Privacy and Security Perceptions in Augmented Cognition Applications

Michael-Brian Ogawa[1], Brent Auernheimer[2], Barbara Endicott-Popovsky[3], Ran Hinrichs[3], and Martha E. Crosby[1]

[1] University of Hawai'i at Mānoa, Honolulu, HI 96822, USA
{ogawam,crosby}@hawaii.edu

[2] Computer Science Department, California State University, Fresno, CA 93740, USA
brent@csufresno.edu

[3] Portland State University, Portland, OR 97201, USA
{endic,hinrichs}@pdx.edu

Abstract: Perceptions of security and privacy influence users' behavior with security mechanisms such as passwords and multifactor authentication. Users tend to practice insecure behaviors based on their perception of security and convenience. This paper highlights the alignment between privacy and security perceptions and the possibilities for augmented cognition in HCI and instructional design to improve security-related behaviors for access control.

Keywords: Security education, privacy, augmented cognition, access control, perceptions of privacy and security

1 Introduction

The subtitle of Derek Thompson's [16] essay of how science advancements are implemented (or ignored) is "invention alone can't change the world; what matters is what happens next". That is, the implementation of an idea changes the world, not simply the invention itself. When it comes to online applications and data, one of the "next things" is security and privacy.

Privacy and security are the nexus of, among other things, applied research in UI/UX, regulations and politics, reward and punishment, cognition, and technology. Perhaps less obvious, access control is a social activity and evokes emotion. If you are wronged, or private information compromised, or worse, you are endangered, past feelings can influence the use of security technology. We suggest that applied research is augmenting the users' cognition with the practices of privacy and security.

Solutions to security and privacy risks involving human behavior assume we consistently act rationally and make deliberate decisions. The preponderance of research from psychology suggests that deliberate thinking is not common. Norman [13] refers to levels of processing: visceral, behavioral, and reflective working together. He states

that reflective memories are often more important than reality when judging an experience because they may weigh positive interactions strongly enough to overlook severe drawbacks.

1.1 Cognitive Processes

Cognitive processes fall under categories labeled either conscious (rational or reflective) or automatic (visceral or behavioral) cognition. According to Kahneman, [7], much of human behavior is controlled by nonconscious automatic cognition. The deliberate rational cognition upon which most security models are based is triggered when automatic cognition detects something that is not normal. Rational cognition is influenced by the automatic cognition that preceded it. Automatic cognition is a process of pattern-matching a stimulus to a person's existing heuristic mental model [15]. These heuristics are influenced by an individual's personality and experiences and are tied to individuals and specific security situations.

Cognition is a necessary part of human functioning that is involved in completing digital tasks [8]. During a digital task, conscious cognition is mainly dedicated to the task while automatic cognition attends to a broader scope of elements of human functioning including the task processing, evaluation of its presentation features and assessment of other components of the general environment. Automatic cognition is fast but not necessarily accurate. It works by matching stimuli in the current context to readily accessible heuristics that are instinctive or learned from past-experience. It may include appraisal activities such as fetching or forming various heuristics and making of nonconscious judgements [7, 9, 15].

1.2 Security Education and Training

Traditional approaches to security education and training assume rational cognition. A different education intervention is needed to improve security compliance as people operate in the automatic cognition mode. [7]. In this case, attempts should be made to change an individual's heuristics or apply interventions that trigger rational or reflective cognition. Sometimes the results of the automatic system trigger the use of rational or reflective cognition. Initial empirical evidence suggests that most people's automatic cognition can detect the need for rational or reflective cognition, but there are large individual differences in choosing whether to override the automatic cognition mode and engage in processes that require considerably more effort. [7].

1.3 Typical Access Controls

A typical access control implementation is multifactor authentication. Typically, two factors are used for authentication (2FA) as a combination of user characteristics (such as fingerprints), knowledge (e.g., passwords), and property (mobile phones, or physical tokens such as "security keys" available to consumers [12]. Marky et al. [10] call this inherence, knowledge, and something that is owned. Each of the three factors present risks: passwords can be shared, weak or forgotten; property (mobile phones, tokens)

can be lost or compromised; and physical characteristics can be immutable, although research addressing this risk is underway [5].

