# Can Johnny actually like security training?

Joakim Kävrestad[a], Evelina Friman[a], Joacim Bohlander[a] and Marcus Nohlberg[a]

[a]University of Skövde, Högskolevägen 1, 541 28 Skövde, Sweden

**Abstract**

Information security is a socio technical domain where a lot of traditional efforts has been placed in the technical domain where security has been considered technical and the solutions has been technical. However, it is well know that human behavior plays a key role in information security and the user is often seen as the weakest link in the security chain. As such, information security is a socio-technical property where the social, or human, side needs increased attention. Security training is commonly suggested as the way to improve user behavior but the effects of various training efforts is also underresearshed. This paper demonstrates how ContextBased MicroTraining (CBMT), a method for information security training, which has been developed over years of researched can be implemented and performs a usability evaluation of that implementation. The paper demonstrates that the CBMT method can aid in development of highly usable security training. The paper also emphasizes the need for user centered design in development of security software intended for end-users.

**Keywords**

CBMT, ContextBased MicroTraining, Usability, Usable security, Security training

## 1. Introduction

Usability and user-centred design of software is a key aspect of modern software development. Users seems to be more likely to use software designed to be highly usable, and that is a truism that hardly surprises anyone. Nevertheless, security functions that are developed to provide users with an added layer of security often fall short in the usability department [1]. A challenge when it comes to security software is that an organisation will strive for an adoption rate of 100% amongst its users so that no single user can be a weakness in the cybesecurity of that organisation. As such, usability testing of security features that are supposed to be adopted by every single user is integral [2].

Information security is, by its nature, socio-technical [3] and proper security work must consider social as well as technical aspects of security [4]. [5] describes that Social-Technical Systems Design (STSD) considers human, social, organizational and technical factors and this is comparable to how information security is commonly described. Our paper presents a usability evaluation of the method ContextBased MicroTraining (CBMT), presented in [6], which provide guidelines for how useful information security training can be performed. CBMT stipulates that information security training should be delivered to users when they encounter a situation where the training is of direct relevance. As such, it requires one component able of detecting such situations and one component that provides the user with training with the goal of improving the users security behaviour, making CBMT socio-technical in nature.

The goal of the paper is to demonstrate how information security training can be performed according to the CBMT method and to assess how the method support development of usable information security training. The focus of this paper is on usability and thus, the social part of STSD. The paper

*6th International Workshop on Socio-Technical Perspective in IS development (STPIS'20), June 08–09, 2020, Online*

EMAIL: joakim.kavrestad@his.se (J. Kävrestad); marcus.nohlberg@his.se (M. Nohlberg)

ORCID: 0000-0003-2084-9119 (J. Kävrestad); 0000-0001-5962-9995 (M. Nohlberg)

