Users perception of using CBMT for information security training

J. Kävrestad, M. Skärgård and M. Nohlberg

School of Informatics, University of Skövde, Skövde, Sweden
e-mail: {joakim.kavrestad; marcus.nohlberg}@his.se

Abstract

It is well established that user behavior is a crucial aspect of information security and archiving secure behavior through awareness and security training is the go-to solution proposed by practitioners as well as the research community. Thus, there is a dire need for efficient training methods for use in the security domain. This paper introduces ContextBased MicroTraining (CBMT), a framework for information security training that dictated that information security training should be delivered to end users in short-sequences when the users are in a situation where the training is needed. Further, the users' perception of CBMT in evaluated in an online survey where about 200 respondents are subjected to training material and asked about how they perceived them. The results show that users like the training material designed according to the CBMT framework and would prefer to use CBMT over other traditional methods of information security training.

Keywords

Information security, training, learning, user behavior, micro training, ContextBased MicroTraining, CBMT

1 Introduction

It is well established that almost any organization is supported by IT and that securing IT systems is a critical component of those organizations. While there is a multitude of technical security controls available on the market, research, as well as the practitioner community, agrees that user behavior is a key aspect of information security (Bulgurcu, Cavusoglu, & Benbasat, 2010; Safa & Von Solms, 2016). While users are commonly referred to as the weak link in security, measures have to be taken to enforce secure user behavior. As discussed by Desman (2003), it comes down to making users understand the consequences of insecure behavior and learn the users to behave in a secure way.

As described by Puhakainen and Siponen (2010), literature often suggests training as a method for encouraging secure behavior, yet there is a need for training methods that are theory-based and empirically evaluated. The goal of any training intervention would be to make users behave in a secure way. On that topic, Parsons (2018), suggest that training should not only be about making the user know how to behave but also stop and think before they behave.

In this paper, ContextBased MicroTraining (CBMT) is presented, a framework for training users to behave securely. CBMT aims to deliver information security training in short sequences and is in that sense similar to, for instance, nano learning. However, CBMT also stipulates that training should be delivered to users in the situation that it is of direct relevance. Thus, the training should be perceived as more relevant and bring a reminding effect. Further, we evaluated how CBMT is perceived by users using a survey where the subjects are presented to three CBMT modules and asked a series of questions about how they perceived using CBMT in relation to other methods of training.

The precise aim of this study is to see if a random selection of Internet users appreciates using material created according to the CBMT framework for information security training. The study is intended to be used as a pilot to prepare for a larger, more practical project.

The remainder of the paper will present the CBMT framework and then describe the research approach used in this paper and the results of the study.

2 ContextBased MicroTraining

The CBMT framework is based on the fundamental belief that people need motivation in order to learn. The idea here is that the likelihood that any adult will learn is increased if the knowledge seems meaningful for the learner (Hedin, 2006). This notion is based on the concept of andragogy, as presented by Knowles (1984). Knowles (1984) argues that adults need motivation in order 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 the knowledge in a context where it is applicable. As discussed by Herrington and Oliver (1995), 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.

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 the past years is microlearning or similar strategies, including nanolearning and micro-training. As described by Wang, Xiao, Chen, and Min (2014), 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 (McLoughlin & Lee, 2008). As described by Bruck, Motiwalla, and Foerster (2012), 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 ContextBased MicroTraining.

On a practical note, 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 user's current context. In this respect, CBMT tries to facilitate the concept of "learn by doing" theories that can be summarized as a describing that learners learn better when they perform tasks instead of just reading (Koedinger, Kim, Jia, McLaughlin, & Bier, 2015). 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 (Boud & Feletti, 2013). In summary, the meaningfulness is achieved by the learner doing some task related to his or her situation.

Given the discussion in the previous sections, CBMT is a teaching method where information is provided in small segments to the learner. Further, the information presented is relevant to the learner in his or her current situation. A simple way of modelling CBMT is provided in Figure 1.

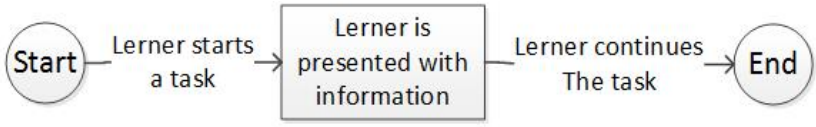

Figure 1: conceptual model of CBMT

Looking at the abstract model in Figure 1, CBMT begins with a learner entering a situation or starting a task. For the sake of this description, that situation can be that the learner opens an e-mail containing a link. Based on this situation, the learner is presented to a learning module with relevant information relating to the current situation. In this example, it could be information telling the learner not to enter account information into links sent via e-mail or to verify that the e-mail address of the sender matches the source that the e-mail appears to be from. The learner is then supposed to carry on with the task, in this case reading and reacting to the e-mail. As such, CBMT is a process where the central concept is that the information presented is relevant for the situation that the learner is in. The format that the information that is presented in is not specified in detail by CBMT but should comply with the ideas of nanolearning, namely facilitate just-in-time learning while the learner can maintain interest in the information.