Marky et al. [10] call this inherence, knowledge, and something that is owned. Although the use of multiple factors may seem obvious to technical staff, users can be frustrated if they don't understand the value of multifactor authentication. Marky et al. note "users are generally willing to follow a longer authentication process in exchange for more security", but the benefit must be "evident".

Passwords have been the most common single factor (knowledge). However, challenges exist between the usability and memorability of passwords. Unlike symmetric keys that are controlled by the verifier, memorized passwords are constructed by the user and are expected to be successfully recalled. Therefore, similar passwords may be composed and used in other logins. In many cases, memorable passwords that rarely change and are used for multiple logins avoid insecure habits such as writing down passwords [1]. The current password environment has design inconsistencies. A study by Choong et al. [3] found that more than 80% of 4573 participants preferred to create memorable passwords and devised ways to write down passwords to remember unrealistic amounts of information. As a result, "getting locked out is perceived as the biggest waste of time" [3]. Moreover, results from a large-scale study of more than 7700 accounts report user frustration of changing passwords. Although users replace passwords, algorithms can predict the new password resulting in a security vulnerability [17]. Furthermore, results from a 109-participant survey found that complex passwords do not aid memorability [6]. This perspective disputes the view that users are the primary source of password insecurities and scrutinize ineffective policy commanding excessive mandates on cognition [3]. Furthermore, the password lifecycle weights memory load and login experiences by impacting password choice regeneration [3]. Although memorable passwords are preferred, usability and security represent different goals [2].

Students in our work authenticate using a combination of passwords, and "pushes" to a mobile phone app (or to a physical token). Although it is practiced in many universities, its requirement varies across campuses. Colnago et al. [4] studied adoption of 2FA at Carnegie Mellon University (CMU) and found students said "it's not really that horrible". Both Marky and Colnago collected qualitative and quantitative data from university students, which highlighted the possibility of more complex authentication approaches with increased security.

With access controls such as passwords and MFA being prominent security concerns for individuals, the goals of the study focused on security behaviors of novice users based on their security background. The research targeted users' perceptions and experiences to guide the inquiry. The following questions were used as a guide for the study:

1. How are students' perceptions of personal computer security impacted by learning about security risks?
2. What type of learning has the greatest impact on participants' security practices?
3. What factors influence password sharing practices?

2 Exploratory Study

2.1 Participants

The initial study was conducted with students enrolled in an introductory computer science course for non-majors. Approximately 200-300 students enroll in the course each semester, which focuses on technology applications and introductory programming concepts. Participants came from over 30 different majors with a majority focusing their studies on Business Administration. The course is taught in a hybrid format and includes a lecture and laboratory component. Both lecture and laboratory portions of the course meet in-person once a week and have an on-line asynchronous session. The lecture focuses on the context and principles of computer science, while the laboratory targets the implementation of application and programming skills. Approximately 75% into the semester, the course includes a week-long unit on computer security, which includes general security concepts and its application using permissions in online environments.

2.2 Polls and Surveys

In-class polls during the security lecture captured live data while students were learning security concepts. These poll questions were implemented using the Poll Everywhere software, where participants submitted their polls via a Web interface. Poll questions highlighted the affordances and drawbacks of active and passive learning opportunities as various pedagogical approaches were utilized to promote learning.

In addition to the live lecture poll, a survey to collect students' insights after the completion of the security unit (both in-class and on-line asynchronous sessions) was implemented. The survey focused on underlying reasons students took actions regarding their security practices and their overall security knowledge development.

2.3 Analysis

A mix of quantitative and qualitative methods were used to analyze data for the guiding questions. The first question utilized a histogram of responses and a t-test to determine if there was as significant change in security perceptions, while the second and third questions included qualitative data that were coded using and open- and axial-coding strategy to determine themes for security actions and practices reported by students.