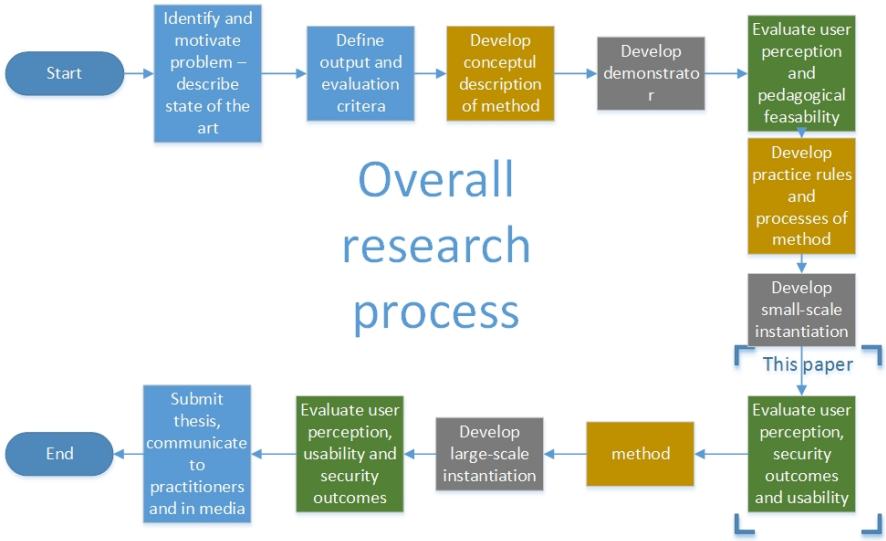


**Figure 1:** Research overview

is structured as follows; Section 2 introduces CBMT and briefly presents the ongoing research effort around CBMT. Section 3 outlines the methodology used in this paper, Section 4 describes the usability analysis performed and section 5 relates the usability analysis to the CBMT method. The paper is concluded in section 6 with a discussion on the papers contributions and directions for future work.

## 2. Description of CBMT and its development

ContextBased MicroTraining (CBMT) is a method for end user training developed for information security and awareness training. This paper makes one part of an ongoing design science effort. The full research process is based on [7], [8] and[9] and described in Figure 1, below. This paper is connected to the evaluation phase of the second design cycle, as denoted in Figure 1. The previous steps in the research is presented in [6].

CBMT is a method that provides goals and guidelines for implementation of information security training. It is described as follow [6]s:

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

The CBMT method is based on the notion that users need motivation to learn [10] and that they learn better if learning is combined with a practical element [11]. CBMT also stipulates that training should be delivered in a situation where it is of direct relevance to the user, i.e. password training should be provided to the user when the user is about to create a password, and in short sequences. This approach is assumed to increase the likelihood that the user makes use of the provided information and provides a awareness increasing mechanism comparable to security nudges.

CBMT requires a technical element that is able to detect situations where a user needs training and an element containing the training itself. The training is intended to improve the users security behaviour, and ultimately increase organizational security culture, making CBMT an example of a socio-technical system as described by [5]. This paper aims at evaluating the social side of CBMT by performing a usability analysis of an implementation of CBMT and connecting the results of that to the theoretical method.

## 3. Methodology

This study is a multi-disciplinary effort with researchers in information security working with User Experience Designer(UXD) experts. The UXD experts performed a usability test of an implementation of CBMT, hereafter refereed to as the implementation. The implementation was a software that provided users of a web-site with training on how to create good passwords. It was activated, and appeared as a pop-up, once a user clicked in the "Create Password" field of an account registration form[1] and is demonstrated in Figure 2, below. The security researchers analysed the results of the usability test in regards to the CBMT method.

Due to the CoVid-19 situation that affected the world during 2020, a user participatory usability study was deemed hard to complete. Instead, the usability analysis was performed as an "individual expert review" as described by [12]. The "individual expert review" entails that the experts evaluate the target software in order to find problem areas that can decrease the users experience of the software and thus hinder user adoption och correct use. The evaluation includes the experts using the software and assessing the various steps in the software in great detail. Two UXD experts without previous knowledge of the implementation or the underlying CBMT theories evaluated the implementation individually and then combining their results. Having individual experts performing the evaluation independently and then combine their results increase the validity of the results [13]. The

[1]The implementation is demonstrated at :https://rr222cy.github.io/SecurityAssistantWidget/