As for the actual implementation of CBMT, there are two distinct ways in which it can be done. In the context of teaching computer users about information security, it would seem feasible to have a software monitor what is happening on the user's computer and present the learning modules whenever the users enter a situation or perform an action where he or she needs the information. In this case, the computer would decide when the user is entering a context where the information is applicable. The implementation of CBMT in such a scenario is modeled in Figure 2.

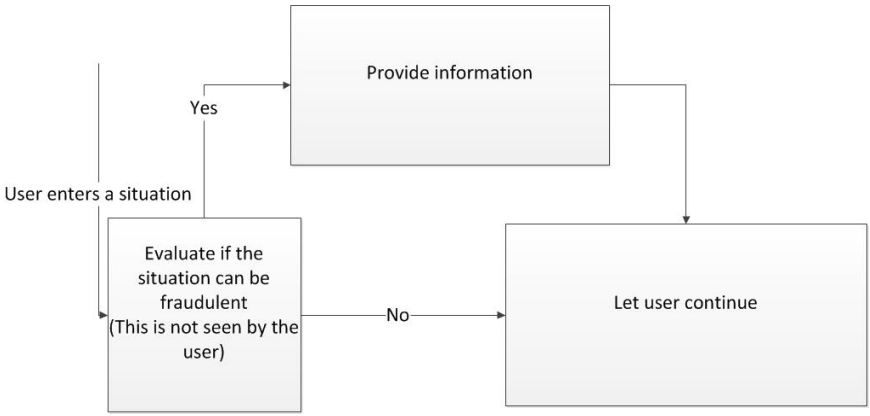

Figure 2: CBMT used to combat online fraud

The case in Figure 2 assumes that CBMT is used to combat online fraud. In this scenario, a computer would evaluate when to detect that a user enters a situation than the user is at risk of meeting a fraudster. If so, the computer will present information to the user so that she can handle the situation.

As described by Kävrestad and Nohlberg (2015), CBMT has been evaluated as a way to teach Internet users about online fraud schemes with positive results. The method was further explored in the same context by Werme (2014) with similar results.

To summarize, CBMT is a learning method where short sequences of information are presented to the learner in a context where it is of direct relevance to the learner. The teaching method is similar to nanolearning. As described by Wang et al. (2014), nanolearning is a teaching method where information is presented in short sequences. The difference between nanolearning and CBMT is that CBMT also presents the information in a context where it is of relevance to the learner. Another difference is that CBMT in itself encourages the learner to immediately use the information presented to her. Thus, CBMT encourages retrieval of information, an important factor in learning (Karpicke & Roediger, 2008).

3 Methodology

This study was conducted using an online survey with Likert-style questions written in Swedish. The survey was preceded with three learning modules, designed according to the CBMT framework and delivered as online videos publicly available on YouTube[1]. A picture demonstrating how the material was presented, in a video about creating strong passwords, is presented in Figure 3, below. All learning modules was

[1] All the videos can be found here:
https://www.youtube.com/channel/UC4gDh8JF8S0z7rjaKPu0ovg

under 60 seconds in length and contained practical elements asking the user to perform some action. The learning modules were designed to teach the participants:

- How to create strong passwords
- Detect phishing emails
- Avoid ransomware

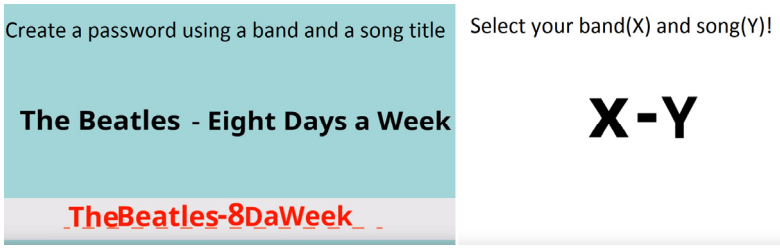

Figure 3: Picture demonstrating one of the learning modules (Translated from Swedish)

Following the learning modules, the participants were asked questions divided into three groups:

- Demographic questions
- Questions about the specific learning modules
- Questions about CBMT in general and compared to other teaching methods.

