



HAL
open science

Assisting Users to Create Stronger Passwords Using ContextBased MicroTraining

Joakim Kävrestad, Marcus Nohlberg

► **To cite this version:**

Joakim Kävrestad, Marcus Nohlberg. Assisting Users to Create Stronger Passwords Using ContextBased MicroTraining. 35th IFIP International Conference on ICT Systems Security and Privacy Protection (SEC), Sep 2020, Maribor, Slovenia. pp.95-108, 10.1007/978-3-030-58201-2_7. hal-03440869

HAL Id: hal-03440869

<https://inria.hal.science/hal-03440869v1>

Submitted on 22 Nov 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Assisting users to create stronger passwords using ContextBased MicroTraining

Joakim Kävrestad¹ and Marcus Nohlberg¹

¹ University of Skövde, Skövde, Sweden
{firstname.lastname}@his.se

Abstract. In this paper, we describe and evaluate how the learning framework ContextBased MicroTraining (CBMT) can be used to assist users to create strong passwords. Rather than a technical enforcing measure, CBMT is a framework that provides information security training to users when they are in a situation where the training is directly relevant. The study is carried out in two steps. First, a survey is used to measure how well users understand password guidelines that are presented in different ways. The second part measures how using CBMT to present password guidelines affect the strength of the passwords created. This experiment was carried out by implementing CBMT at the account registration page of a local internet service provider and observing the results on user-created passwords. The results of the study show that users presented with passwords creation guidelines using a CBMT learning module do understand the password creation guidelines to a higher degree than other users. Further, the experiment shows that users presented with password guidelines in the form of a CBMT learning module do create passwords that are longer and more secure than other users. The assessment of password security was performed using the zxcvbn tool, developed by Dropbox, that measures password entropy.

Keywords: Security Training, Passwords, ContextBased MicroTraining, CBMT

1 Introduction

As the digital era continues, almost everyone around the world is becoming ever more present online. As our dependence on digital services increases so does our need for information security, and a key aspect of information security is security behavior including the ability to select good passwords to protect our social media accounts, work accounts, encrypted data and more. However, there is a wealth of papers demonstrating that users tend to select passwords that are easy to guess for an attacker [1-3]. Practitioners, as well as researchers, continuously try to find ways to make users select good passwords, by enforcing complexity rules or using different support systems [4, 5]. Another commonly proposed solution is to use other means of authentication instead of, or in combination with, passwords. Those other means of authentication include one-time passwords, hardware tokens, and password managers, and while the security benefits are undeniable they fail to be widely adopted [6]. A common denominator for why users select not to adopt a more secure behavior is usability, users seem to prefer ease of use over security [7, 8]. As such, a fundamental demand of any security function, especially one designed for the general population, should be usability.

In this paper, we consider a password to be a socio-technical property and argue that a secure password mechanism, for instance, an account registration web site, must not only consider computational security, but also the user. As argued by [9], a password mechanism's effectiveness relies on its ability to make a user select a good password willingly. Yet another important factor in information security is awareness [10]. It is widely believed that users will act more securely if they are aware of the risks of insecure behavior. A common suggestion for how to make users more aware is to train them. In this paper, we propose and analyze how the use of a novel training approach can make users select good passwords during password creation.

The aim of this study is to implement and test how the learning method called ContextBased MicroTraining (CBMT) can assist users in creating stronger passwords. The aim is studied using a two-step method beginning with a survey where participants are asked to create an account. During account creation, the participants are faced with password creation guidelines in different ways and the survey measures how well they learned the password guidelines that were proposed for the survey. The second step involved an experiment where users set to register an account for a local Internet Service Provider were presented with password creating guidelines presented according to the principles of CBMT. The passwords were evaluated and measured against passwords created by a control group that was not faced with any password creation guidelines. The results of this paper will be a demonstration of how CBMT can be implemented. The contexts of passwords were chosen since it is easy to measure the effect on passwords strength and passwords are unarguably crucial to security today.

