

Introduction to the HICSS-59 Minitrack on Innovative Behavioral IS Security and Privacy Research

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

Karen Renaud
University of Strathclyde
karen.renaud@strath.ac.uk

Anthony Vance
Virginia Tech
anthony@vance.name

Allen C. Johnston
University of Alabama
acjohnston5@ua.edu

This minitrack provides a venue for innovative research that rigorously investigates the risks to information system security and privacy, with a specific focus on individual behaviors within this nomological net. Domains include work related to detecting, mitigating, and preventing both internal and external human threats to organizational security. Papers may include theory development, empirical studies (both quantitative and qualitative), case studies, and other high-quality research manuscripts, with a particular interest in emerging, rigorous research methods for investigating their phenomenon of interest.

This year's minitrack features one session, which focuses on **Tools, Behaviors and Fatigue** and includes three papers that will stimulate further discussion and exploration of the key phenomena within this domain.

The first paper titled "*Going the 'Extra' Mile: The Role of Sensemaking in Extra-Role Security Behaviors*" by Thurwat, Frank and Jaeger discusses the antecedents of extra-role security behaviors (ERSBs), discretionary, voluntary employee behaviors helping organizational information security beyond formal requirements. Applying sensemaking theory, the authors developed a process-based model tracing how individuals manage organizational ambiguity, decode cultural and emotional cues, and make sense of how to decide on performing ERSBs. The

study addresses an increasingly urgent challenge facing organizations in the evolving world of cybersecurity

The second paper, titled "*The Framing Effect in Privacy Management Tools*" by Al Natour, Cavusoglu, Benbesat and Aleem examines the application of Generative AI (GenAI) for phishing detection and user education. Drawing on phishing vulnerability research, feedback theory, and human decision-making theory, the authors speculate that GenAI-generated advice and explanations, when incorporated in warning emails, can improve both phishing detection accuracy and learning. The dual focus on current performance and long-term learning provides a sharp shift in security research, away from automation towards augmenting end-user decision-making.

The third paper is by Cram, D'Arcy and Benlian titled "*Now and Later? Comparing a Nomothetic and Idiographic Analysis of Cybersecurity Fatigue*." This paper examines the stability of cybersecurity fatigue mechanisms longitudinally by comparing cross-sectional (nomothetic) relationships with those of a three-wave longitudinal (idiographic) panel study. The article makes not only a methodological contribution to the literature, but also raises impactful theoretical issues about how perceptions and behavior associated with fatigue develop, or fail to develop, over time.