Title: Using ContextBased MicroTraining to enforce secure behavior among computer users.

Author: Joakim Kävrestad, School of Informatics, University of Skövde

Submission format: Poster

Abstract:

While there are many technical security controls available, the research- as well as the practitioner-community agrees that a key aspect of information security is user behavior(Bulgurcu, Cavusoglu, & Benbasat, 2010; Safa & Von Solms, 2016). It is also well established that users are usually a target somewhere in the attack chain in any intrusion attempt at a computer system or network. Thus, measures has to be taken to enforce secure user behavior. While technical controls are an important part of security, making users understand the consequences of insecure behavior and behave in a secure way is another key to good security. A common suggestion, in this regard, is training (Puhakainen & Siponen, 2010). On the topic of training, Parsons (2018) suggests that training should not only be about learning security, but also make users stop and think before they act.

In this presentation, ContextBased MicroTraining (CBMT), a framework for training users to behave securely and has been developed during several years is presented (Kävrestad & Nohlberg, 2015; Skärgård, 2017; Werme, 2014). CBMT aims to deliver information security training in short sequences and is in that regard similar to, for instance, nano learning. However, CBMT also stipulates that training should be delivered to users in a situation where it is of direct relevance. Thus, the training should be perceived as more relevant and bring a reminding effect. Following the presentation of CBMT, the poster will describe how CBMT has been evaluated so far and with what results. The poster will end with a discussion on future research directions and suggestions for practical implementations of CBMT.

References

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.

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

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.

Skärgård, M. (2017). Mikroträning som utbildningsmetod inom informationssäkerhet. In.

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