The rest of this paper is structured as follows. Section 2 describes ContextBased MicroTraining (CBMT) and the password creation guidelines that were handed to participants in the study. Section 3 describes the methodology used. Section 4 presented the results of the study before it is concluded in section 5.

2 Background

This research demonstrates how CBMT can be used to train users to select good passwords and measures the effects of using CBMT in a real-world context. Therefore, this chapter is devoted to an explanation of what CBMT is and the theoretical foundation of CBMT. Further, the password guidelines proposed in the CBMT learning modules are explained and motivated.

2.1 CBMT

CBMT is a theoretical framework that outlines how information security training of users can be executed. In essence, CBMT can be summarized as follows [11]:

“CBMT stipulates that training should be delivered in short sequences, in an accessible format, when needed”.

On a more practical note, this means that training designed according to the principles of CBMT should be implemented so that it is presented to a computer user when he or she is in a situation where the training is of direct relevance. Further, it should be presented in a way that is easy to understand and short to minimize disruption [12].

The CBMT framework is based on the principle that people need motivation to learn. The idea is that the likelihood that any adult will learn is increased if the knowledge seems meaningful for the learner [13]. This notion is based on the concept of andragogy as presented by Knowles [14]. Knowles [14] argues that adults need the motivation to learn. The foundation in this way of thinking is that the learner will learn better if the knowledge presented seems meaningful. One way to accomplish this is to present knowledge in a context where it is applicable. As discussed by Herrington and Oliver [15], presenting knowledge to learners in a situation where the knowledge is applicable will cause a more meaningful learning experience. This is the first requirement that CBMT tries to facilitate. Also, by providing knowledge to a user when the user needs it brings a reminding effect. In this particular case, a user creating a password will be reminded to select a strong password. As discussed by [16], reminding users to behave in a secure way is likely to be effective in the information security domain.

Further, an obstacle in the sense of providing the computer user with knowledge about information security has been to make the users participate in education. One technique that has gained an increasing interest in recent years is microlearning or similar strategies including nanolearning and micro-training. As described by Wang, Xiao [17], nanolearning is a teaching method where information is presented in short sequences. The idea is to facilitate just-in-time learning meaning that information is provided in small chunks, thus making the time needed to absorb the information short and in an on-demand fashion [18]. As described by Bruck, Motiwalla [19], there has been research showing positive results of microlearning both in terms of learner participation and satisfaction. Microtraining is the second fundamental building block of Context-Based MicroTraining.

CBMT can be described as a framework that describes learning objects from two directions. The first direction concerns the delivery of the learning objects and states that the learning objects should be short sequences delivered in an on-demand fashion. The second direction concerns the content of the learning objects. In this respect, CBMT demands that the information presented in a learning module is of immediate use to the learner and therefore assumes that the information is relevant to the user in the users' current context. In this respect, CBMT tries to facilitate the concept of "learn by doing" theories that can be summarized as describing that learners learn better when they perform tasks instead of just reading [20]. CBMT is also a learning method that includes aspects of problem-based learning (PBL) in that it is designed to guide the learner through real-world tasks [21]. In summary, the meaningfulness is achieved by the learner doing some task related to his or her situation.

CBMT was first introduced by [22] and [23] who argued that CBMT could be used as an efficient way to counter online fraud. CBMT has been further evaluated in [11] where study participants reported that they perceived CBMT as a good way to learn about security [11]. CBMT has also been used to develop teaching material for technical courses in higher education with success [12].

In this study, CBMT is implemented as a means of teaching users how to create strong passwords at the point of account registration. In essence, a learning module is presented when a user that is creating an account hits the “create password” field. The module contains guidelines for how to create a strong password, as outlined in the next section. The approach, in this case, is inspired by security nudges as described by [24] but attempts to combine passive support with active intervention. At the end of the module, the user is asked to create her password. The steps of the learning module is presented in Figure 1, below.

