ContextBased MicroTraining: A Framework for Information Security Training

Joakim Kävrestad, Marcus Nohlberg

ContextBased MicroTraining: A Framework for Information Security Training

Joakim Kävrestad[1] and Marcus Nohlberg[1]

University of Skövde, Sweden *firstname.lastname*@his.se

Abstract. This paper address the emergent need for training measures designed to improve user behavior in regards to security. We do this by proposing a framework for information security training that has been developed for several years and over several projects. The result is the framework ContextBased MicroTraining (CBMT) which provides goals and guidelines for how to better implement information security training that supports the user in the situation where the user needs support. CBMT has been developed and tested for use in higher education as well as for the support of users during passwords creation. This paper presents version 1.0 of the framework with the latest refinements.

Keywords: Security training · awareness · ContextBasedMicroTraining · information security

1 Introduction

It is well established that insecure user behavior is a major problem in information security [25]. Users are commonly referred to as the weak link in security and while there are many technical security measures that address technical security issues, there is still a need for ways to improve user behavior with regards to security [7]. Threat actors recognize this notion and are often exploiting users, making the need for measures towards secure behavior emergent [11]. Desmand [8] described a need for making users understand the consequences of insecure behavior and learn them to behave in a secure way [8].

The common suggestion for how to improve user behavior is through the use of training [24]. Further, there are many different suggestions on how to carry out security training, from the practitioner as well as the research community. Different training measures range from lectures to micro training and nudges or special purpose tools such as password strength meters. While there are research examples of individual studies where researchers provide good evidence that specific methods work, there are reports that suggests that organizations training programs are not grounded in empirical evidence of their validity [1, 2]. As such, the need for further research into this area is apparent.

This paper reports on research in this area that has been ongoing since 2014 intending to address the following objectives:

- O1: Develop a framework of guidelines for user training that supports user awareness and security-related decision making.

– O2: Evaluate how the framework developed in O1 can assist in making users act more securely
– O3: Evaluate if the framework from O1 can be applied in higher education

As such, the paper will present and discuss the framework developed in the projects and focus on the later parts of the development where the framework is refined. Following the presentation of the research process, previously published work will be accounted for and briefly described. The paper will then discuss the final part of the research process and present the final framework developed in the research. The paper will be concluded with a discussion on the topics and directions for future work.

2 Research process

The research has been carried out in multiple steps and the complete process is outlined in figure 1, below. The emphasis in this paper is on the final parts of the research process (made bold in Figure 1) The research as a whole employs a

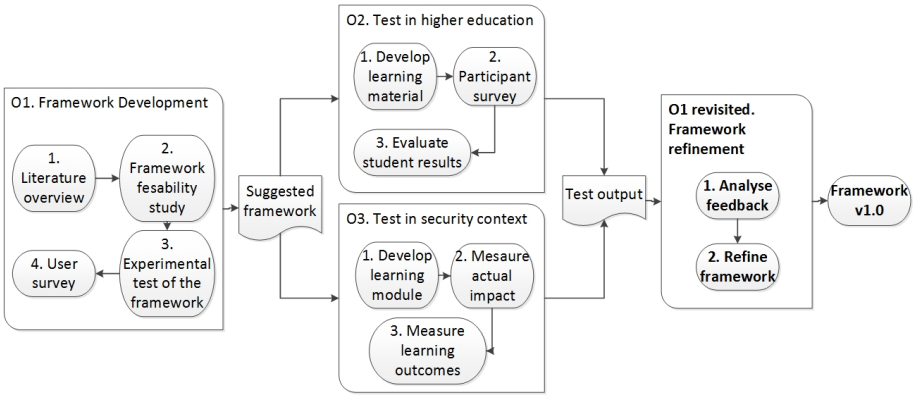

Fig. 1. Research process

mixed-method approach using qualitative as well as quantitative methods. The reasoning behind this approach is twofold:

– Some research steps are intended to provide input to the development of the framework, making a qualitative approach feasible, while other steps intended to measure the effects of implementations of the guidelines making a quantitative approach feasible.
– Using different methods in research around the same objective, triangulation, can increase the validity of the outcomes [21].

While a discussion on all methodological approaches used in the research is well beyond the scope of this paper (and previously published [12, 16, 18, 17, 13])

the remainder of this section will introduce the methodology used in the final research steps, "Framework refinement".

