ABSTRACT

In today's digital era, the concept of transactions at your fingertips has revolutionized how we conduct financial transactions, allowing us to conduct them anywhere and anytime. Unfortunately, this is followed by inappropriate information security-related behaviors, such as using the same password for multiple accounts and assuming transactions with public WiFi are fully secure, etc. Inappropriate behaviors related to information security increase the risk of cybercrime. Therefore, this study aims to explore the factors that are relevant to fostering positive information security behaviors among mobile banking users in Indonesia. The constructs in this study consist of password management, infrastructure management, email management, security perception, and privacy concerns. Data collected from 197 respondents was derived from distributing online questionnaires and analyzed using Partial Least Squares-Structural Equation Modeling (PLS-SEM) techniques and descriptive analysis. This study reveals that security perceptions contribute the most to fostering positive information security behavior, followed by infrastructure management, privacy concerns, email management, and password management. Based on the descriptive analysis from the security perception section, mobile banking users should be more aware that using public WiFi for financial transactions is risky. On the other hand, in Indonesia, mobile banking users have shown a good indication of concern for the security of their devices, which needs to be maintained. This research can be a reference for service providers to educate their users and create regulations such as mandatory password changes. These can minimize the risk of cybercrime among mobile banking users.

Keywords*: email management, information security behavior, infrastructure management, mobile banking, password management, privacy concerns, security perception*