3 Results

3.1 How are students' perceptions of personal computer security impacted by learning about security risks?

Prior to learning about computer security, the researchers polled the students to determine their perceived knowledge about computer security (Fig. 1). Overall, 56% of

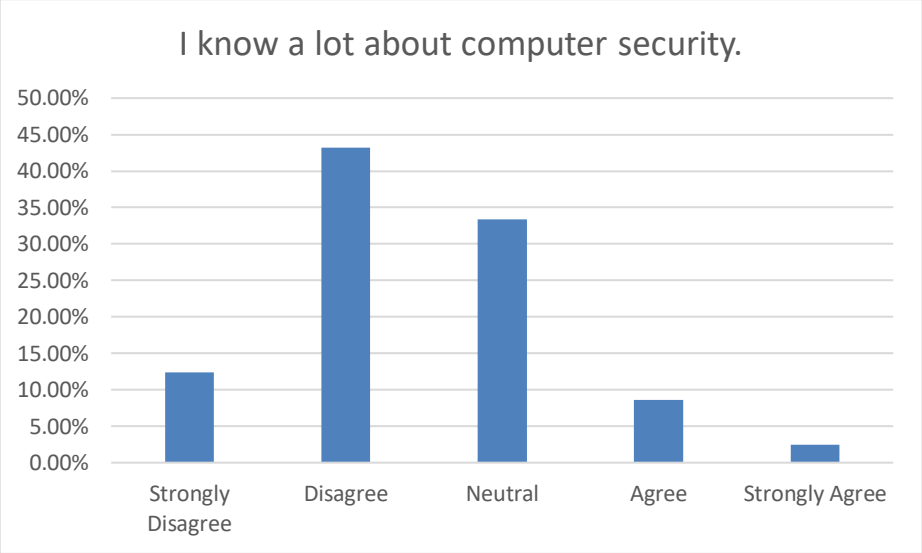

Fig. 1. Student initial perceptions about computer security prior to learning.

students felt that they did not know a lot about computer security, 11% believed that they had a strong background in the field, and 33% were neutral. Although students felt that they did not have a strong background in computer security, many were quite comfortable with the general security of their device usage (Fig. 2). Approximately 85% of students felt "okay" or better about their computer security prior to learning about security issues. Without learning about security, many participants did not have a strong background in the field and were quite comfortable with the security of their devices. After polling students, the instructor shared vignettes about security issues over the last decade including Heartbleed, Spectre, Meltdown, and various data breaches. After learning about these security issues, students were much more concerned about their security, with approximately 60% feeling vulnerable or not safe when asked about their feelings when using their devices. The paired t-test highlighted a significant change in means comparing the before and after responses by students ($p<.01$), with a before average of 2.60 and an after average of 2.07. These findings illustrate that those without knowledge of security issues were more comfortable with their security and that a short lecture (~10 minutes) about security risks can make a significant differences in perceptions of one's own security and its importance. It is vital to determine how the increase in knowledge-base can impact security practices of the participants to expand on Marky and Colnago's work.

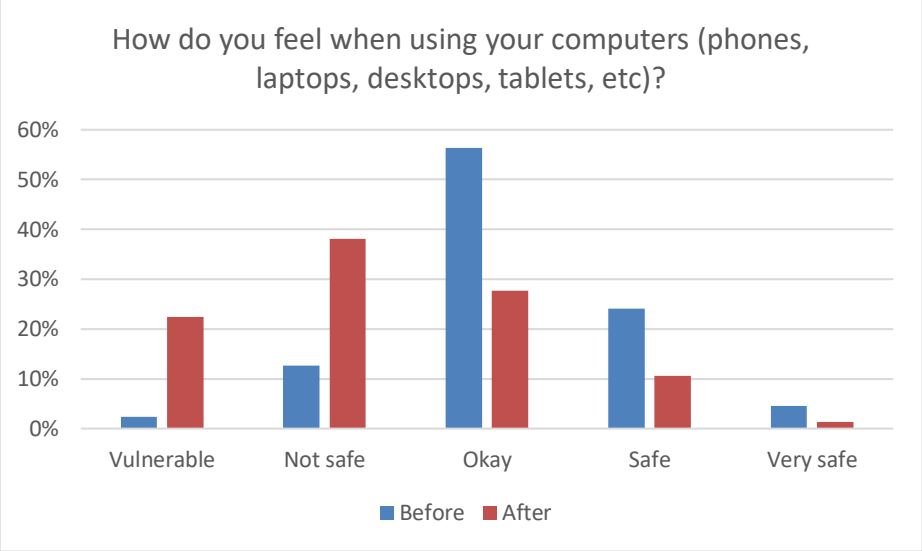

Fig 2. Comparison of vulnerability levels before/after security vignettes.