During the evaluation step, quantitative data was used to evaluate implementations of the framework and qualitative data about the frameworks as well as the implementation of the framework was gathered. The data was gathered using free-text survey questions. Further, the suggested framework was presented at the 19th Seminar within the Framework of a Swedish IT Security Network for PhD students (SWITS) [13] and the following discussions were summarized and considered in the framework refinement. The gathered data was analyzed using the principles of thematic coding [5]. The following codes were established prior to the analysis:

- Strengths
- Weaknesses
- Clarification needed

The first code was used to identify the strengths of the framework. The second and third codes were used to identify areas in the framework that needed reconsideration or improvement. The coding was performed together by the authors and the results were used to refine the framework and establish the final framework as presented in this paper.

3 Previous research steps

This chapter briefly presents previous research in this project beginning with the developed framework, ContextBased MicroTraining(CBMT). Then, the implementation and evaluation of CBMT based training will be presented.

3.1 CBMT and the development thereof

The development began with a literature search that intended to find what goals the framework should seek to fulfill. Fundamental problems in the domain of information security training were identified to be that users are not actively participating in information security training measures [19] and that users, while worried about cyber threats, lack awareness about the possible damage they can cause [22]. It was also evident that several sources reported that security measures must, in themselves, be easy to use, appear useful and interrupt the user's normal computer usage as little as possible [28, 23, 3]. Following the literature search, four requirements for what was called a "Situated Learning based defense mechanism" were established:

- Provide training that users want to make use of, instead of forcing users to participate in the training
- Include an awareness increasing mechanism
- Provide training to the user when the user is in a situation where the training is relevant

– Require no prior knowledge from the user

The first two bullets were achieved by the third bullet and the idea was that information security training should be delivered to the user when the user entered a situation where the training was of direct relevance. For instance, a training module designed to teach the user about online fraud would be presented to the user when she was in a situation where she risked being defrauded [12]. A fundamental notion in the requirements is that people need motivation in order to learn and that adults will be more likely to learn if the presented information seems meaningful, a notion based on the concept of andragogy [20, 10].

A demonstrator of a defense mechanism based on the requirements was implemented, the context was online fraud. A survey containing the demonstrator and questions about how the respondents perceived it was presented. 98 respondents answered the survey and it revealed that the respondents were, overall, positive towards the defense mechanism. The survey data did, however, stress that it was important for a defense mechanism to not be enforcing and that it should be possible to read the information presented quickly [12]. This falls well in line with what Nanolearning tries to facilitate [26]. Previous research into microlearning also shows positive results in terms of learner participation [6]. Supporting a high degree of user participation is one of the fundamental problems this research aims to address. The requirements were updated, and expressed as a small framework of goals and guidelines were the goals reflect the overall goal of the framework and the guidelines are more practical implementation guidelines. The goals were the following:

– Provide training that users want to make use of, instead of forcing users to participate in the training
– Include an awareness increasing mechanism
– Require no prior knowledge from the user
– Be short and easy to absorb

And the guidelines were:

– Delivered to users when it is relevant to their current situation.
– Delivered in short sequences
– Relevant to the users' current situation
– Include a practical element
– Must be possible to opt-out

Simultaneously, an experiment where participants were asked to use the defense mechanism before rating fraudulent ads from Swedish online marketplaces was carried out. A control group rated the same ads without training. The experiment showed that the group that performed the training was better at detecting fraudulent ads than the participants in the control group. They were also better at correctly identifying legitimate ads as legitimate suggesting that the defense mechanism could be useful [16].

Next, another survey measuring how the respondents perceived using training modules developed according to the framework was performed. In this case,

the respondents were asked to follow three different training modules (password creation, ransomware, and phishing) and then asked about their experience. In summary, the participants were positive towards the training modules and stressed that short sequences of training in-the-moment are preferable to training that is timeconsuming [18]. As such, the framework was established and the research continued to an evaluation phase. The Framework was named ContextBased MicroTraining (CBMT).

To summarize, CBMT is a teaching method that suggests that information should be presented in short sequences to the learner. It should also include a practical element and be of direct relevance to the user's current situation. A visual representation of CBMT is presented in figure 2, below.

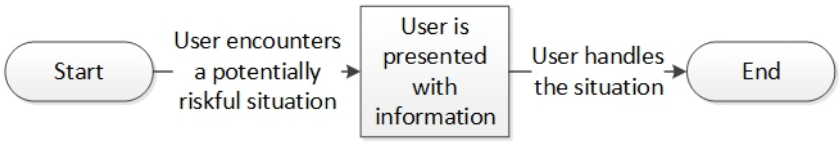

Fig. 2. CBMT overview

3.2 Evaluation of CBMT for use in higher education

Following the establishment of the framework, it was evaluated in two settings. First, for use in higher education. In this evaluation, a technical undergraduate course was used and the purpose was to measure learning outcomes of CBMT based training. The course was a Cisco Network Academy course and was selected since it was very practical in nature and it teaches a standardized curriculum and is examined using a standardized test. In this particular case, the course was thought by the researchers and the use of standardized material served as a means of minimizing bias. Applying the framework to a course was selected because it allows for a relatively controlled environment where the actual learning outcomes can be compared to the learning outcomes from previous times the course has been given.