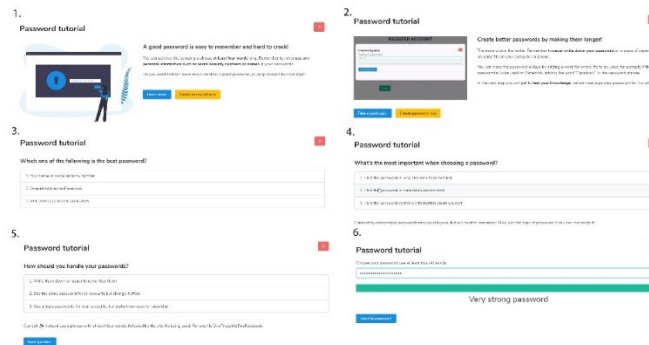


Fig. 1. Implementation of CBMT used in this study

The first part of the learning module presents the user with some fundamental password guidelines. The user may then continue to learn even more. After the second window, the user can test herself by answering three questions about the presented guidelines. An incorrect answer will generate feedback, and a correct answer will allow the user to continue. In the final windows, the user can create her password. A strength meter is also present on the last page. The user may choose to go directly to the last page from the first or second page.

2.2 Password guidelines

This paper is concerned with teaching users to select good passwords. What a good password actually is, is a question that is debated among scientists as well as practitioners. For instance, as of October 4th 2019, Microsoft suggest long and easy to remember passwords while Apple and Yahoo suggest that a password should include as many different character groups as possible [25-27]. Looking to influential standardizing organizations, NIST now suggest that password guidelines should suggest long passwords that are easy to remember, such as passphrases [28]. On the other hand, ENISA suggest mixing character types [29]. ISO/IEC 27002:2017, as another example, does state that a good password should easy to remember but does also discourage the use or words in passwords [30].

The password guidelines used in this paper are based on ongoing research into strong and memorable passwords and are based on [31] and [32]. They are designed to generate long passwords and read as follows:

- A good password is hard to crack and easy to remember
- It should consist of at least four words
- The password should not contain information relating to the password holder
- Passwords should never be written down
- A password can be made unique by adding the name of the site or service where it is used to itself

3 Methodology

This paper seeks to evaluate whether the presented CBMT learning module can assist users in creating stronger passwords. As described by [33], scientific validity is enhanced if a problem is researched from several angles. This study was carried out in two steps beginning with a survey where the participants were asked to create an account and then answer some questions about the password guidelines that was presented to them upon account creation. Then the learning module was implemented on the account creation site of a local ISP. The survey measured how well the users took notice of the presented guidelines and the experiment measured the actual effect the learning module had on password strength. To ensure compliance with ethical guidelines [34], care was taken to ensure that no passwords was disclosed to the researchers or any external party. An overview of the research process is shown in Figure 2, below.

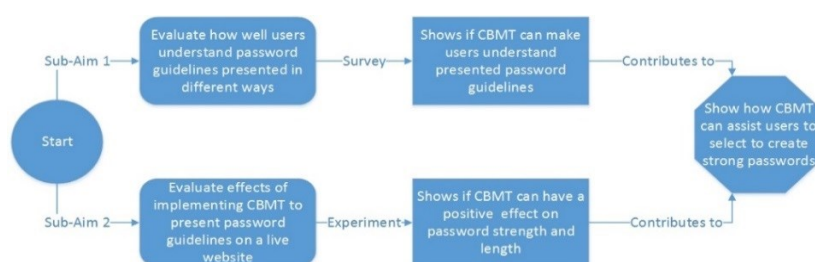


Fig. 2. Research process overview

Throughout the study, two different metrics was used to measure password strength. The first metric was password length in characters. The second metric is called score and is derived from zxcvbn, a password strength estimator developed by Dropbox [35]. According to a large study by [36], zxcvbn was found to be the most accurate password strength estimator. While zxcvbn calculates a number of metrics, the only one used in this paper is called score. The score is a value between 0 and 4 and the scored are described as follows [35]:

