Assisting Users to Create Stronger Passwords Using ContextBased MicroTraining

Joakim Kävrestad[†] and Marcus Nohlberg[†]

[†]School of Informatics, University of Skövde, Skövde, Sweden

Introduction

This poster presents our paper [2], in which we describe and evaluate ContextBased MicroTraining (CBMT). CBMT is a method for implementation of Security Education, Training, and Awareness (SETA) for end-users. This research intends to meet the need for effective means of assisting users to behave securely and thereby combat the problem of insecure user behavior.

ContextBased MicroTraining

CBMT is a method for SETA targeting end-users and has been developed through several years of research. CBMT stipulates that *training should be delivered in short sequences, in an accessible format, when needed.*

CBMT is expressed as goals that SETA should meet and guidelines for implementation of SETA[3]. The core functions of CBMT are [4]:
1. Identify when a user encounters a risky situation
2. Then present the user with training tailored to the specific situation
A conceptual overview of CBMT is shown below.
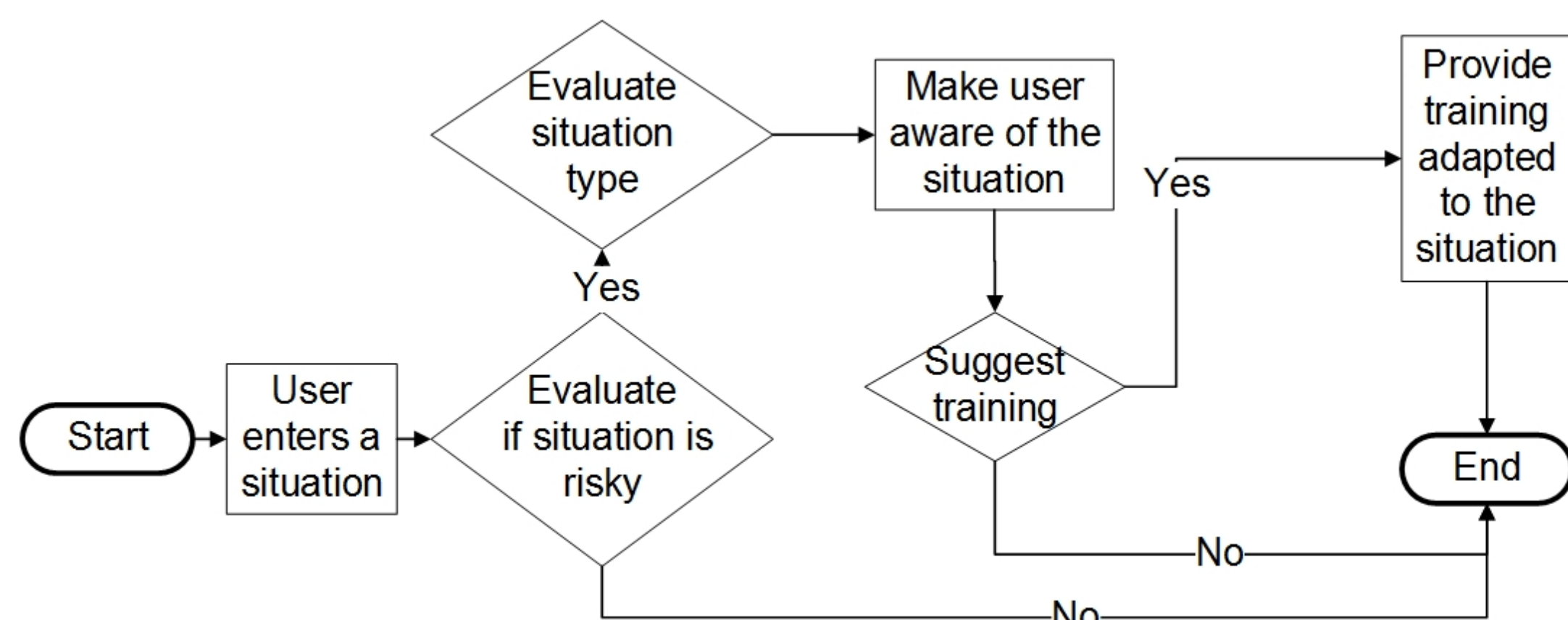
Methodology

This research evaluated the effects of using CBMT to teach password security tips (emphasizing long passwords [6]) to users of a website in two steps.

1. Participants were directed to a sign-up form where a CBMT based tool was present. Upon completing the form, the participants were given a quiz on what password tips were just presented to them.

2. The CBMT tool was deployed at the website of a local ISP and its effect on the password strength of newly registered users was evaluated.