3.2 What type of learning has the greatest impact on participants' security practices?

The in-class lecture included a range of activities such as passive learning approaches (lecture) and active learning opportunities (activities completed by students). To supplement the passive lecture components, the instructor included poll questions to assess learning, guide content, and engage the students. The asynchronous lecture also utilized passive learning strategies (video lecture) and active learning approaches (working on activities and responding to questions on a quiz). Approximately 96% of the participants checked their email address at haveibeenpwned.com. Although 96% is a compelling number of participants, it is likely due to the check serving as one of the in-class activities. Therefore, the researchers measured the reported actions taken outside of class based on the in-class and asynchronous lectures (Fig. 3). Sixty-one percent of the students took a security action outside of class with 43% changing a password and 30% informing others about security risks. Thirty-nine percent did not take any actions to change their security practices. Of those that took action, 94% reported that the in-class lecture and activities were the main reason for taking action and 6% indicated that the asynchronous lecture was the underlying reason.

When reviewing the students' open-ended responses for taking action, we came across two major themes supporting the instructional approaches that led to students taking security actions outside of class. The first theme was the students' knowledge of data breaches and being a part of them by checking their email accounts at haveibeenpwned.com. Many found the in-class activity to check their email accounts to be engaging and quite surprising when they were a part of a data breach that included different types of sensitive information such as usernames, passwords, phone number, etc.

Fig. 3 Actions participants took as a result of instruction

When they found that they were a part of a data breach, they changed their passwords on breached sites. A student highlighted concerns with breaches, "My bank account got hacked less than a week after the lecture bc of a PayPal data breach." While another discussed their password changing habits due to the issue, "[I] Changed password due to data breach." The second theme that emerged was the use of the same or similar passwords across on-line platforms. Many students cited their newly learned concern about credential stuffing, using known credentials on other Web sites. A student that changed their passwords indicated, "I found that I use similar passwords and email on numerous sites." The instructional approaches supporting both of these themes included a short lecture component (a few minutes) and an in-class activity to highlight the issues and were demonstrative of the issue. Therefore, embedding active learning strategies with passive lectures yielded more action from the students than any single approach.

3.3 What factors influence password sharing practices?

To address password sharing practices, we surveyed students to determine if they share their passwords along with the different types of accounts they use. Passwords were categorized as either school credentials (official use) or service credentials/sub account (such as streaming video services using another site's email address as a username). Interestingly, 30% of respondents shared their school credentials, while 79% shared their service credentials (Fig. 4). Students' feedback highlighted the varied perspectives on the services and why they shared their passwords or not. For their official school account, they noted that it was tied to many different services including their course-work, registration, records, financials, and campus services. They found these services to be essential and were concerned about sharing this content with others. Students who