- 0 # too guessable: risky password. (guesses < 10^3)
- 1 # very guessable: protection from throttled online attacks. (guesses < 10^6)
- 2 # somewhat guessable: protection from unthrottled online attacks. (guesses < 10^8)
- 3 # safely unguessable: moderate protection from offline slow-hash scenario. (guesses < 10^{10})

- 4 # very unguessable: strong protection from offline slow-hash scenario. (guesses $\geq 10^{10}$)

The score is based on how many attempts an attacker would have to make to guess a password (entropy). To calculate the entropy, zxcvbn takes several factors into account including:

- Password length, longer passwords mean higher entropy
- Password complexity, use of different character types mean higher entropy
- Occurrence of common passwords, use of passwords common in leaked databases mean lower entropy, and use of individual words such as “potato”
- Repeated patterns, repeating patterns such as abcabcabc mean lower entropy

The full and exact algorithm used is presented in [35]. Both the score and the password length are considered to be numerical values in all statistical analyses used in this paper. The remainder of this section will detail the survey and the experiment.

3.1 Survey test

The first part of the study was a survey designed to measure if the participants paid attention to the password creation guidelines presented to them during account creation. The survey itself was not anonymized. Instead, the participants were asked to register an account with their e-mail address and a password of their choosing. They were also told that they would receive personal feedback containing their answers and a summary of the answers from the rest of the population.

The participants were invited to the survey via an e-mail containing a survey link. The survey was distributed to municipalities as well as university staff and students. The link led to a web-based informed consent form where the participants were asked to accept the conditions of the study. Upon accepting the conditions, the participants were randomly assigned to one of three groups; CBMT, TEXT, and LINK. They were then forwarded to the first part of the survey, account creation. During account creation, the participants were asked to register their e-mail and create a password. Password guidelines were shown the participants in the following different ways:

- The CBMT group was shown the CBMT module after clicking on the “select password” box.
- The TEXT-group was given the same guidelines in plain text just above the registration form
- The LINK-group was shown a link to text-based password guidelines labeled “Click here to learn more about good passwords”

Following registration, the password was analyzed as previously described and the participants were handed questions about demographic aspects including their IT-competence. Following the demographic questions, the participants were given the following questions about the password guidelines that was shown to them during account creation:

- Concerning the password guidelines presented on the previous page, how long passwords were suggested?
- What was suggested as a way to create strong passwords?
- What was described as most important for a password to be secure?
- What was described as most important of the following?
- What tip was given on how to create unique passwords for each of your accounts?

The first question was designed to see if the user's noticed the main point of the guidelines, the password length suggestion of four words. Questions two and three were used to see if the users understood the secondary suggestions, creating long and memorable passwords. The final two questions measured if users noticed tips that were presented at later stages in the guidelines, on how to make passwords even better and unique. In data analysis, two indexes were created. One that reflected how many correct answers each respondent gave to the first three questions and one index of correct answers to all questions. The results for the first question were also analyzed on its own.

For data analysis, the survey data were grouped based on the three test-groups. The participants were further grouped based on their reported IT-competence since previous research suggests that IT-competence is a key factor in security behavior [38]. The Shapiro-Wilks test was used to test whether the generated data were normally distributed [38], and the means and median are reported for the three variables (the first question and the indexes) in all groups. Based on central tendencies observed using descriptive statistics, hypothesis testing was used to evaluate if the tendencies were significant. Because of space limitations, the results are presented in condensed form. The hypotheses were expressed as follows:

H1: Group X scores higher than group Y regarding variable Z

H0: There is no difference between groups X and Z regarding variable Y

Further, Mann-Whitney U-test was used for hypothesis testing. Mann-Whitney U-test was selected in favor of T-test since no samples were normally distributed and are therefore more suitable than T-test [38]. The significance level used in this study is the conventional 95% meaning that results are significant if $p < 0.05$. SPSS was used for statistical analysis.

3.2 Experiment

In the second part of the study, the learning module presented in Section 2.1 was implemented on the account registration page of a local ISP. It was implemented so that 50% of the visitors used the learning module when they registered their account and the other 50% was presented with an unmodified version of the registration page. The unmodified registration page does not propose any password guidelines and is displayed in Figure 3, below.