Results

The first step measured how much of the training the participants took notice of. A quiz with five questions was used and the participants got one point per correct answer. A participant could get a score between zero and five. One control group received the same information as plain text next to the sign-up form while another received a link to the same text. As seen below, the CBMT group had the highest score and the difference between LINK and CBMT was statistically significant.
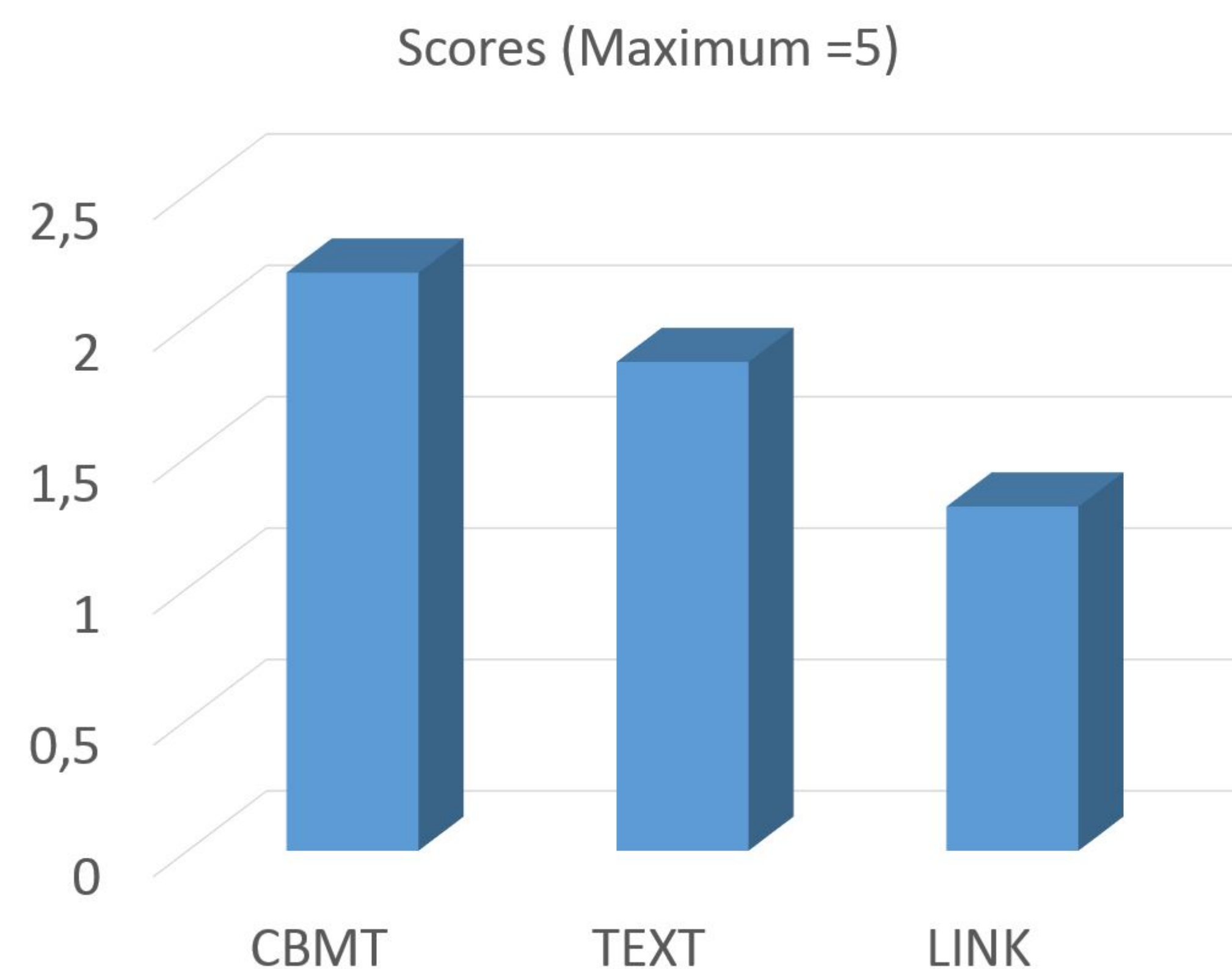
The second step measured the effect of the training when deployed on a live website. The password length and strength according to the zxcvn [1] measure were captured and compared to a control group. The results, shown below, show that the users using CBMT created longer and stronger passwords. the results were statistically significant.
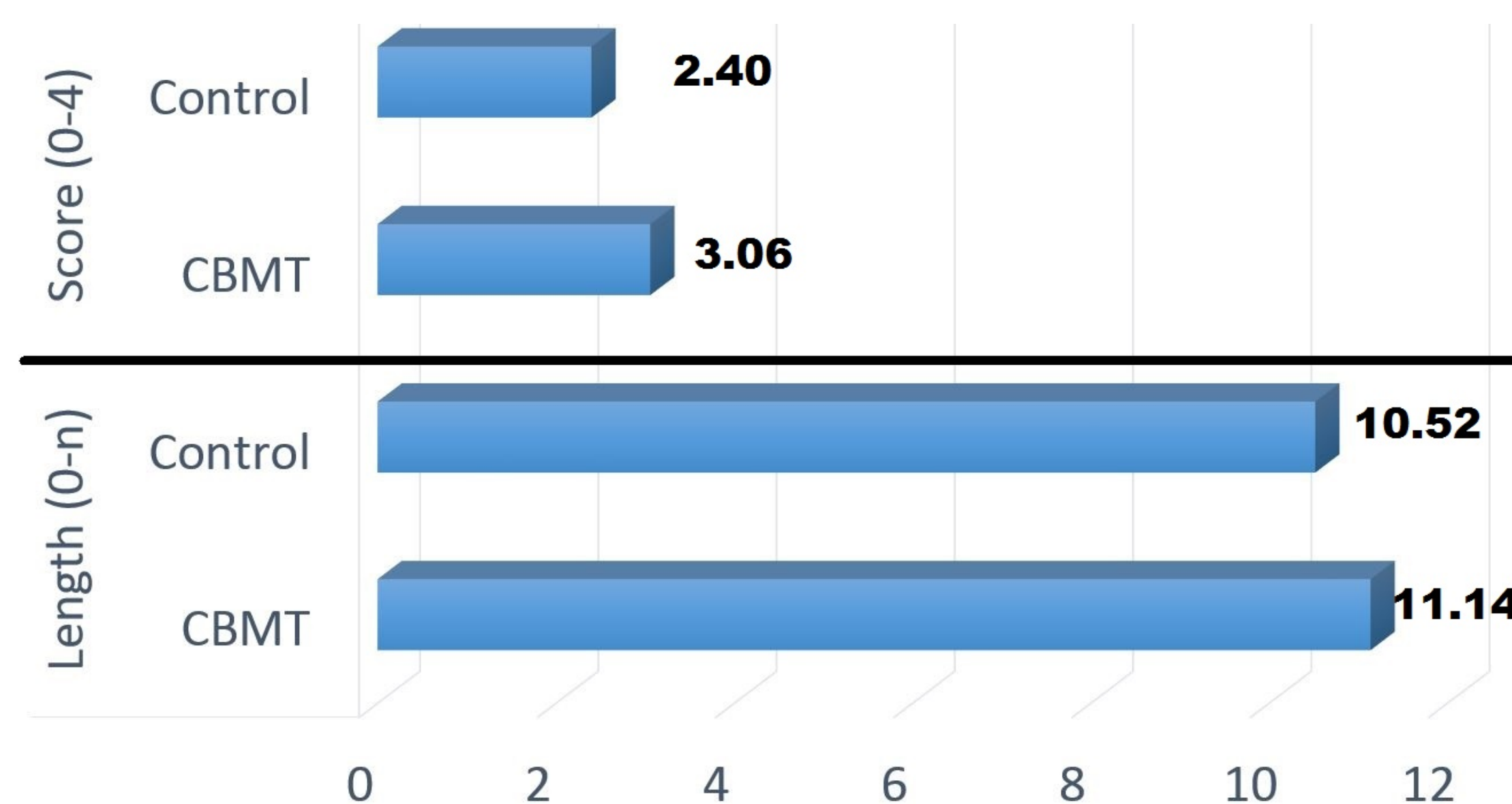
Conclusions