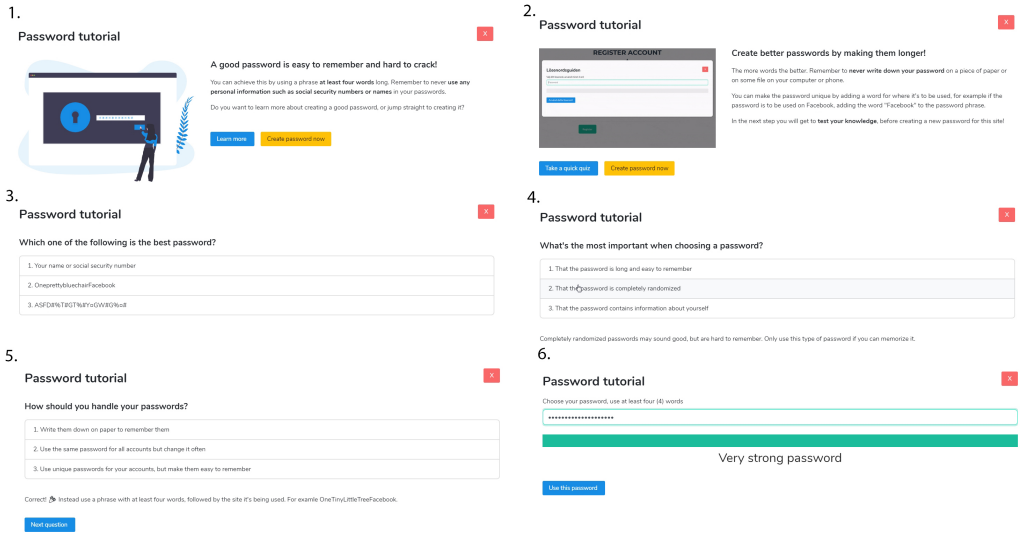


**Figure 2:** Implementation of CBMT

analysis identified problem areas that were categorised according to [14] approach for categorization of problem areas and ranked based on severity. The analysis was then complemented by a one participant usability analysis, as suggested by [12], that analyzed the following requirements:

- *The software should be highly learnable* meaning that the user should easily understand the purpose of the software and how to use it
- *The presented text should be understandable to the user* meaning that the user should understand all information presented while using the software
- *The user should learn something about password creation after using the software*

Taking the usability analysis outcomes as input, thematic coding, as described by [15] was used to identify information relating to the theoretical CBMT method and the identified information was summarised as the result of this study. Information considering the particular implementation rather than the CBMT method was disregarded in this study since it does not impact the theoretical foundation of CBMT.

## 4. Usability analysis

This section describes the steps in the performed usability analysis.

### 4.1. Expert analysis

The implementation was analyzed by two UXD experts using the expert analysis method described by [12]. To increase validity, the two experts performed the analysis individually and then compared their results. The analysis revealed the following 22 problem areas:

1. The implementation presents a pop-up that cant be escaped and can be seen as interrupting the users workflow
2. The "Create password now" button disappears it the user closes the implementation rendering the user unable to create a password at all
3. The implementation is not expected by the user and forces the user into a workflow the user did not expect
4. An option to navigate backwards is missing
5. The implementation cannot be closed by clicking outside of the implementation window
6. The user does not get visual feedback when selecting an answer in the Quiz-part of the implementation
7. The implementation contains emojis that are displayed in different ways in different browsers
8. The ending "Use this password" button works even if the user did not type any password
9. The user is not made aware of the length of the quiz
10. The graphic included in the implementation does not match the actual implementation
11. The password typed by the user is censored and the censorship cannot be removed
12. The quiz do not provide feedback on correct answers
13. The implementation could include examples on "approved" passwords
14. The implementation could include, or link to, more information about the risks with bad passwords
15. Some buttons appear to be far from text elements
16. The "Create you password" button is blue while other buttons with similar purpose are yellow
17. The last sentence on the "Create better passwords by making them longer" is confusing
18. The button used to move forwards from the last quiz question says "Next question"
19. Spelling error in question 3
20. The graphic is oddly cropped
21. The strength meter on the "Create password" page could be clarified with levels
22. The module cannot recognize if a user follows of disregards the presented guidelines

The identified issues was further classified based on severity as suggested by [14]. Issue 1-3 was classified as catastrophic, 4-11 were classified as severe, 12 - 18 were classified as smaller issues and 19 - 22 was considered cosmetic.

