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

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 vulnerabilities. Besides connecting self-reported behavioral intent with actual security program usage behavior, this study established the role of personality in moderating the former relationship. Specifically, conscientiousness and agreeableness were shown to lead to increased usage behavior among those who reported intent to adopt this security software.

2. Theoretical background

2.1. *Endpoint security*

The greatest threat to information security lies not beyond the security perimeter (hackers, malware, etc.), but rather with the careless or malicious actions of internal users such as employees and other trusted constituents with easy access to organizational information resources (Willison and Warkentin, 2013; Pfleeger and Caputo, 2012; Posey et al., 2011; Warkentin and Willison, 2009; Capelli et al., 2006). Each individual end user represents an endpoint in a computer network or a system and without security-compliant behaviors on the part of each end user, the network will not be secure. Secure behaviors include making regular backups, changing passwords, scanning for viruses, and many other activities identified by Whitman (2003) and others. Other security activities include updating applications, installing patches, turning off unnecessary ports, and configuring firewalls (Rosenthal, 2002; Stanton et al., 2003; Whitman, 2003).

There are salient differences between information security software usage and usage of other information technologies. In contrast to productivity-enhancing technology such as email utilities or spreadsheet applications, the benefits associated with security software are not immediately evident (Warkentin et al., 2004). Rather than providing a clear functionality for daily workplace activity, security software's benefits often go largely unnoticed. Information security tools, such as anti-spyware programs or biometric access controls, provide a means of controlling computing environments or maintaining a healthy technological baseline from which to employ productivity enhancing technologies. Therefore, performance benefits may not be explicitly recognized by end users. In addition, many end users lack the ability to appraise security risks and identify appropriate countermeasures (Adams and Sasse, 1999; Furnell et al., 2002; Siponen, 2001). The burden falls upon IT managers, information security specialists, and software designers to understand and predict problems related to endpoint security, and to address the sources of threats in an appropriate manner. Towards a better understanding of end user behaviors, the dependent variable of interest is initial use (adoption) of information security software by individual end users.

2.2. *Attitude*

Following Fishbein and Ajzen's seminal Theory of Reasoned Action (1975), many behavioral studies have used attitude to explain behavioral intentions (Karahanna et al., 2006). Within the information systems field, this theoretical foundation has been extended to predict behavioral intent to adopt and use of various information technologies (Assadi and Hassanein, 2010). The Technology Acceptance Model (TAM) (Davis, 1989), one of the most widely applied and cited models in the field, is comprised of two independent variables: perceived usefulness (PU) and perceived ease of use (PEOU) (Davis, 1989). PU is defined as “the degree to which a person believes that using a particular system would enhance his or her job performance,” while PEOU is “the degree to which a person believes that using a particular system would be free of effort.”

PU and PEOU were selected as antecedents of adoption behavior in this research for three reasons. First, although the two constructs were originally developed to explain adoption of spreadsheet software, they have also been applied to many other information technologies with much success (Bagozzi, 2007; Hirschheim, 2007; Karahanna et al., 2006; Venkatesh et al., 2007; Wang and Benbasat, 2007). They have also been referenced in a variety of disciplines outside of information systems (Duxbury and Haines, 1991). Finally, the TAM model is more parsimonious than later models, such as the Unified Theory for the Acceptance and Use of Technology (UTUAT) (Venkatesh et al., 2003).

A third attitudinal construct, perceived organizational support (POS) was included in the research model. POS hails from the organizational citizenship behavior research stream, and is defined as the degree to which an individual believes that the organization values his or her contribution and cares about his or her well-being (Eisenberger et al., 1986). There has been very limited research on perceived organizational support (POS) as a direct antecedent of IS security compliance, though IS research has been using organizational support as a control variable. It has been used to predict a range of employee organizational citizenship behaviors (Peele, 2007), including the adoption and use of information technology (Reid et al., 2008). Greene and D'Arcy (2010) analyzed the influence of employee-organization relationship factors such as POS on the decision of users' IS security compliance. Organizational motivational factors such as job satisfaction and POS all have positive impact on security compliance intention (D'Arcy and Greene, 2009). POS differs from PEOU and PU in that it concerns individual perceptions of the organization, not the technology. Previous studies have stated that employees who perceive support from the organization take it as a commitment of the organization towards them and pay it through commitment towards the organization such as focusing on organizational goals and policies (Eisenberger et al., 1986; Rhoades and Eisenberger, 2002). Because of its wide range of applications, and because it represents an additional dimension of end user attitude, POS was included in the research model.