All questions were designed as Likert-style questions where the participants were asked to rate how well they agreed to a statement. They had the following answer options:

- Fully agree
- Mostly agree
- Partially agree
- Agree to some extent
- Do not agree

In analyzing the responses, all answers were dichotomized. The answers “Fully agree” and “Mostly Agree” was converted to 1 and the other options to 0. Thus, 1 represent an agreeing answer. The dichotomized variables were used to created indexes reflecting how the participants experienced the learning modules and how they perceived CBMT in relation to other types of training.

The results of the survey will be presented using the mean values of the indexes. Further, one-sample T-test will be used to calculate a 95% confidence interval and test if the results are significantly separated from 2. 2 is used since it is half of the possible max value. Further, as described by Siponen (2001), it is reasonable to assume that training will be perceived differently between professional computers users and other

users. Thus, mean values grouped by the respondents reported computer skills will also be presented and independent sample T-test used to analyze the difference in means between those groups.

4 Results

The survey was distributed via social networks, and 198 respondents completed the survey. The answers were used to compute and analyze indexes that describe how the participants perceived the learning modules used in this study, and CBMT in general. Before answering the questions, the respondents were asked to use three learning modules designed according to the CBMT framework. They were presented to the respondents as videos and covered the following content:

- How to create strong passwords (V1)
- How to avoid phishing (V2)
- How to avoid ransomware (V3)

The remainder of this chapter will describe how the indexes were calculated, and their results.

4.1 The learning modules

The participants were asked to use three learning modules designed according to the CBMT framework. They were then asked to rate the following statements about the videos (X being the particular video):

- I find that the content about X was clearly presented.
- I find that the content about X was useful
- I find that I learned something from the video about X
- If I had seen the video in a situation related to X it would have affected my actions.

The answers to the questions were dichotomized so that the two most positive answer options were represented by 1 and the three least positive answers were represented by 0. An index of all questions was computed by adding the variables together. To exemplify, if a respondent provided positive answers to all four questions, the index value became 4, if a respondent provided positive answers to two of the questions, the index value became 2. The results are presented for the entire sample and grouped by the respondent answer to the question about whether or not she considers herself a professional computer user. The results are presented in Table 1.

As seen in table 1, the mean values for the entire sample were above 2 for all videos. This means that the average participant provided more than 2 positive responses for each video. A one-sample T-test, using 2 as test value, was used over the entire sample and showed that the mean value in the population is above two, with a 95% confidence level. The literature suggests that information security training can be perceived differently between professional computer users and regular users. Thus, the index

values grouped on this variable is also shown in Table 1. The difference in mean was tested using an independent sample T-test that shows that there is a significant difference between those groups. In summary, the analysis of how the participants perceived the learning modules suggest that the participants did perceive them as good and useful, and that non-professional computer users were more positive than professional computer users.

Video	Index Mean N=198	T-test (2)	Confidence interval	Mean Unprof. N=86	Mean Prof. N=103	T-test	Confidence interval of the difference
V1	2.7	0.000	2.53-2.86	2.9	2.5	0.025	0.05-0.70
V2	2.5	0.000	2.35-2.70	2.7	2.0	0.023	0.06-0.75
V3	2.2	0.013	2.05-2.43	2.5	2.3	0.004	0.18-0.93

Table 1: Statistics for indexes over videos. 95% confidence level is used in all tests, p=0.05.

4.2 CBMT in general

Following the questions about the individual learning modules, the participants were asked the following four questions about CBMT in general:

- I would like to see more videos like this
- I would like to have access to videos like this when I perform tasks that could include security risks
- I think that the videos are well-suited to teach me information security
- I liked the videos

An index reflecting the respondent's answers to the questions was calculated in the same way as for the video-related questions. The statistics are presented in Table 2, below.

Index Mean N=198	T-test (2)	Confidence interval	Mean Unprof. N=86	Mean Prof. N=103	T-test	Confidence interval of the difference
2.7	0.000	2.48-2.84	2.9	2.4	0.017	0.08-0.82

Table 2: Statistics for indexes over CBMT in general. 95% confidence level is used in all tests, p=0.05.

As seen in Table 2, the confidence interval for the entire sample was 2.48 to 2.84 showing that the mean for the sample was positive to more than two of the statements. Again, non-professional users were more positive than professional users. In summary, the respondents are positive to CBMT in general, and non-professional users are more positive than professional users.

4.3 CBMT compared to other methods of training

The survey ended with the following question about CBMT compared to other methods of training:

- I prefer this type of training over classroom-training
- I prefer this type of training over written text about information security
- I prefer this type of training above longer videos online

Again, an index of the respondents' answer was calculated. The statistics are presented in Table 3. Note that this index only contains three items, thus the max value is 3.

