

A Qualitative Behavioural Study Exploring User Adoption of Security Measures in Malaysia for Mobile Devices

PRASAD KRISHNAPILLAI^{1*}, DEWI A. SAPUAN^{2*}

^{1,2} School of Business Administration, Wawasan Open University

*Corresponding Author: prasadk1970@gmail.com, dewisapuan@wou.edu.my

ABSTRACT

Cases of cybercrimes have gone rampant globally where significant losses have been reported as a result of personal information being stolen via mobile devices. In Malaysia, such data leaks have been monitored by the Royal Malaysia Police together with the Malaysian Communications and Multimedia Commission. In 2018, cybercrime cases contributed to losses amounting to almost RM400 million, and this amount increased to almost RM500 million in a span of a year. These statistics confirm that we have taken the safety and security of our integral mobile devices for granted. This study will explore how user behaviour can be changed in order to adopt security measures for one's mobile devices. It seeks to gain insights into understanding user perception of risks and their attitude toward potential risks in terms of security, breach of privacy and confidentiality. Previous studies on mobile users' adoption of security measures have largely been largely quantitative in nature, examining relationships between user behaviour and technology adoption, and its usage. Qualitative studies explaining mobile user behaviour, specifically, with regard to risk-taking is scarce. The objective of this research is to gain an understanding of user behaviour, and their lived experience in response to the grim cybercrime phenomenon. The research questions will revolve around the different ways users execute controls or take measures in ensuring the privacy and security of their information. In short, this study explores perceived behaviour and behavioural predictions using dimensions such as perceived benefits, behaviour motivation, and behavioural intentions adopted from theories such as the Protection Motivation Theory, and Unified Theory of Acceptance and Use of Technology 2. The qualitative research methodology approach is exploratory as it discusses the subject of security threats that people are generally aware of but uncertain about how to overcome. A survey questionnaire is designed based on behavioural intention constructs and will be disseminated to 100 mobile users in three main cities in West Malaysia, namely, Johor Bahru, Kuala Lumpur, and Penang. These three cities have been identified because the population is dense, hence have a higher number of mobile device subscribers compared to other cities in the country. The descriptive quantitative findings will then be used to inform the design of semi-structured interview questions for in-depth interviews and well focus group interviews. The initial data collection phase will consist of three focus group sessions with five respondents per group, all of the different demographic backgrounds from the three cities. This initial data collection phase will then be followed by in-depth interviews with six key respondents holding strategic level positions in regulatory bodies and service provider organizations. More of such key informants will be sourced through a snowballing technique if required to reach saturation. Findings from the various sources are then triangulated for sense-making to solicit insights that could pinpoint how mobile owners can be coaxed into taking greater responsibility in ensuring the safety of the contents of their mobile devices. Ultimately, it is hoped that this research can inform policymakers and service providers in designing mechanisms to reduce cybercrime cases and their related financial and social implications in Malaysia.

Keywords: qualitative methodology, behavioural change, cybercrime, mobile devices, user adoption