Full Citation: Kävrestad J., Nohlberg M. (2020) Assisting Users to Create Stronger Passwords Using ContextBased MicroTraining. In: Hölbl M., Rannenberg K., Welzer T. (eds) ICT Systems Security and Privacy Protection. SEC 2020. IFIP Advances in Information and Communication Technology, vol 580. Springer, Cham. https://doi.org/10.1007/978-3-030-58201-2_7

Link to published paper: https://link.springer.com/chapter/10.1007/978-3-030-58201-2_7

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.