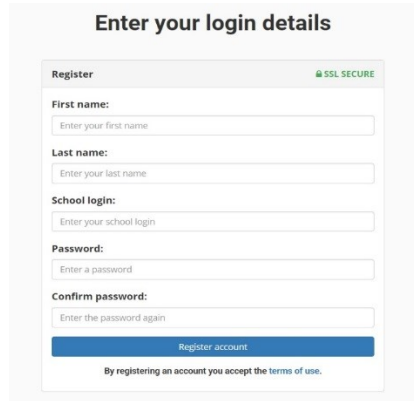


Fig. 3. Unmodified registration page

The password entered during the testing period was analyzed and password length and score were captured. Whether or not the password was created using the learning module was also recorded to allow for analysis of the effects of the learning module. For data analysis, the test data were grouped based on whether the passwords were created using the CBMT module or not. The Shapiro-Wilks test was used to test if the generated data was normally distributed [37], then means and median was reported for the two variables in both groups. Further, Mann-Whitney U-test was used to differences in values between the two groups. Mann-Whitney U-test was used since no samples were normally distributed and are therefore more suitable than T-test [38]. The significance level used in this study is the conventional 95% meaning that results are significant if $p < 0.05$.

4 Results

This section details the results gathered from the two parts of the study.

4.1 Survey

The survey was completed by 179 participants distributed among the answer groups as follows:

- CBMT: 54
- TEXT: 68
- LINK: 57

61 of the respondents rated the IT-competence as being “IT-professionals”, 50 respondents were students, 121 were working and 8 respondents reported having some other occupation. A majority of the respondents were between 20 and 30 years old (120), 31 were between 31 and 40 years and the rest were older. Following the calculations of the indexes, the mean and median values for the different metrics are displayed in Table 1,

below. The measures were not normally distributed in any group, mean and median values are displayed once for all respondents and then once for all respondents that did not report being IT-professionals.

Table 1. Mean and median values or metrics from survey

Variable	Group	Mean	Mean_noIT	Median	Median_noIT
Q1	CBMT	0,59	0,69	1	1
Q1	TEXT	0,40	0,38	0	0
Q1	LINK	0,19	0,16	0	0
Index1_3	CBMT	1,61	1,75	1	2
Index1_3	TEXT	1,27	1,20	1	1
Index1_3	LINK	0,77	0,67	1	0
Index1_5	CBMT	2,20	2,44	2	2
Index1_5	TEXT	1,86	1,84	2	2
Index1_5	LINK	1,31	1,18	1	1

As seen in Table 1, the CBMT group has the highest score for all metrics, followed by the group TEXT. The group LINK that only saw a link to password creation guidelines is last in all cases. Furthermore, the values for all metrics in the CBMT group increases when the responses from IT-professionals are disregarded. The same action fields the opposite result in the group TEXT.

Looking at the descriptive statistics in Table 1, the users that were presented with password guidelines using CBMT appears to understand the contents of the guidelines to a higher degree than in the other groups. Mann-Whitney U-test was used to test if the observed tendency is significant. The test was applied pairwise and for the complete answer groups as well as for all respondents except the IT-professionals. The test and results are presented in Table 2, below.

Table 2. Results of Mann-Whitney U-test, results are significant if $p < 0.05$.

Variable	Case	p	p noit
Q1	CBMT-TEXT	0,033	0,013
Q1	CBMT-LINK	0,000	0,000
Q1	TEXT-LINK	0,014	0,031
Index1_3	CBMT-TEXT	0,087	0,03
Index1_3	CBMT-LINK	0,000	0,000
Index1_3	TEXT-LINK	0,004	0,019
Index1_5	CBMT-TEXT	0,203	0,091
Index1_5	CBMT-LINK	0,000	0,000
Index1_5	TEXT-LINK	0,009	0,019

As seen in Table 2, all test values involving the group LINK are significant, showing that the participants shown a link to password guidelines understands the passwords guidelines to a lower degree than users shown the guidelines in text or using CBMT. Further, the test values for CBMT-TEXT are significant for Q1, showing that the users

of CBMT does understand the key part of the guidelines better than the other groups. Further, the value for CBMT-TEXT for Index1_3 is significant if users that consider themselves IT-professionals are disregarded.

