most remember about opening a safe in IT 482?

Even though it is early in the class, it seems to impact the students significantly.

Responses include:

"the patterns of how most pin codes are created, they from left to right and top to bottom and that the pins are combination of characters that matters most to the owner."
"I remember that there is a pattern to follow in unlocking the safe."
"it was way easier then I thought it was going to be."
"That it can be easy to break through patterns."
"Listening to the clicks of the numbers when rotating"
"the pattern we used and also the hints in opening a safe"
"I remember that you can guess the code by observing any pattern of the rubbed off buttons."
"Patterns, humans being creatures of habit,"
"The patterns and the keys that have been pressed most often."

3.3 How has your password management practices improved after your experience in IT 482

We used a five-point Likert scale from much better to much worse. As budding cyber-security professionals, they all started at different levels, and we were asking about improvement. The results can be seen in figure 3. The bulk of the learners felt that they password management practices improved greatly by taking IT 482.

3.4 Do you agree that the safe cracking exercise helped you better understand human behavior and good password management?

We used a five-point Likert scale from strongly agree to strongly disagree. The results are shown in figure 4. We can see that most of the subjects felt that they better understood human behavior based on the safe cracking exercise.

3.5 Q7 - When you think about opening a safe in IT 482, how do you relate that to cyber security?

ISSN: 2473-4901
v8 n5757

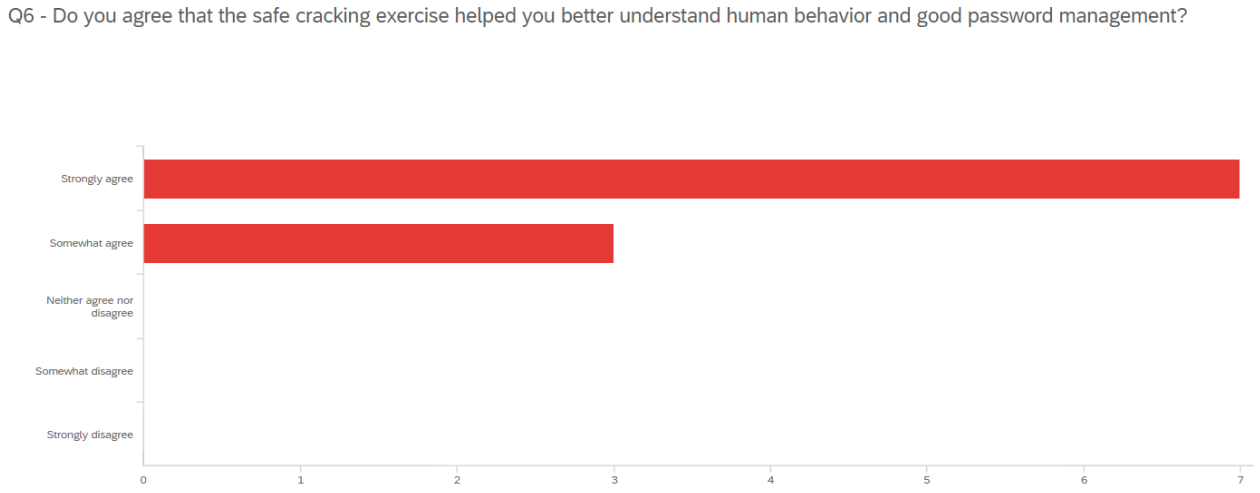

Figure 4 Safe cracking exercise helped you better understand human behavior

Finishing off the related questions with an open-ended question, we get some feedback on how it relates to cyber security.
"It is related by making it safe and not telling anyone you are opening it."
"Always make authentication hard so that information being kept is not very easy to hack. "
"Recognizing patterns and how people think and operate will help you secure and lock down systems better. "
"Hackers would learn users' pattern and habits so they can have more clues on how to cracking users' password."
"It is related by making it safe and not telling anyone you are opening it.
"Always make authentication hard so that information being kept is not very easy to hack. "
"Recognizing patterns and how people think and operate will help you secure and lock down systems better."
"Hackers would learn users' pattern and habits so they can have more clues on how to cracking users' password."