During this evaluation, several learning modules were designed according to the goals and guidelines of the framework. The students were then handed the modules as primary lecturing material. The nature of the modules was that they asked the students to listen to a short theoretical presentation and then do or follow a practical task. One module covered a small bit of theory and the time needed to consume one module was kept to a minimum. Several modules were created and combined into video lectures that covered the full curriculum. A version of the modules can be found and used freely at YouTube [1] The teaching was combined with supervision that allowed the students to ask questions and

[1] www.youtube.com/playlist?list=PLEjQDf4Fr75qADv9J0UbNaiUmB8zMhw6V

discuss the content of the learning modules. The course ended with a practical and theoretical test. In terms of learning outcomes, the students that used the material developed according to the CBMT framework performed similar to, or slightly better than students from previous years where the same material was delivered as traditional lectures. The students were handed a survey that measured how they perceived the lecture material and 26/28 students reported that they preferred the CBMT learning modules over traditional lectures, when asked to pick one or the other. Further, the students reported that the CBMT learning modules motivated them in their studies and made them understand the theoretical material [17]. In terms of usage, 75% of the students reporting using 9 or 10 of the 10 available video lectures.

3.3 3.3 Evaluation of CBMT for Information security training

In another evaluation, CBMT was evaluated as a means of assisting users in selecting better passwords. In this case, an interactive CBMT module was created and implemented at the account creation page of a local internet service provider. The module was activated when a user clicked in the "create password" field and is showcased as a demonstrator at GitHub[2] . In essence, a window presenting basic password security tips was presented, the guidelines themselves were based on Kävrestad et al. [15]. The tip was to use passwords made up of four words or more. The user could then decide to learn more or to create a password. Upon selecting learn more, the user was presented with a series of questions that gave direct feedback and upon clicking create password, the user was taken to a password creation step.

50% of the users on the web site were assigned to use the CBMT module during account creation, the other 50% used the original account creation page. The strength of passwords created by the users was measured using the zxcvbn method by Dropbox [9]. The experiment showed that users that used the CBMT module created stronger passwords than users in the control group. The effect was measured on a 4-graded scale that reflected password entropy as described by [27]. The group using the CBMT module had a median value of 3 while the other group had a median or 2, and the result was statistically significant at the 99% level.

Following the experiment, a survey was executed where participants were presented with password creation guidelines using the CBMT module, in plain text or using a link to plain text. They then received questions about the guidelines just presented to them. The survey suggested that the participants presented with the CBMT module were slightly more aware of the password guidelines than the users presented with plain text. They were significantly more aware of the guidelines compared to the users that received a link to plain text guidelines. The results of this evaluation show that CBMT can serve as a framework for the development of effective information security training that fulfilled the goals of

[2] https://rr222cy.github.io/SecurityAssistantWidget/

the CBMT framework. The results of this study are accepted for publication in IFIP SEC 2020.

4 Guideline refinement and establishment

Following the evaluation of the CBMT in higher education and for presentation of password creation guidelines, the framework was further refined. This refinement was used in a three-step process:

1. Insights acquired by the researchers during the evaluation were considered.
2. The framework was presented and discussed at the 19th Seminar within the Swedish IT Security Network for PhD students (SWITS).
3. Free-text answers acquired from the surveys in the evaluation phase were analyzed.

During the evaluation of CBMT for use in higher education is became evident that while the framework suggests that training should be carried out in naturally occurring situations, such as when a user is browsing the Internet, this is not always possible. In some cases, the situations need to be constructed. A constructed situation includes a situation that the user is put in rather than a situation that the user encounters. A user would, for instance, encounter phishing making that encounter a natural situation. On the contrary, a constructed situation would be when the user is asked to carry out a task as part of education or training. Subsequently, when CBMT is used in a natural situation it is used in direct relation to a practical element and does not in itself include the practical element. On the other hand, it must include a practical element itself when used in a constructed situation. The guidelines in the framework were updated to support this insight.

