The Adoption of Security Control Apps among Smartphone Users in Tanzania

Daniel Koloseni, The Institute of Finance Management, Dar es Salaam, Tanzania
Eliamani Mathew Sedoyeka, The Institute of Finance Management, Dar es Salaam, Tanzania

ABSTRACT

Threats to mobile devices and smartphones, in particular, are on the rise, suggesting that data and information residing in the mobile device such as smartphones are in danger of being attacked. The current study employs an extended TBP as a theoretical framework to investigate the adoption of security control apps (i.e. antivirus) to safeguard against the attacks. A theoretical framework was tested using structural equation modelling (SEM) with data collected from 233 respondents. The study found that social influence, attitude and security awareness have an influence on the intention to adopt antivirus software while perceived behavioral control and individual risk propensity have no influence. Further security awareness has an influence on the attitude of smartphone users towards using antivirus software.

KEYWORDS

Adoption, Antivirus, Apps, Awareness, Risk Propensity, Security, Smartphone, Tanzania

BACKGROUND

There is a massive increase in smartphones usage among individuals in recent years. The smartphone is a simple version of a traditional computer which allows installation of programs or applications and can be programmed like a traditional computer (Jeon, Kim, Lee, & Won, 2011). The massive increase of smartphones for personal and business use is due to its portability, easy to use, affordability and easy internet accessibility. Smartphones are widely used in learning, health, business operations and for social purposes (Agrebi & Jallais, 2015; Wang, Xiang, & Fesenmaier, 2016; Dufau et al., 2011; Shin, Shin, Choo, & Beom, 2011; Strom, Vendel, & Bredican, 2014).

The capabilities of the smartphone to allow installation of applications, connection to the internet, connection to external storage devices such memory cards and on-the-go (OTG) place smartphones in similar information security threats and vulnerabilities as a normal or a traditional computer. Information security vulnerabilities to smartphones include malfunctions caused by implementation errors, risks of installing applications from untrusted sources, risks of connecting to the untrusted and unsecure wireless network and risks of improper applications configurations (Jeon et al., 2011). These vulnerabilities may create security loopholes that can be used by malware, to launch wireless network attacks and phishing attacks. Information security mechanisms which can be applied to secure smartphones include anti-virus to prevent against malware, spam filters to prevent spams and access to phishing sites and firewall to prevent network related attacks such as blocking malicious traffic (Jeon et al., 2011).

Smartphones contain a vast amount of personal data which is generated as the owner use or access apps (such as WhatsApp, Facebook, Twitter etc.) in his or her smartphone. The attacks on

DOI: 10.4018/IJTD.2019100101

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
smartphones may jeopardise severely security of user’s information and privacy. With the increasing use of smartphones to perform various offices works and for personal uses such as accessing e-services and social networks, we believe more efforts should be directed to the security of smartphones.

The number of people who uses antivirus applications is still low despite the increase in smartphone malware attacks. The study conducted by Hamza, Gadanya, Spikin and Abba (2015) indicates that only 17% of respondents are using antivirus in their smartphones as compared to 48% in desktop computers. A similar trend in poor adoption of security software for smartphones is also observed by Chiang et al., 2017, Mylonas, Kastania, and Gritzalis (2013) and Zhang, Li, and Deng, 2017. The threat of virus on smartphones increases exponentially. Currently, there are more than 400 different mobile viruses in circulation (Jeffrey & Bickford, 2012). Antivirus software is categorised as a security protection technology which is used as a security measure to offer proactive security defence against viruses (Blakley, McDermott, & Geer, 2001; Furnell & Clarke, 2012; Venter & Eloff, 2003). To the best of our knowledge, few studies such as Han, Wu and Windsor (2014) and Parker et al. (2015) have investigated the adoption of smartphone security controls such as antivirus. However, Parker et al. (2015) did not study the adoption of antivirus as a security control or measure instead paid attention to authentication controls and anti-theft controls. Hence, there is the scarcity of studies which investigate the factors influencing the adoption of security control measures such as using antivirus on smartphones.

Further, the literature on smartphone information security behaviour concentrated on security awareness leaving behind other security behaviour aspects such as attitude, social influence, perceived behavioural control, risk propensity etc. For example, Mylonas, Kastania and Gritzalis (2012) investigated security awareness regarding installations of apps from official repositories, Chin, Felt, Sekar and Wagner (2012) examined general installation habits, awareness on smartphone security and privacy, Ophoff and Robinson (2015) studied general awareness of smartphone security, Jones and Heinrichs (2012) studied general awareness of smartphone security practices and Parker, Ophoff, Belle and Karia (2015) investigated security awareness and security controls. Furthermore, a close examination of previous studies indicates that security awareness was mainly investigated using descriptive studies; therefore, little is known to what extent this factor has an influence on smartphone security behaviour. This study employs a theory of planned behaviour (TPB) as a foundational model to address the identified knowledge gaps.

In the process of addressing the knowledge gaps identified above, the current study offers contributions to the body of knowledge in two main areas. Firstly, despite many extensions of TPB, just a few studies in both desktop related security behaviours and smartphone security behaviour have paid attention to the relationship between information security awareness and risk propensity on intention to adopt antivirus apps in smartphones. Therefore, this study proposed an extended theoretical framework born out of TPB. The extended theoretical framework included two new constructs, security awareness and risk propensity which were rarely investigated in previous studies along with TPB constructs when investigating security behaviours of smartphone users. Second, unlike previous studies, security awareness is investigated in the explanatory study to understand the extent to which this factor has an influence on smartphone security behaviour. By doing so, we contribute to the understanding of the extent to which security awareness affects information security behaviours of smartphone users when adopting security control apps such as antivirus. Generally, this study contributes to the advancement of knowledge, through examining and discussing implications for researchers, security control apps developers, smartphone vendors and users.

RELEVANT THEORETICAL ADOPTION MODELS

Numerous theories from the information systems research literature can be used to investigate the adoption of security control apps among smartphone users. Relevant and predominantly IS research theories which can be used are Theory of Reasoned Action (TRA), Theory of Planned Behaviour
In Search of Women-Supportive Media for Sustainable Development in Nigeria
www.igi-global.com/chapter/in-search-of-women-supportive-media-for-sustainable-development-in-nigeria/187924?camid=4v1a

ICT Strategy for Development: Lessons Learnt from the Egyptian Experience in Developing Public-Private Partnerships
www.igi-global.com/chapter/ict-strategy-development/44314?camid=4v1a