In conclusion, the results of the survey show that using CBMT or just plain text to present password guidelines is significantly better than presenting users with a link to the guidelines. Further, the results suggest that CBMT will make the users notice the password guidelines better than presenting the guidelines as text. It is also worth mentioning that the observed results are more significant amongst users that do not consider themselves IT-professionals.

4.2 Experiment

In the experiment, a CBMT module showing the password guidelines was implemented at the account registration page of a local ISP. The passwords created by the users during the experiment were analyzed. A password score and the password length was registered. The passwords were never made available to the researchers but kept confidential by the ISP. During the test period, data was gathered from 124 users that created new accounts. 64 was presented with the CBMT learning module (This group is referred to as CBMT) and 60 was presented with the unmodified registration page (This group is called control). The mean values for password length and score are presented in Table 3, below.

Table 3. Descriptive statistics from experiment data

Variable	Group	Mean	Median	Normality test
Length	CBMT	11.14	11	Not normally distributed
Length	Control	10.52	9.5	Not normally distributed
Score	CBMT	3.06	3	Not normally distributed
Score	Control	2.40	2	Not normally distributed

As seen in Table 1, the values from the CBMT group is higher for password length as well as score. Further, no datasets were normally distributed and thus, the median is the most accurate measure. Reading the median values, the CBMT group scored 1.5 characters higher in password length and 1 higher in password score. The descriptive statistics bring the following hypotheses for testing:

- H1: Users presented password guidelines in the form of a CBMT learning module create longer passwords than users not presented with any guidelines.
- H2: Users presented password guidelines in the form of a CBMT learning module create passwords with a higher score than users not presented with any guidelines.

The corresponding null hypotheses are that no such difference can be observed. Mann-Whitney U-test was used to test if the observed tendency is significant. The results are presented in Table 4, below.

Table 4. Results of Mann-Whitney U-test, results are significant if $p < 0.05$

Variable	Group	Mean rank	Sum of ranks	p
Length	CBMT	70.15	4489.50	0.013
Length	Control	54.34	3260.50	
Score	CBMT	71.96	4605.50	0.002
Score	Control	52.41	3144.50	

As seen in Table 4, Mean rank and Sum of rank columns indicates that the passwords in the CBMT group are longer and have a higher score. The p-values are below 0.05 in both cases showing that the results are significant. In conclusion, the null hypotheses can be rejected in favor of H1 and H2. Thus, the experiment shows that the users who used CBMT to create passwords created stronger passwords than the users that used the unmodified registration page.

5 Conclusions

This paper presents the learning framework CBMT and analyzes if it can be used to help users create good passwords. The study explores the aim from two different directions; first by using a survey to measure to what degree users understand password creation guidelines presented in different ways and second, by implementing CBMT on the registration page of a local ISP and analyze the actual impact on password strength and length. Length and strength are used as independent measures since it is possible to create a longer password that is computationally weaker than a shorter. The results of the survey suggest that users that are presented with password creation guidelines with CBMT modules do indeed understand the guidelines to a higher degree than if users are presented with the guidelines as text, or with a link to password creation guidelines elsewhere. From the survey data, it is also worth mentioning that presenting password creation guidelines as text is better than a link. Furthermore, the results of the experiment show that using CBMT helps users create passwords that are longer and stronger than if the users are not presented with any password creation guidelines at all. As such, this paper concludes that using CBMT to present password creation guidelines will lead to users creating better passwords and understand the password creation guidelines to a higher degree than if the guidelines are presented in other ways.