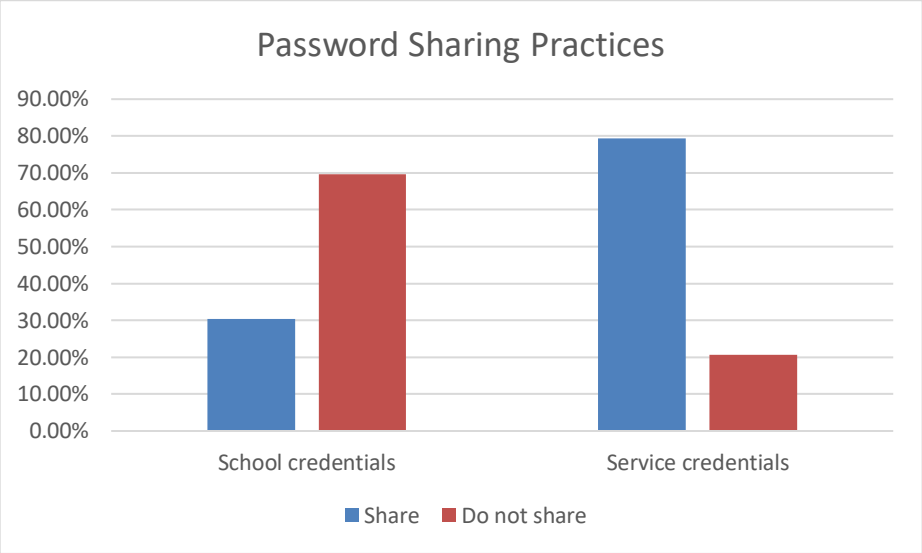

Fig 4. Password sharing practices

shared their credentials noted that they shared it with their parents to help account for services such as tuition payments. Participants also noted that multifactor authentication was a feature of their school account, so sharing passwords was less useful since the secondary authentication was needed. Respondents viewed service credentials as a specific usage compared to their school account. Many believed that they were paying for a service that could be utilized by multiple users such as streaming media. Therefore, they felt that they were getting "more bang for their buck" as others could use the service when they were not using it. In these cases, many reported sharing their credentials with those outside their immediate family, which is the opposite of school credentials that were shared with immediate family. They also found the lack or minimal use of multifactor authentication to be supportive of sharing their passwords. When comparing the two types of accounts, it is evident that convenience was a critical factor in sharing credentials with others.

The sharing of passwords was concerning to the researchers. They further studied credential sharing by asking if students planned to stop sharing their credentials after learning about its issues in the security unit. Of the respondents that shared passwords, 59% indicated that they intended to stop sharing credentials, while 41% stated that they would continue with their prior practices. We find these numbers to be promising and believe that using different instructional design strategies informed by augmented cognition has the potential for increased impact on behaviors.

4 Emergent Study

4.1 Participants

Additional research emerged from the results of the initial study. It was conducted with 25 undergraduate computer science students enrolled in a Human-Computer Interaction (HCI) course. HCI covers concepts and methodologies from human factors, psychology and software engineering that address ergonomic, cognitive, and social factors in the design and evaluation of human-computer systems. The course meets synchronously online once a week for class discussions and on-line asynchronous sessions to work on group projects. Each week students submit answers for the weekly discussions prior to each class meeting. During the class, they actively participate in class discussions on the posted questions and after class they submit their reflections on the class discussion by the end of the day.

4.2 Questions and Reflections

Previous results suggested that participants valued convenience and that it was an important factor contributing to their actual behavior for the following topics: remembering their passwords, credential stuffing (reusing their credentials), sharing their credentials, and multifactor authentication. The researchers examined how these topics naturally emerged during the posts prior to the class discussion, during the discussion itself and in their reflective posts at the end of the class day. During the fourth week of the semester, readings from Norman, D. [13] were assigned. They read chapter 3, "Knowledge in the Head and in the World." This chapter includes, among other things, general ideas and several examples concerning computer security. The assigned question that they were required to answer was: Explain what Norman means when he stated, "Make something too secure, and it becomes less secure." The class discussion was related to implementation issues concerning privacy and security.

4.3 Results

Using their rational or reflective cognition, the students were aware of recommended safe password protection and multifactor authentication practices. However, the posted answers to the discussion questions, the class discussion and the reflection comments indicated that their behavior depended more on convenience than on their rational implementation of safe cybersecurity practices. The initial posts for 24 of the 25 students posted something about passwords and how best practices were not routinely followed (Fig. 5).