### 4.2. Usability test

The expert review was followed by a usability test with one participant. The participants was not a IT professional but considered himself to be a skilled computer user with general knowledge about security practices. He did, for instance, claim to posses knowledge about how to create strong passwords before the test started. The usability test was used to validate the results of the expert analysis and assess the implementation in regards to the following established requirements:

- The software should be highly learnable
- The presented text should be understandable to the user
- The user should learn something about password creation after using the software

The usability test suggest that the software fulfills the analyzed requirements. Another insight from the usability test was that the participant, when asked to create an account using a standard account creation form, was surprised by the appearance of the implementation. The participant also expressed concerns about the quiz part of the implementation similar to the problems discovered by the expert review. The participant did, however, not express any concerns with the software itself, nor did the participant express any problems understanding the information presented by the implementation. To summarize, the usability analysis suggests that the implantation fulfilled the requirements established for the usability test. Further, it validates the expert review since several problem areas was identified by the participants, and one was contradicted.

## 5. Analysis of usability analysis in relation to the CBMT method

To relate the usability analysis to the CBMT method, the results of the usability analysis was analyzed using thematic coding. The results was classified as related to the CBMT method or related to the implementation itself. The Following bullets was considered to relate to the CBMT method:

- The implementation presents a pop-up that cant be escaped and can be seen as interrupting the users workflow (From the expert analysis and the usability test)
- The implementation is not expected by the user and forces the user into a workflow the user did not expect (From the expert analysis and the usability test)
- The implementation is easy to use and provides useful information (from the usability test)

The first two bullets suggests that a usability hinder is the fact that CBMT states that the users workflow should be intercepted under certain conditions, namely when a security situation occurs. In this case, the user does not expect the implementation to be activated since he is not aware of it and it deviates from the standard behaviour of registration forms. The final bullet suggests that the user does find the implementation useful as tool for learning about security.

The CBMT method, as well as many other common security functions, must interrupt the users workflow in order to provide its intended function. As the usability analysis highlight this as a problem it shows that developers of interrupting security functions must take special care to make those functions as user friendly as possible. The CBMT method attempts to do this by suggesting that the information presented to users should be in a short and easy-to-digest format. A conundrum that should require further research it that previous research has shown that being interuptive can improve security behaviour to the better[16], but this analysis suggests that it hinders usability. A question raised is inevitably how security behaviour can be increased with minimal negative impact on usability, and what level of interruption that is optimal. that is, however, beyond the scope of this paper.

## 6. Conclusions

This paper described the CBMT method developed for information security training and positions it as a social-technical system that uses technical elements to identify situations where users need training and then provides training designed to improve the users security related behaviour. We argue that usability and user-centric design is a key factor in development of security software designed for end-users as it will increase the adoption rate and acceptance amongst end-users, a pre-requisite in order to achieve the security function the software is intended to provide.

This paper subjects an implementation of CBMT to rigorous usability analysis using an expert review method where the implementation is scrutinized by UXD experts. The expert review is complemented by a usability test with one participant and the results are related back to the CBMT method. The results of the study suggests that the CBMT method can support development of usable security training algorithms that provide users with easy-to-understand information and serves as a validation of the CBMT method. This notion aligns well with previous research reporting on user perception of CBMT-based training [17, 18]. The results contribute to increased knowledge around the human element of STSD related to information security. The paper also contribute to the practical community with a concrete demonstration of how information security training can be performed.

The main negative finding in the usability analysis is that the implementation was unexpected by the user and interrupted the users workflow. It is well known that security seldom is the users primary target making most security functions perceived as interruption the users workflow [19, 20, 21]. Nevertheless, security functions is a necessity in order to establish a healthy security behaviour. As such, this study emphasises the need to employ a user-centric approach to development of security functions in order to minimize annoyance to the greatest extent possible in order to maximize acceptance and adoption.

