Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Personality, attitudes, and intentions: Predicting initial adoption of information security behavior

Jordan Shropshire [a], *Merrill Warkentin* [b,*], *Shwadhin Sharma* [b]

[a] *University of South Alabama, School of Computing, 150 Jaguar Drive, Mobile, AL 36688-7274, USA*
[b] *Mississippi State University, College of Business, P.O. Box 9581, Mississippi State, MS 39762-9581, USA*

ARTICLE INFO

Article history:
Received 23 July 2014
Received in revised form
22 September 2014
Accepted 3 January 2015
Available online 12 January 2015

Keywords:
Attitudes
Intention
Personality
Information security behavior
Conscientiousness
Agreeableness

ABSTRACT

Investigations of computer user behavior become especially important when behaviors like security software adoption affect organizational information resource security, but adoption antecedents remain elusive. Technology adoption studies typically predict behavioral outcomes by investigating the relationship between attitudes and intentions, though intention may not be the best predictor of actual behavior. Personality constructs have recently been found to explain even more variance in behavior, thus providing insights into user behavior. This research incorporates conscientiousness and agreeableness into a conceptual model of security software use. Attitudinal constructs perceived ease of use and perceived usefulness were linked with behavioral intent, while the relationship between intent and actual use was found to be moderated by conscientiousness and agreeableness. The results that the moderating effect of personality greatly increases the amount of variance explained in actual use.

1. Introduction

Why do some well-meaning computer users practice safe computing habits, while others do not, despite the intentions to do so? As early as the 12th Century, Saint Bernard of Clairvaux noted that good intentions do not always lead to positive actions (basis for the adage that “the road to hell is paved with good intentions”). It is common for individual computer users, despite knowing that their individual information resources are at risk, to fail to act on their intentions to practice safe computing behavior. (Safe behaviors include frequently changing passwords, archiving important data, scanning for malware, avoiding opening suspect emails, etc.) It is imperative that employees and others follow the intent to adopt secure technologies (such as anti-virus and anti-spyware software) with actual usage behavior (Furnell et al., 2007), but such follow-through is not universal. People within organizations, despite having the intention to comply with information security policies, are still considered to be the weakest link in defense against the existing information security as their actual security behavior may differ from the intended behavior (Han et al., 2008; Guo et al., 2011; Capelli et al., 2006; Vroom and Solms, 2004). These “trusted agents” inside the firewall may have the intention to comply with the organization's policy. However, there is a good probability that

* *Corresponding author*. Tel.: +1 662 325 1955; fax: +1 662 325 8651.
E-mail address: m.warkentin@msstate.edu (M. Warkentin).

http://dx.doi.org/10.1016/j.cose.2015.01.002
0167-4048/© 2015 Elsevier Ltd. All rights reserved.

they engage in risky behaviors of violating the integrity and privacy of sensitive information through non-malicious accidental actions such as passive noncompliance with security policies, laziness, or lack of motivation (Warkentin and Willision, 2009; Rhee et al., 2009). It is a common observation that people often fail to act in accordance with their behavioral intention (Ajzen et al., 2004). This is one of the reasons why the "internal threat" is often cited as the greatest threat to organizational information security (Capelli et al., 2006) despite employees usually having the intention to comply with information security policies.

However, the issue of intention leading to actual use has been uncritically accepted in Social Science research and information systems (IS) research (Bagozzi, 2007). Venkatesh et al. (2003, p. 427) stated that "role of intention as predictor of behavior…. has been well established." Ajzen and Fishbein (1980, p. 41) stated that "intention is the immediate determinant of behavior." The primary focus of the previous research has been on the formation of behavioral intention to measure the actual information technology (IT) behaviors almost to the exclusion of other factors that would affect the actual behavior of the respondent (Limayem et al., 2007). Many IS researchers have used behavioral intention to measure actual behavior of users (for example, Ifinedo, 2012; Johnston and Warkentin, 2010; Herath and Rao, 2009; Sharma and Crossler, 2014; Warkentin et al., 2012; Dinev and Hu, 2007).