During the discussion at SWITS, several conference participants were positive about the framework but suggested that what the framework presents must in itself be easy to follow. The original intention of the framework was to not consider the actual material presented, only the delivery thereof. However, the consensus in the discussion at SWITS led to a new guideline reflecting that the information presented must be easy to follow. That is certainly in line with the goal that states that no prior knowledge should be required by the users. The need for this addition was further made evident from the evaluation in the context of password guidelines. It is clear that many password creations guidelines are hard to use [14, 4, 29] and one can consider the meaning of a good delivery if the information itself is hard to use.

The free text answers from the surveys in two validations steps (O2 and O3) were analyzed using thematic coding. The coding was performed by the authors together simultaneously to enhance inter-coding validity. The coding revealed no negative comments about the framework and 11 comments that were positive but did not otherwise add to the development of the framework.

Several users expressed that they did not follow the guidelines in favor of their own more complex password creation guidelines. None of these users reported

being negative about the learning module. This suggests that the learning module was not annoying for advanced users. Typical information security training tools, including this, is targeting all users. We argue that training presented to users that do not perceive that they need the training can be interpreted as an annoyance rather than provide value. It is therefore important that tools built using the CBMT framework are developed so that they minimize interruption and annoyance, and provide a way for users to skip the training, especially if it is repetitive.

In line with this reasoning, it is important that the presented material really highlights the most important aspects of the subject matter, a notion that was also identified in the analyzed material. While it is important that the presented material covers the essential information the users need, it is evident from the analyzed information that most users will only notice some aspect of the presented material. It is therefore important that the most crucial points in the material are, in some way, highlighted even more. One example of highlighting, which was used in the password training module, was to make the most important points bold.

Following the refinements, the final goals and guidelines of CBMT are as follows (modifications in the refinement step are in *italic*):
Goals:

- Provide training that users want to make use of, instead of forcing users to participate in the training
- Include an awareness increasing mechanism
- Require no prior knowledge from the user
- Be short and easy to absorb
- *Should minimize annoyance for all users, especially users already familiar with the subject*

Guidelines:

- Delivered to users when it is relevant to their current situation. *The situation can be constructed or natural.*
- Delivered in short sequences
- Relevant to the users' current situation
- Include *or directly relate to* a practical element
- *The information presented must in itself be easy to understand*
- *The most crucial points of the information should be highlighted*
- Must be possible to opt-out *or skip*

5 Discussion

This paper reports on the latest steps of research that has been ongoing for several years and spanned several projects. The overall aim of the research has been to address the area of end-user training in information security. In this area, many suggestions for how to conduct information security and awareness training

have been presented and tested, yet we are still in the situation that end-user behavior remains one of the most highlighted threats in the cyber domain.

This research began with a review of the area and initial ideas for how information security training could be conducted leveraging theories about how humans are motivated to learn. It was found feasible to train users about topics that relate to what they are doing, and present training in situations where it is of direct relevance and use to the user. At this point, a suggested framework of goals and guidelines for how to implement training mechanisms was presented.

The suggested framework was tested and analyzed in two different contexts, higher education and password creation. Higher education was chosen because it offered an opportunity to present students with reoccurring training and an ability to measure not only the direct effect but also the learning outcomes some weeks after the training was performed, in the form of exams. Password creation was chosen as the other case since it offered a good way to measure the effects of the training. In this particular case, passwords created after being presented with a password guideline training module were measured and compared with passwords that were not created using the training module and was found to be stronger. As such, the two parts of the testing process shows that the CBMT framework can yield direct results and sustained knowledge for the user.

The emphasis in this paper has been the final refinement of the framework following the testing. The refinement was based on insights drawn during the implementation of the guidelines, conference discussions and qualitative data gathered during the testing phase. The refinement phase revealed that several users were positive to the CBMT learning modules they have used and some refinements that were previously presented.

The scientific contribution of this paper is further insight into how effective information security training should be carried out. It also presents a concrete framework for information security training that we consider to be a version 1.0. It is tested in some contexts but can be developed, tested and extended further and we encourage others to continue to research around the framework that we present. The research also raises an interesting ethical point, is it ethical to continue to use the training methods that are proven not to be effective or should effort be made into developing new and better methods?

The research also brings value to the practitioner community. First, the research has resulted in implementations of CBMT that are free to use [3] . Second, the paper present a concrete and tested framework for how effective information security and awareness training can be implemented.

While this paper present a framework that we argue is ready for use, there is still room for further development and verification. Future projects could take a pedagogical angle and review the framework from a pedagogical perspective. Another area for future work is to implement CBMT in more security-related

[3] Password guideline module: github.com/rr222cy/SecurityAssistantWidget, Cisco Certified Network Associate training videos: www.youtube.com/playlist?list=PLEjQDf4Fr75qADv9J0UbNaiUmB8zMhw6V

contexts and evaluate the results. This can, for instance, include phishing, online fraud and more.