The study shows that users presented with password creation tips according to the CBMT method create longer and stronger passwords compared to users are not. Further, users presented with password creation tips using the CBMT method notice the tips to a greater extent than users presented with the same tips as plain text. As such, CBMT is a promising method for cybersecurity training of end-users and future research will evaluate CBMT in other security contexts. The password creation tips presented to users in this research emphasized length over complexity and were derived from our previous research into usable password guidelines [6].

Ending remarks

This research is ongoing and CBMT has also been evaluated for pedagogical use [4] and by how users perceive getting training according to it [5], with positive results. An ongoing project will develop a CBMT tool for phishing, fraud, and fake news training and test that specifically for users with cognitive disabilities. We welcome any comments and thought about this research, or our other research in this domain (as cited in this poster). Joakim Kävrestad is the head researcher on this project and can be contacted at joakim.kavrestad@his.se.

References

[1] Dropbox. *Low-Budget Password Strength Estimation.* https://github.com/dropbox/zxcvbn. Accessed: 2019-10-07.

[2] Joakim Kävrestad and Marcus Nohlberg. "Assisting Users to Create Stronger Passwords Using ContextBased MicroTraining". In: *IFIP International Conference on ICT Systems Security and Privacy Protection.* Springer. 2020, pp. 95–108.

[3] Joakim Kävrestad and Marcus 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.

[4] Joakim Kävrestad and Marcus 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.

[5] Joakim Kävrestad, Marie Skärgård, and Marcus 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.

[6] Joakim Kävrestad et al. "Constructing secure and memorable passwords". In: *Information & Computer Security* (2020).