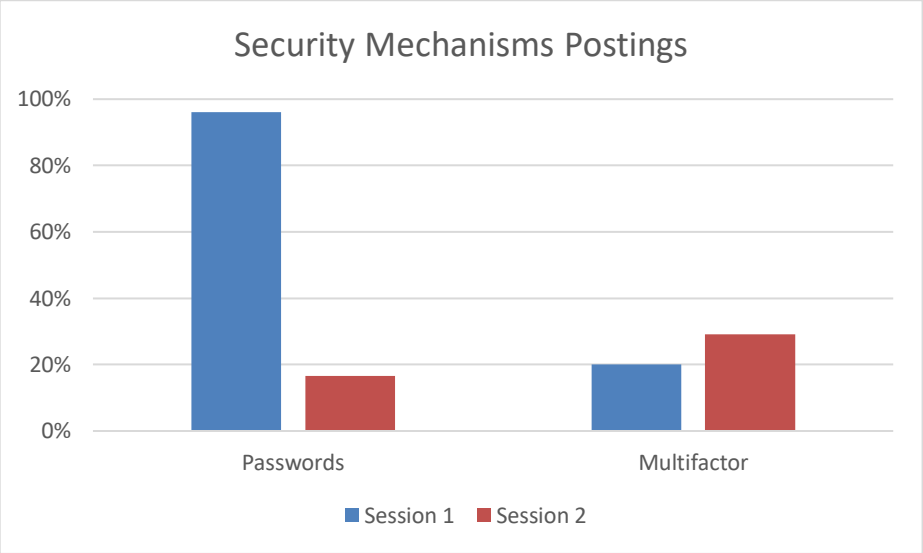

Fig 5. Postings about security mechanisms

For example one student posted the following comment:

> We value convenience more than anything. This is the reason why we create the same password for every website, so that we don't have to write them down everywhere, or remember a handful of passwords. This leads to a less secure person because if one account is compromised, then all accounts could be compromised. [sic]

Another student said:

> The internet is a mess of credentials all of which are supposed to be unique (but almost never are in practice.) In my job, every time there is a large data breach, we will search through all the exposed accounts for any campus email addresses and disable any that used the same password for their university account as the exposed website. This usually is not more than 100 or so accounts for each data breach, but almost all accounts used the same password for both the exposed site and their university account. In 2019 when Chegg had a data breach, we disabled thousands of university users' accounts. It is clear in practice almost no one follows internet password security recommendations.

Password issues were only mentioned by 4 of the 24 students in their final posting, a dramatic decrease from the almost unanimous initial posting.

> In the initial posting, only 5 of the 25 students discussed multifactor authentication, however, it was mentioned during the class discussion and mentioned by 7 of the 24 students in the final posting at the end of the class day. One of these students posted: After discussing what Norman says, the one comment that I found interesting the most is about two-factor authentication or 2FA. One said about how 2FA is required on their bank account and how tedious it can be. This tediousness leads to checking on the bank account less which is bad since checking on your bank account is important to do. [sic]

5 Augmented Cognition Applications

These studies highlighted the impact of instruction on perceptions of security risk and practices. Participants tended to increase their perception of risk and actual practices based on increased knowledge. The largest impacts came from mini lectures supported by active learning activities, which influenced participants' security practices including changing passwords and informing others about security risks. These findings serve as a foundation for future research utilizing augmented cognition to inform security-focused instruction.

When developing security education programs, one of the major challenges is to increase knowledge and change behaviors. For example, in teaching computing ethics in security, it is important to not only have students understand the ethical course of action but to make the ethical decision when the issue comes up in the "real world." Therefore, highlighting the mix of lecture and active learning opportunities may be critical to influence real-world decisions. Therefore, we propose augmented cognition approaches in future studies to better understand these factors and improve behaviors aligned with security-oriented education. Using time-based data aligned with on-line activities can help researchers to identify additional challenge and thought-process factors when refining learning opportunities for students. These time-based mechanisms can be used with a range of activities including tests, simulation assignments, and practical activities.

Human Computer Interaction (HCI) is a field that analyzes how users interact with information. Changes in psychophysiological signals of the human body are highly revealing of cognitive and emotional responses to stimuli, capturing even subtle and transient events. Psychophysiological tools, such as heart rate and skin conductance, can be very helpful in the characterization of emotional responses during human information interaction. Cognitive functioning activates various body systems such as the brain, facial brow muscles, heart and electrodermal systems. Various relationships between cognition and psycho-physiological signal change have been studied and documented. For example, some signals have been found to reflect such cognitive experiences as variation in mental workload [11], shift in attentive focus, and experiences of emotional affect such as disgust [14] Future research plans are to explore various psychophysiological correlates of cognitive interaction with cybersecurity events.