Index Mean N=198	T-test (2)	Confidence interval	Mean Unprof. N=86	Mean Prof N=103	T-test	Confidence interval of the difference
2.2	0.023	2.02-2,3	2.3	2.0	0.141	-0.08-0.82

Table 3: Statistics for index over CBMT compared to other methods of training. 95% confidence level is used in all tests, p=0.05.

The results presented in Table 3 shows that the mean value of the entire sample is above 2, meaning that the respondents prefer CBMT over other types of training to a large extent. In this case there is no significant difference between non-professional and professional computer users.

5 Discussion

The aim of this paper was to analyze how the teaching framework CBMT was perceived by computer users as a method of information security training. A second aim was to investigate if CBMT was perceived differently between processional computer users and regular computer users. The evaluation was carried out by means of an online survey where respondents were asked to complete three learning modules before filling out a form with questions about how they perceived the particular learning modules, CBMT in general and if the preferred CBMT over other means of training.

The analysis was done using an index that reflected how many positive responses the respondents gave to each group of questions. The analysis of the survey data suggests that the respondents were positive to the learning modules and that they appreciated using CBMT in general. In numbers, the mean values for the entire population were above 2 positive responses out of 4 for each video and for CBMT in general. Further, the comparison of professional and non-professional computer users showed that non-professional computers users were more positive than professional computers users.

The final part of the survey analyzed if the respondents preferred CBMT over other typed of information security training. In this case, the mean values for the entire population were above 2 positive responses out of 3. This suggests that CBMT is a method of training that is preferred over others, by the users.

In conclusion, this study suggests that CBMT is a training method that is appreciated by the users, and that is preferred above other methods of training. The study also suggests that CBMT is more appreciated among users that are nonprofessional computers users. As such, the results do motivate further research into the actual effects of CBMT, especially compared to other methods of information security training.

An important note to make is that this study measured how CBMT is appreciated by users. The study is not concerned with the actual results of the different training methods. While one can argue that it is important for a training method to be appreciated by its users, one planned direction for further research is to actually use CBMT as a method of information security training in a real-world setting for which this was a pilot study. It should also be mentioned that this study was completed in a laboratory environment rather than in a real-world setting. Thus, another direction for future work would be to repeat this study in a real-world case with a larger sample. A future study should also look into differences among demographic groups, a factor that was not considered in this pilot study.

6 References

Boud, D., & Feletti, G. (2013). *The challenge of problem-based learning*: Routledge.

Bruck, P. A., Motiwalla, L., & Foerster, F. (2012). Mobile Learning with Micro-content: A Framework and Evaluation. *Bled eConference, 25*.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34*(3), 523-548.

Desman, M. B. (2003). The ten commandments of information security awareness training. *Information Systems Security, 11*(6), 39-44.

Hedin, A. (2006). Lärande på hög nivå. *Uppsala universitet*.

Herrington, J., & Oliver, R. (1995). Critical characteristics of situated learning: Implications for the instructional design of multimedia.

Karpicke, J. D., & Roediger, H. L. (2008). The critical importance of retrieval for learning. *science, 319*(5865), 966-968.

Knowles, M. S. (1984). Andragogy in action: Applying principles of adult learning. *San Farancisco: Jossey-Bass*.

Koedinger, K. R., Kim, J., Jia, J. Z., McLaughlin, E. A., & Bier, N. L. (2015). *Learning is not a spectator sport: Doing is better than watching for learning from a MOOC.* Paper presented at the Proceedings of the second (2015) ACM conference on learning@ scale.

Kävrestad, J., & Nohlberg, M. (2015). *Online Fraud Defence by Context Based Micro Training.* Paper presented at the HAISA.

McLoughlin, C., & Lee, M. (2008). Mapping the digital terrain: New media and social software as catalysts for pedagogical change. *Ascilite Melbourne*.

Parsons, K., Butavicius, M., Lillie, M., Calic, D., McCormac, A., & Pattinson, M. (2018). *Which individual, cultural, organisational and inerventional factors explain phishing resilience?.* . Paper presented at the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018) Dundee, Scotland, UK: University of Plymouth.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, 757-778.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451.

Siponen, M. T. (2001). Five dimensions of information security awareness. *SIGCAS Computers and Society, 31*(2), 24-29.

Wang, M., Xiao, J., Chen, Y., & Min, W. (2014). *Mobile learning design: The LTCS model.* Paper presented at the Intelligent Environments (IE), 2014 International Conference on.

Werme, J. (2014). Security awareness through micro-training: An initial evaluation of a context based micro-training framework. In.