# Context-Based Micro-Training – a Method for cybersecurity training of end-users

Joakim Kävrestad, University of skövde

This research addresses the human aspect of cybersecurity by developing a method for cybersecurity training of end-users. The reason for addressing that area is that human behaviour is widely regarded as one of the most used attack vectors. Exploiting human behaviour through various social engineering techniques, password guessing, and more is a common practice for attackers. Some reports even suggest that human behaviour is exploited in 95% of all cybersecurity attacks.

Human behaviour with regard to cybersecurity has been long discussed in the research. It is commonly suggested that users need support to behave securely. Training is often suggested as the way to improve user behaviour, and there are several different training methods available. The available training methods include instructor-led training, game-based training, eLearning, etc. However, even with the diversity of existing training methods, the effectiveness of such training has been questioned by recent research. Research suggests that existing training does not facilitate knowledge retention and user participation to a high enough degree.

This research aims to address the problems with current training practices by developing a new method for cybersecurity training of end-users. The research used a design science approach to develop the new method in three increasingly complex design cycles. Principles for cybersecurity training were developed based on previous research and the technology acceptance model and made the theoretical foundation of the work. The result is a theoretically grounded method for cybersecurity training that outlines goals and guidelines for how such training should be implemented. It has been evaluated in several steps with more than 1800 survey participants and 300 participants in various experiments. The evaluations have shown that it can both support users towards secure behaviour and be appreciated by its users.

The main contribution of this research is the method for cybersecurity training, Context-Based Micro-Training (CBMT). CBMT is a theoretical contribution that describes good practices for cybersecurity training for end-users. Practitioners can adopt it as a guide on how to implement such training or to support procurement decisions. The research also shows the importance of integrating usability into the development of security practices. Users must positively receive both training and the guidelines imposed by training since positive user perception increases user adoption. Finally, the research shows that following security guidelines is difficult. While training is essential, this research suggests that training alone is not enough, and future research should consider the interplay between training and other support mechanisms.