This paper shows that CBMT can assist users in the creation of good passwords. However, it is interesting to notice that not even the participants that used CBMT noticed the presented guidelines to a very high degree. Looking at the most emphasized tip, using 4 words as the password only 59% of the respondents in the CBMT group remembered the tip. Looking at the scores for the index of all five questions the mean value in the CBMT group was 2.2 of 5. These numbers suggest that it is hard to make users notice password creation guidelines at all. An explanation could be that users are simply not too concerned with security, or that they do not care about what a certain application proposes.

It is, however, also interesting to see that CBMT has a high impact on password quality. In this particular example, the mean password strength was increased by 1 on

a 0-4 scale and the mean password length was increased by 1.5. The increase in password strength has an undeniable and direct effect on security since the passwords are much harder to crack. One explanation as to why the users using CBMT select stronger passwords might be that they understand the password creation guidelines to a greater extent. However, the relatively low scores from the survey suggests that that may not be a complete explanation. Another explanation can be that the CBMT forces the users to integrate with it and thus, reminds them of security.

The implications of this paper are twofold. The paper demonstrates and validates a concrete method for the presentation of password guidelines. The method described in this paper can be implemented by practitioners seeking to increase password security in their organization. The paper also presents a framework for how information security training can be used to improve user's security behavior. As such, the paper contributes to the scientific and practitioner community with new insights into the information security training domain.

Following this study, future projects could further examine the results presented in this paper with more studies using other and larger samples. Another direction for future research could be to analyze how CBMT can be used in other information security contexts to, for instance, assist users in dealing with online fraud, fake news or phishing. It would also be interesting to examine the long term effects of using CBMT. Knowledge retention and organizational security awareness are good starting points. A future study could examine the password culture before, during and after using CBMT for information security training.

References

1. Kävrestad, J., F. Eriksson, and M. Nohlberg, *Understanding passwords—a taxonomy of password creation strategies*. Information & Computer Security, 2019.
2. Wang, C., S.T. Jan, H. Hu, D. Bossart, and G. Wang. *The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services*. in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*. 2018. ACM.
3. Woods, N. and M. Siponen, *Too many passwords? How understanding our memory can increase password memorability*. International Journal of Human-Computer Studies, 2018. **111**: p. 36-48.
4. Brumen, B., *Security analysis of Game Changer Password System*. International Journal of Human-Computer Studies, 2019. **126**: p. 44-52.
5. Shay, R., et al., *Designing Password Policies for Strength and Usability*. ACM Trans. Inf. Syst. Secur., 2016. **18**(4): p. 1-34.
6. Petsas, T., G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis. *Two-factor authentication: is the world ready?: quantifying 2FA adoption*. in *Proceedings of the eighth european workshop on system security*. 2015. ACM.
7. Das, S., A. Dingman, and L.J. Camp. *Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key*. in *Proceedings of the International Conference on Financial Cryptography and Data Security*. 2018.