6 Acknowledgements

This material is based upon work supported by the National Science Foundation (NSF) under Grant No. 1662487. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

References

1. Adams, A., & Sasse, M. A. (1999). "Users are not the enemy." Communications of the ACM 42(12): 40-46.
2. Andriotis, P., Tryfonas, T., & Oikonomou, G. (2014). Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In the International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 115-126). Springer, Cham.
3. Choong, Y. Y. (2014). A cognitive-behavioral framework of user password management lifecycle. In the International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 127-137). Springer, Cham.
4. Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., & Christin, N. "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. April 2018. pp. 1-11. https://dl.acm.org/doi/10.1145/3173574.3174030
5. Feng, L., Cho, K.L., Song, C., Xu, C., and Jin, X. (2018). Brain Password: A Secure and Truly Cancelable Brain Biometrics for Smart Headwear. In MobiSys '18: The 16th Annual International Conference
6. Gao, X., Yang, Y., Liu, C., Mitropoulos, C., Lindqvist, J., & Oulasvirta, A. (2018). Forgetting of passwords: ecological theory and data. In 27th {USENIX} Security Symposium ({USENIX} Security 18) (pp. 221-238).
7. Kahneman D. 2011.Thinking, fast and slow. Macmillan.
8. Karray F, Alemzadeh M, Saleh JA, Arab MN. Human-computer interaction: Overview on state of the art. January 2008 International Journal on Smart Sensing and Intelligent Systems 1(1):137-159 DOI:10.21307/ijssis-2017-283
9. Loos L.A., Ogawa M.B., Crosby M.E. (2020) Cognitive Variability Factors and Passphrase Selection. In: Schmorrow D., Fidopiastis C. (eds) Augmented Cognition. Human Cognition and Behavior. Human Computer Interaction International 2020 and the Augmented Cognition Affiliated Conference, On-line, Copenhagen, Denmark. Lecture Notes in Computer Science, vol 12197. Springer, Cham.
10. Marky, K., Ragozin, K., Chernyshov, G., Matviienko. A., Schmitz, M., Mühlhäuser, M., Eghtebas, C., and Kunze, K. 2022. "Nah, it's just annoying!" A Deep Dive into User Perceptions of Two-Factor Authentication. ACM Transactions on Computer-Human Interaction. 29, 5, Article 43 (October 2022), 32 pages. https://doi.org/10.1145/3503514
11. Mogire, N., Minas, R., and Crosby, M., (2020) Probing for Psychophysiological Correlates of Cognitive Interaction with Cybersecurity Events in Foundations of Augmented Cognition 14th International Conference, AC Proceedings, Schmorrow, D., Fidopiastis, C. (eds.), Springer Lecture Notes in Artificial Intelligence.
12. Nield, D. (2023). (2023, February, 19), How to Unlock Your iPhone With a Security Key. Wired. https://www.wired.com/story/how-to-unlock-iphone-physical-security-key/

13. Norman, D. (2013). The design of everyday things. Revised and expanded edition. Basic Books.
14. Picard, R. (2016). Automating the recognition of stress and emotion: from lab to real-world impact. Multimed. IEEE. 23, 3–7 https://doi.org/10.1109/MMUL.2016.38.
15. Posner M. I., Snyder C. R. R. (1975). "Attention and cognitive control," in Information Processing and Cognition: The Loyola Symposium, ed Solso R. L., editor. (Hillsdale, NJ: Lawrence Erlbaum Associates), 55–85.
16. Thompson, Derek. Why the Age of American Progress Ended: Invention alone can't change the world; what matters is what happens next. *The Atlantic*. January/February 2023.
17. Zhang, Y., Monrose, F., & Reiter, M. K. (2010). The security of modern password expiration: An algorithmic framework and empirical analysis. In Proceedings of the 17th ACM conference on Computer and communications security (pp. 176-186). ACM