The usability analysis performed in this study relied on a methodology that did not require a large sample of participants. The methodology was chosen since the Covid-19 pandemic made participant based usability analysis hard to perform under social restrictions that applied world-wide during the spring of 2020. One could even argue that such a study could contribute to the spread of infection and thus, putting participants at risk in an unethical manner. Follow-up studies using a participant based methodology is an obvious direction for future work. Another direction for future work could focus on evaluation user perception and learning outcomes from using CBMT over en extended period of time.

## References


[1] L. Coles-Kemp, R. B. Jensen, C. P. Heath, Too much information: Questioning security in a post-digital society, in: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, pp. 1–14.

[2] A. Adams, M. A. Sasse, Users are not the enemy, Communications of the ACM 42 (1999) 40–46.

[3] B. Al Sabbagh, S. Kowalski, St(cs)2 - featuring socio-technical cyber security warning systems, in: Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012, pp. 312–316.

[4] E. Paja, F. Dalpiaz, P. Giorgini, Managing security requirements conflicts in socio-technical systems, in: W. Ng, V. C. Storey, J. C. Trujillo (Eds.), Conceptual Modeling, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 270–283.

[5] G. Baxter, I. Sommerville, Socio-technical systems: From design methods to systems engineering, Interacting with computers 23 (2011) 4–17.

[6] J. Kävrestad, M. Nohlberg, Contextbased microtraining: A framework for information security training, in: International Symposium on Human Aspects of Information Security and Assurance, Springer, 2020, pp. 71–81.

[7] A. R. Hevner, A three cycle view of design science research, Scandinavian journal of information systems 19 (2007) 4.

[8] K. Peffers, T. Tuunanen, M. A. Rothenberger, S. Chatterjee, A design science research method-

ology for information systems research, Journal of management information systems 24 (2007) 45–77.
[9] S. T. March, G. F. Smith, Design and natural science research on information technology, Decision support systems 15 (1995) 251–266.
[10] M. Knowles, Andragogy in action: applying modern principles of adult learning, 1984.
[11] A. Hedin, Lärande på hög nivå, Uppsala universitet (2006).
[12] C. Wilson, User interface inspection methods: a user-centered design method, Newnes, 2013.
[13] M. Hertzum, N. E. Jacobsen, R. Molich, Usability inspections by groups of specialists: perceived agreement in spite of disparate observations, in: CHI'02 extended abstracts on Human factors in computing systems, 2002, pp. 662–663.
[14] M. J. Kahn, A. Prail, Formal usability inspections, in: Usability inspection methods, 1994, pp. 141–171.
[15] V. Braun, V. Clarke, Using thematic analysis in psychology, Qualitative research in psychology 3 (2006) 77–101.
[16] K. Parsons, M. Butavicius, M. Lillie, D. Calic, A. McCormac, M. Pattinson, Which individual, cultural, organisational and interventional factors explain phishing resilience?, in: International Symposium on Human Aspects of Information Security Assurance (HAISA 2018), Dundee, Scotland, UK, August 29-31, 2018, 2018.
[17] J. Kävrestad, M. Skärgård, M. Nohlberg, 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.
[18] J. Kävrestad, 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, pp. 1–10.
[19] C. Braz, A. Seffah, D. M'Raihi, Designing a trade-off between usability and security: A metrics based-model, in: C. Baranauskas, P. Palanque, J. Abascal, S. D. J. Barbosa (Eds.), Human-Computer Interaction – INTERACT 2007, Springer Berlin Heidelberg, Berlin, Heidelberg, 2007, pp. 114–126.
[20] R. Kainda, I. Fléchais, A. W. Roscoe, Security and usability: Analysis and evaluation, in: 2010 International Conference on Availability, Reliability and Security, 2010, pp. 275–282.
[21] G. Dhillon, T. Oliveira, S. Susarapu, M. Caldeira, Deciding between information security and usability: Developing value based objectives, Computers in Human Behavior 61 (2016) 656–666.