Understanding Information Security Behaviours of Tanzanian Government Employees:
A Health Belief Model Perspective

Daniel Ntabagi Koloseni, Universiti Tunku Abdul Rahman, Kampar, Malaysia

Chong Yee Lee, Universiti Tunku Abdul Rahman, Kampar, Malaysia

Ming-Lee Gan, Universiti Tunku Abdul Rahman, Kampar, Malaysia

ABSTRACT

This article investigates security behaviours of employees using the Health Belief Model (HBM) as a theoretical lens. Given the fact that previous studies on security behaviours paid much attention to conscious information security behaviours; this article extends the HBM to study both habitual or automatic security behaviours (security habit) and conscious security behaviours of Tanzanian government employees. A structural equation modelling (SEM) technique was used for data analysis. The study found that, the intentions of government employees to practice information security behaviour is influenced by perceived severity, perceived susceptibility, perceived barriers, and cues to action and security habits. Their intentions, however, is not affected by perceived benefits and self-efficacy. Further, an employee's intentions and security habits has a significant effect on actual security practice. Generally, the extended research model enriches the understanding of the role played by both conscious and habitual security behaviours on information security behaviours of employees.

KEYWORDS

Behaviours, HBM, Information security, Security habit, Tanzania

INTRODUCTION

The application of e- government systems has become a norm in the delivery of e-services to citizens worldwide. The provision of e-services has transformed the manner in which services are delivered to citizens, providing the government with an innovative avenue for offering new services that can easily and conveniently be accessed by the citizens. In fact, the provision of e-services offers a number of benefits to both the government and the citizens, such as accelerating work processes, transparency, accountability and reducing the costs of operations (URT, 2013). Further, e-services improve citizen's participation and interaction in government activities (Al Hujran, Aloudat, & Altarawneh, 2013) In order to reap the benefits of e-services, the government of Tanzania has established a number of e-government services in recent years (Sawe, 2007; URT, 2013).

However, successful provision of e-government services heavily depends on citizen's trust on the security of information transacted over the network and e-government information systems during e-service delivery (Al Hujran et al., 2013; Jiménez et al., 2012; Wimmer & Bredow, 2002). Privacy and security of personal information are the most prominent barriers in e-government services delivery

DOI: 10.4018/IJTHI.2019010102

and critical for developing citizen trust and confidence to use the e-government services (Carter & Bélanger, 2005; Lee & Turban, 2001) Citizen's trust on security of information communicated over e-government systems should, therefore, be developed in order to encourage them to adopt the e-services (Warkentin, Gefen, Pavlou, & Rose, 2002).

With increasing prevalence of information security attacks, virtually all information systems are prone to attacks. Similarly, Tanzania e- government information systems are exposed to security threats. Primary factors that may lead to the breach of information security in Tanzania e-government information systems are: (1) poor perceptions with regard to potential susceptibility (vulnerability) and severity of security threats, benefits, and barriers of practising information security (Dewa & Zlotnikova, 2014; Pahnila, Siponen, & Mahmood, 2007; TCRA, 2012; Waziri & Yonah, 2014); (2) lack of security awareness and inadequate ICT security skills such as inability to apply proper security measures in case of security incidents (Dewa & Zlotnikova, 2014; Bakari, Tarimo, Yngstrom, & Magnusson, 2005; Shaaban, Conrad, & French, 2012); and (3) inappropriate information security habit such as sharing login credentials with colleagues, family members, friends and acquaintances to access ICT system (Shaaban, 2014); and connection of personal modems to workplace's mobile gadgets for internet accessibility that could pave the path for attackers to hack or misuse the organisation's information systems (Bakari, 2013; Dewa & Zlotnikova, 2014).

Without effective measures, the above problems are likely to continue and, therefore, may retard Tanzania government efforts to provide e- services to its citizens. Thus, a need arises to investigate information security behaviours of Tanzania government employees to practice information security behaviour during e- service provision.

Various studies have been carried out to investigate the influence of conscious behaviours such as perceived susceptibility, severity, benefits, barriers and self-efficacy on the practice information security behaviours (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Chan et al., 2005; Claar, 2011; Claar & Johnson, 2012; Dinev, 2008; Hanus & Wu, 2016; Liang & Xue, 2009; Ng et al., 2009; Pahnila et al., 2007; Pahnila, Siponen, & Mahmood, 2007; Safa et al., 2015; Workman et al., 2008). Nevertheless, only a handful have examined the role played by security habits (habitual behaviours) (Pahnila et al., 2007; Vance, Siponen, & Pahnila, 2012; Yoon, Hwang, & Kim, 2012). For example, Vance, Siponen and Pahnila (2012) investigated user's automatic compliance with information security policies, while Yoon, Hwang and Kim (2012) investigated user's automatic response to removing malicious software and viruses and suspicious emails. While the authors acknowledge various studies on the role played by of perceived susceptibility, severity, benefits, barriers and self-efficacy on information security behaviours, little attention has been paid to the role played by security habits (habitual or automatic behaviours) of the end users.

Specifically, this study focuses on investigating the information security behaviours of employees through the lens of the Health Belief Model (HBM) and contributes to the body of knowledge in information security behaviours in three ways. First, to the best of author's knowledge, prior studies on information systems (IS) have yet to extend the HBM model to measure information security habit. The addition of information security habit into the HBM may increase the capability of the model to measure information security behaviours. Second, HBM was designed to predict likelihood (intention) of performing health behaviours (Rosenstock, 1974). However, the behavioural intention may not lead to actual behaviour (Hsu & Huang, 2010) because what an individual intends to do may not be what an individual actually does (Herath, 2013). Therefore, the model has also been extended by adding another variable: information security behaviour to measure actual information security behaviours of employees when using e-government information systems. Third, Pahnila et al. (2007) suggested that information security habit could enhance respondents' intention to practice information security. Thus, determining the relationship between information security habits and information security behaviours is indeed important. This is because end-users who possess a certain level of security habits are likely to perform information security practices.

The Contributions of Perceived Graphic and Enactive Realism to Enjoyment and Engagement in Active Video Games

Jih-Hsuan Lin and Wei Peng (2015). *International Journal of Technology and Human Interaction (pp. 1-16).*

www.igi-global.com/article/the-contributions-of-perceived-graphic-and-enactive-realism-to-enjoyment-and-engagement-in-active-video-games/128400?camid=4v1a

Mobile Virtual Blackboard as Multimodal User Interface

Sladjana Tesanovic, Danco Davcev and Vladimir Trajkovik (2009). *Multimodal Human Computer Interaction and Pervasive Services (pp. 366-388).*

www.igi-global.com/chapter/mobile-virtual-blackboard-multimodal-user/35898?camid=4v1a