

Tackling the Awareness-Behaviour Divide in Security: (step 1) Understand the User

Keynote Talk

Lynne Coventry

Psychology and Communication Technology, University of Northumbria, UK

Abstract. Various factors influence user's behaviour and interactions with technology. This means security has a socio-technical element, that continues to present a challenge in research and attempts to improve security behaviour. Users may not be the enemy but their (un)intentional (mis)use of technology is certainly part of the problem in security. To solve this problem, we must do more than simply pay lip service to the need to address the human element; we need to systematically explore the environmental, social and personal influencers of behaviour within the context of cybersecurity. Those who seek to ensure cybersecurity must learn to utilise such influencers as efficiently as those who seek to exploit them. Awareness training is touted as the solution, awareness may be necessary but it is seldom sufficient. Psychological research and organisational reports suggest that increased user awareness alone is insufficient when it comes to changing actual behaviour. This may make users' behaviours seem irrational, but they are understandable if you appreciate the cognitive biases people are prone to and the heuristics they use when the time, effort and knowledge required to follow a "rational" decision making process outweighs the benefits perceived by the user. This talk provides a short overview of the issues worthy of exploration in security research and suggests several strategies on how to tackle the security awareness - behaviour divide.