**Preparation of papers for Persona-centred Information Security Awareness** (EV\_Title)  
Duncan Ki-Aries, Shamal Faily (Authors of the paper)

Affiliation: Bournemouth University, Department of Computing & Informatics, UK (EV\_Kontakt)  
Email: dkiaries@bournemouth.ac.uk, sfaily@bournemouth.ac.uk

**Abstract**

Maintaining Information Security remains a critical concern for businesses, as human factors, whether accidental or malicious, are primary contributors to data breaches. This paper discusses an approach to address these issues by incorporating personas into information security awareness programs. Grounded in empirical data, personas can help identify security risks and tailor awareness activities to meet specific business needs. This study presents a 90-day cycle awareness program evaluated through a case study. Findings suggest that a persona-centred approach can adapt to business demands and mitigate security risks through tailored awareness initiatives.

**Keywords:** Information Security, Security Awareness, Human Factors, Personas, Risk

**1. Introduction (HEADING 1)**

In today’s digital age, Information Security is a vital concern for organisations, particularly where breaches can lead to regulatory and reputational consequences. As demonstrated in PwC’s 2015 Data Breach Report, many data security breaches are linked to human factors. These factors may stem from intentional, accidental, or malicious actions. Consequently, businesses can no longer depend solely on technology and processes but must integrate people effectively into their security strategies. Traditional methods, such as compliance-based security awareness, fail to consider the unique human factors involved in security risks, leading to a one-size-fits-all approach.

**2. Paper Submission Procedure**

**Steps for submitting a paper on Persona-centred Information Security Awareness**:  
• Submit your manuscript in PDF or DOCX format through the editorial system.  
• The review process will be managed by the editor, who will return feedback for revisions.  
• After acceptance, authors must update the manuscript and resubmit.  
• The editor will liaise with authors during the final formatting stage before publication.

**3.** **Methodology (HEADING 1)**

This paper outlines a persona-centred approach to enhancing Information Security awareness. Personas are constructed based on empirical data gathered from interviews with staff, enabling the identification of security risks tied to human behavior. These personas are then integrated into a 90-day awareness cycle tailored to business-specific security challenges.

**Subchapters:**

3.1 **Personas**  
The development of personas involves detailed interviews with staff to understand their behaviours, attitudes, and risks in the security context. These personas represent archetypes that embody user goals and security challenges. By analysing these user models, businesses can tailor security programs that address actual human risks.

3.2 **Design and Development**  
Tailored security content is designed based on the identified personas. This content includes interactive tools, games, and quizzes to promote engagement and a deeper understanding of security risks.

**4. Conclusion**

This paper highlights the effectiveness of using personas in information security awareness. Tailored approaches to security training are more likely to influence behaviour positively, reducing security risks through targeted awareness initiatives.

**References**  
[1] Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security, 70*, 663-674.  
[2] PricewaterhouseCoopers LLP. (2015). *Data breach report*.