References

1. Al-Daeef, M.M., Basir, N., Saudi, M.M.: Security awareness training: A review. In: Proceedings of the World Congress on Engineering. vol. 1, pp. 5–7 (2017)
2. Alshaikh, M., Maynard, S.B., Ahmad, A., Chang, S.: An exploratory study of current information security training and awareness practices in organizations. In: Proceedings of the 51st Hawaii International Conference on System Sciences (2018)
3. Beckles, B., Welch, V., Basney, J.: Mechanisms for increasing the usability of grid security. International Journal of Human-Computer Studies **63**(1-2), 74–101 (2005)
4. Biocco, P., Anwar, M.: Grid framework to address password memorability issues and offline password attacks. In: International Conference on Applied Human Factors and Ergonomics. pp. 52–61. Springer (2017)
5. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative research in psychology **3**(2), 77–101 (2006)
6. Bruck, P.A., Motiwalla, L., Foerster, F.: Mobile learning with micro-content: A framework and evaluation. Bled eConference **25**, 527–543 (2012)
7. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly **34**(3), 523–548 (2010)
8. Desman, M.B.: The ten commandments of information security awareness training. Inf. Secur. J. A Glob. Perspect. **11**(6), 39–44 (2003)
9. Dropbox: Low-budget password strength estimation. https://github.com/dropbox/zxcvbn, accessed: 2019-10-07
10. Hedin, A.: Lärande på hög nivå. Uppsala universitet (2006)
11. Joinson, A., van Steen, T.: Human aspects of cyber security: Behaviour or culture change? Cyber Security: A Peer-Reviewed Journal **1**(4), 351–360 (2018)
12. Kävrestad, J.: Defining, categorizing and defending against online fraud (2014)
13. Kävrestad, J.: Using contextbased microtraining to enforce secure behavior among computer users. In: 19th Seminar within the Framework of a Swedish IT Security Network for PhD students, 3-4 June 2019, Karlstad (2019)
14. Kävrestad, J., Eriksson, F., Nohlberg, M.: Understanding passwords–a taxonomy of password creation strategies. Information & Computer Security (2019)
15. Kävrestad, J., Lennartsson, M., Birath, M., Nohlberg, M.: Constructing secure and memorable passwords. Information & Computer Security (2020)
16. Kävrestad, J., Marcus, N.: Online fraud defence by context based micro training. In: Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), Lesvos, Greece, 1 July 2015 through 3 July 2015. pp. 256–264. University of Plymouth Press (2015)
17. Kävrestad, J., Nohlberg, M.: Using context based micro training to develop oer for the benefit of all. In: Proceedings of the 15th International Symposium on Open Collaboration. pp. 1–10 (2019)
18. Kävrestad, J., Skärgård, M., Nohlberg, M.: Users perception of using cbmt for informationsecurity training. In: Human Aspects of Information Security & Assurance (HAISA 2019) International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019), Nicosia, Cyprus, July 15-17, 201 (2019)

19. Kim, E.B.: Recommendations for information security awareness training for college students. Information Management & Computer Security (2014)
20. Knowles, M.: Andragogy in action: applying modern principles of adult learning (1984)
21. Lincoln, Y.S., Guba, E.G.: Naturalistic inquiry (1985)
22. Marinos, L., Belmonte, A., Rekleitis, E.: Threat landscape 2013 (2013)
23. Payne, B.D., Edwards, W.K.: A brief introduction to usable security. IEEE Internet Computing **12**(3), 13–21 (2008)
24. Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: an action research study. MIS quarterly pp. 757–778 (2010)
25. Safa, N.S., Von Solms, R.: An information security knowledge sharing model in organizations. Computers in Human Behavior **57**, 442–451 (2016)
26. Wang, M., Xiao, J., Chen, Y., Min, W.: Mobile learning design: The ltcs model. In: 2014 International Conference on Intelligent Environments. pp. 318–325. IEEE (2014)
27. Wheeler, D.L.: zxcvbn: Low-budget password strength estimation. In: 25th {USENIX} Security Symposium ({USENIX} Security 16). pp. 157–173 (2016)
28. Whitten, A., Tygar, J.D.: Why johnny can't encrypt: A usability evaluation of pgp 5.0. In: USENIX Security Symposium. vol. 348, pp. 169–184 (1999)
29. Woo, S.S., Mirkovic, J.: Guidedpass: Helping users to create strong and memorable passwords. In: International Symposium on Research in Attacks, Intrusions, and Defenses. pp. 250–270. Springer (2018)