4. CONCLUSIONS

Teaching students to crack physical safes is an effective way to engage students in the class using physical objects they already comprehend to launch them into understanding the same concept, but virtually. It is an engaging activity that helps to entrench the desired learning.

5. ACKNOWLEDGEMENTS

Special thanks to Autumn Barraclough for being an excellent research assistant who significantly improves the work done in this paper. She graduates in Spring 2023 and is currently a senior double majoring in English and Information Technology. Her time helping to proofread and discuss the paper's topic has benefited the thoughts shared in the paper.

6. FURTHER RESEARCH

We suggest a study about password management instruction and comprehension with traditional learning vs augmented with experiential learning.

Another study with pedagogy and retention in cyber security would be beneficial. Do learners interested in cyber security learn better with joint productive activities, developing language competency, making it meaningful by connecting it to the student's life, teaching complex thinking, or engaging through dialogue?

7. REFERENCES

Alber, R. (2011, May 24). 6 Scaffolding Strategies to Use With Your Students. *Edutopia*. Retrieved June 15, 2022, from https://www.edutopia.org/blog/scaffolding-lessons-six-strategies-rebecca-alber

Dalton, S. S. (1998). Pedagogy Matters: Standards for Effective Teaching Practice. Retrieved June 15, 2022, from https://escholarship.org/uc/item/6d75h0fz#main

Wang, D., Gu, Q., Huang, X., & Wang, P. (2017, April). Understanding human-chosen pins: characteristics, distribution and security. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (pp. 372-385). Retrieved June 15, 2022, from https://doi.org/10.1145/3052973.3053031

Emanuel Von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. 2015.

Easy to Draw, but Hard to Trace?: On the Observability of Gridbased (Un)lock Patterns. In *Proc. the Conference on Human Factors in Computing Systems (CHI '15). ACM*, 2339--2342. Retrieved June 15, 2022, from http://dx.doi.org/10.1145/2702123.2702202

Erickson, M., & Kim, P. (2021). Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning. *Issues in Information Systems, 22(4)*, 9–20. Retrieved June 15, 2022, from https://doi.org/10.48009/4_iis_2021_9-21

Federal Trade Commission. (2022, February). *Consumer sentinel network*. Retrieved June 15, 2022, from https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf

Hemann, J. (2021). Mitigating It Security Risk in United States Healthcare: a Qualitative Examination of Best Practices *(Doctoral dissertation, Walden University)*. Retrieved June 15, 2022, from https://byuh.idm.oclc.org/login?url=https://www.proquest.com/dissertations-theses/mitigating-security-risk-united-states-healthcare/docview/2582085354/se-2?accountid=9816

Eiband, M., Khamis, M., Von Zezschwitz, E., Hussmann, H., & Alt, F. (2017, May). Understanding shoulder surfing in the wild: Stories from users and observers*. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 4254-4265). Retrieved June 15, 2022, from https://doi.org/10.1145/3025453.3025636

McKeachie, W. J., & Svinicki, (2006). McKeachie's teaching tips: Strategies, research, and theory for college and University Teachers (12th ed.). Houghton Mifflin.

Moscaritolo, A. (2018, July 20). 35 percent of people never change their passwords. *PCMAG*. Retrieved June 14, 2022, from https://www.pcmag.com/news/35-percent-of-people-never-change-their-passwords

Raman, M., Mclaughlin, K., Violato, C., Rostom, A., Allard, J., & Coderre, S. (2010). Teaching in small portions dispersed over time enhances long-term knowledge retention. *Medical Teacher*, 32(3), 250–255. Retrieved June 15, 2022, from https://doi.org/10.3109/01421590903197019

Security.org Team. (2021, October 1). America's password habits 2021. *Security.org*. Retrieved June 14, 2022, from https://www.security.org/resources/online-password-strategies/