8. Whitten, A. and J.D. Tygar. *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*. in *USENIX Security Symposium*. 1999.
9. Weirich, D. and M.A. Sasse. *Pretty good persuasion: a first step towards effective password security in the real world*. in *Proceedings of the 2001 workshop on New security paradigms*. 2001. ACM.
10. Safa, N.S., M. Sookhak, R. Von Solms, S. Furnell, N.A. Ghani, and T. Herawan, *Information security conscious care behaviour formation in organizations*. *Computers & Security*, 2015. **53**: p. 65-78.
11. Hedin, A., *Lärande på hög nivå*. Uppsala universitet, 2006.
12. Knowles, M.S., *Andragogy in action: Applying principles of adult learning*. San Francisco: Jossey-Bass, 1984.
13. Herrington, J. and R. Oliver, *Critical characteristics of situated learning: Implications for the instructional design of multimedia*. 1995.
14. Parsons, K., Butavicius, M., Lillie, M., Calic, D., McCormac, A., & Pattinson, M., *Which individual, cultural, organisational and interventional factors explain phishing resilience?* , in *Twelfth International Symposium on Human Aspects of Information Security & Assurance*, 2018: Dundee, Scotland, UK: University of Plymouth.
15. Wang, M., J. Xiao, Y. Chen, and W. Min. *Mobile learning design: The LTCS model*. in *Intelligent Environments (IE), 2014 International Conference on*. 2014. IEEE.
16. McLoughlin, C. and M. Lee, *Mapping the digital terrain: New media and social software as catalysts for pedagogical change*. Ascilite Melbourne, 2008.
17. Bruck, P.A., L. Motiwalla, and F. Foerster, *Mobile Learning with Micro-content: A Framework and Evaluation*. Bled eConference, 2012. **25**.
18. Koedinger, K.R., J. Kim, J.Z. Jia, E.A. McLaughlin, and N.L. Bier. *Learning is not a spectator sport: Doing is better than watching for learning from a MOOC*. in *Proceedings of the second (2015) ACM conference on learning@ scale*. 2015. ACM.
19. Boud, D. and G. Feletti, *The challenge of problem-based learning*. 2013: Routledge.
20. Kävrestad, J. and M. Nohlberg. *Online Fraud Defence by Context Based Micro Training*. in *HAIISA*. 2015.
21. Werme, J., *Security awareness through micro-training: An initial evaluation of a context based micro-training framework*. 2014.
22. Kävrestad, J., M. Skärgård, and M. Nohlberg. *Users perception of using CBMT for informationsecurity training*. in *Human Aspects of Information Security & Assurance (HAIISA 2019) Nicosia*, 2019.
23. Kävrestad, J. and M. Nohlberg. *Using context based micro training to develop OER for the benefit of all*. in *Proceedings of the 15th International Symposium on Open Collaboration*. 2019. ACM.
24. Furnell, S., R. Esmael, W. Yang, and N. Li, *Enhancing security behaviour by supporting the user*. *Computers & Security*, 2018. **75**: p. 1-9.
25. Microsoft. *Security Identifier*. 2019 [cited 2019; Available from: <https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/security-identifiers#security-identifier-architecture>.
26. Yahoo. *Password tips*. n.d; Available from: <https://safety.yahoo.com/Security/STRONG-PASSWORD.html>.

27. Apple. *Security and your Apple ID*. n.d [20190912]; Available from: <https://support.apple.com/en-us/HT201303>.
28. Grassi, P., et al., *NIST Special Publication 800-63b: Digital Identity Guidelines*. 2017, National Institute of Standards and Technology (NIST).
29. ENISA. *Authentication Methods*. n.d [20191004]; Available from: <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods>.
30. ISO/IEC, *Information technology - Security techniques - Code of practice for information security controls*. 2017, ISO/IEC.
31. Lincoln, Y.S. and E.G. Guba, *Naturalistic inquiry*. Vol. 75. 1985: Sage.
32. Schrittwieser, S., M. Mulazzani, and E. Weippl. *Ethics in security research which lines should not be crossed?* in *Security and Privacy Workshops (SPW), 2013 IEEE*.
33. Wheeler, D.L. *zxcvbn: Low-Budget Password Strength Estimation*. in *USENIX Security Symposium*. 2016.
34. Carnavalet, X.D.C.D. and M. Mannan, *A large-scale evaluation of high-impact password strength meters*. *ACM Transactions on Information and System Security (TISSEC)*, 2015. **18**(1): p. 1.
35. Dropbox. *Low-Budget Password Strength Estimation*. 2019 [20191007]; Available from: <https://github.com/dropbox/zxcvbn>.
36. Siponen, M.T., *Five dimensions of information security awareness*. *SIGCAS Computers and Society*, 2001. **31**(2): p. 24-29.
37. Mendes, M. and A. Pala, *Type I error rate and power of three normality tests*. *Pakistan Journal of Information and Technology*, 2003. **2**(2): p. 135-139.
38. McKnight, P.E. and J. Najab, *Mann-Whitney U Test*. *The Corsini encyclopedia of psychology*, 2010: p. 1-1.