In the context of protective behaviors (such as wearing seat belts, eating healthy diets, smoking cessation, etc.), it is evident that a great percentage of individuals have the intent to act in safe ways, but only some of these individuals will act on this intent. Empirical support for the relationship between user intentions and actual behavior is weak (Bagozzi, 2007), indicating that there may be other factors that explain why certain individuals may not act on their intentions and follow through with appropriate behaviors. Studies suggest that measuring intention rather than actual behaviors can be troublesome as intention doesn't always lead to behaviors (Crossler et al., 2013; Anderson and Agarwal, 2010; Mahmood et al., 2010; Straub, 2009). This gap between intention and behavior could be attributed to differences in cognitions or other unknown variables (Amireault et al., 2008) and to the fact that intentions are usually under cognitive control (Gollwitzer, 1996), whereas actual choices are often made rather impulsively and even unconsciously (Willison and Warkentin, 2013; Wansink and Sobal, 2007). Fishbein and Ajzen (1975) used a normative concept to explain the intention-behavior discrepancy while past behavior or habit have also been used as a moderating variable to explain this discrepancy (Limayem et al., 2007; Oullette and Wood, 1998; Triandis, 1977).

Few previous research studies have found additional predictive ability of intention to behavior by inclusion of constructs such as self-identity (Sparks and Guthrie, 1998), anticipated regret (van der Pligt and deVries, 1998), affect (Manstead and Parker, 1995), and moral norms (Conner and Armitage, 1998). Campbell (1963) traced the discrepancy to individual's dispositions – individuals with moderate dispositions respond favorably in the hypothetical context but unfavorably in the more demanding real context. Furthermore, behavioral intention to predict specific behavior may depend on "individual difference" factors or personality traits (Wong and Sheth, 1985). A combination of personality traits helps to narrow the discrepancy between intention and behavior by increasing predictive ability of intention on user's behavior (Corner and Abraham, 2001; Courneya et al., 1999; Rhodes and Courneya, 2003). Various personality factors have been suggested as possible moderators of the intention-behavior relationship, such that certain personality traits may explain why only some individuals will act upon their intentions.

The present study seeks to establish the role of personality factors in determining the likelihood that an individual will or will not follow through and act on the intent to engage in protective behaviors. Although this has been demonstrated in other disciplines (Meyerowitz and Chaiken, 1987), it has just begun to be studied in the information security field. For instance, Milne et al. (2000) recognized the role of personality factors in influencing an individual's perceptions of risk and vulnerability, and therefore his or her adoption of recommended responses to threats. Warkentin et al. (2012a) explain how the big five personality traits may influence intention to comply with security policies. Other studies have analyzed personality with regards to security-based decision making (Da Veiga and Eloff, 2010; Mazhelis and Puuronen, 2007). The IS literature has started to use personality assessment to understand users behavior and one of the widely used personality test is the "Big Five" test (Warkentin et al., 2012a; Karim et al., 2009; Shropshire et al., 2006). Of these personality traits considered, conscientiousness has been found to be consistently related to intentions and behaviors (Corner and Abraham, 2001) and is thus, the most important personality trait in relation to behaviors (Booth-Kewley and Vickers, 1994; Hu et al., 2008). People with higher conscientiousness are thought to be more organized, careful, dependable, self-disciplined and achievement-oriented (McCrae and John, 1992), adopt problem-focused rather than emotion-focused coping responses (Watson and Hubbard, 1996) and are less likely to use escape-avoidance strategies (O'Brien and Delongis, 1996). Information security executives with a higher degree of conscientiousness incline to react more cautiously to a given situation (Li et al., 2006). Similarly, agreeableness has been found to have significant influence on individual concern for information security and privacy (Korzaan and Boswell, 2008). Individuals with agreeableness traits are worried about what others would think of them and are more likely to be concerned about privacy issues (Brecht et al., 2012). Previous research has found agreeableness and conscientiousness to predict organizational citizenship behaviors such as following rules and procedures when behavior is not monitored (Rogelberg, 2006; Organ and Paine, 1999; Podsakoff et al., 2000). Konovsky and Organ (1996) used agreeableness and conscientiousness as two of the big five personalities that would predict satisfaction and some forms of organizational citizenship behavior. The choice of these conscientiousness and agreeableness to study the intention-behavior relationship for this paper is theoretically justified. Moreover, the other three traits are not conceptually linked to secure behaviors.

For the present study, the participants were shown a web-based tool that can provide useful information regarding security risks, and were informed that they could visit the website later from their own computer to assess its