2.3. *Personality*

Personality traits have long been used to explain various behavioral outcomes (Bosnjak et al., 2007; Funder, 1991; James and Mazerolle, 2002). Within information systems research, personality constructs have been used in various capacities, including system use (Klein et al., 2002; Pemberton et al., 2005; Vance et al., 2009; Kajzer et al., 2014). Further, Burnett and Oliver (1979), for example, observed that personality, product usage, and socio-economic variables moderate the effectiveness of attitudes on use behavior. Because of the potential increase in predictive power, the psychological constructs *conscientiousness* and *agreeableness* were used in this research to provide an improved understanding of adoption and use security software (Chenoweth et al., 2007; Devaraj et al., 2008; Shropshire et al., 2006; Vance et al., 2009). Both constructs stem from the Five Factor Model of personality as defined by John and Srivastava (1999). These two were specifically chosen because they were found to be highly relevant factors in contexts similar to organizational information security, such as precaution adoption, safety, and other related domains (Geller and Wiegand, 2005; Ilies et al., 2006). Cellar et al. (2001) found conscientiousness and agreeableness as the two most influencing personality types in workplace environment. Also, previous studies have shown conscientiousness and agreeableness as better predictors of 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) also choose conscientiousness and agreeableness as the two most important personality types to predict satisfaction and organizational citizenship behavior in work environment.

The personality factor conscientiousness is described as “socially prescribed impulse control that facilitates task and goal-oriented behavior, such as thinking before acting, delaying gratification, following norms and rules, and planning, organizing, and prioritizing tasks.” Several behavioral studies have identified a significant inverse relationship between accident involvement and conscientiousness (Cellar et al., 2001). Individuals who rate themselves as higher in delaying gratification, thinking before acting, following norms and rules, and planning and organizing tasks were less likely to be involved in accidents than those who rated themselves as lower on the same attributes (Geller and Wiegand, 2005).

Agreeableness is defined as “contrasting a pro-social and communal orientation towards others with antagonism, and including traits such as altruism, tender-mindedness, trust and modesty.” As with conscientiousness, agreeableness has been found to have a significant relationship with work safety, accident involvement, and organizational citizenship (Cellar et al., 2001; Ilies et al., 2006); those with stronger interpersonal orientations are more likely to agree to adopt safety recommendations.

3. Research hypotheses

The present study investigates the relationship between attitudes, personality, and the initial use (adoption behavior) of information security software (see Fig. 1). First, the relationship between the attitudinal constructs (perceived ease of use, perceived usefulness, and perceived organizational support) and adoption intention is confirmed. Then, the effects of adoption intention, conscientiousness, and agreeableness on initial use are explored. Specifically, it is purported that the personality constructs moderate the relationship between intent and use.

The first three hypotheses correspond with the attitudinal variables. Perceived Usefulness (PU) is “the degree to which a person believes that using a particular system would enhance his/her job performance” (Davis, 1989). Previous studies show that behavioral intention to use an Information System is largely driven by perceived usefulness (Davis, 1989, 1993; Straub, 2009; Fu et al., 2006). Perceived Ease of Use (PEOU) is the individual's assessment of the mental effort involved in using a system (Davis, 1989). Prior research indicates that perceived ease of use is a significant determinant of behavioral intention to use information technology (Gefen and Straub, 2000; Davis et al., 1989, 1992). Similarly, TAM2 and TAM3, which are expansions of Technology Acceptance Model (TAM) show PU and PEOU both affecting the behavioral intention to use a technology (Venkatesh and Davis, 2000; Venkatesh and Bala, 2008). The roles of perceived usefulness and perceived ease of use on IS security adoption have also been studied regularly in the past (Lee and Kozar, 2008; Lu et al., 2005). An individual's intention to adopt security software has been regularly linked to usefulness of the security software and its ease of use. Thus, it is hypothesized that:

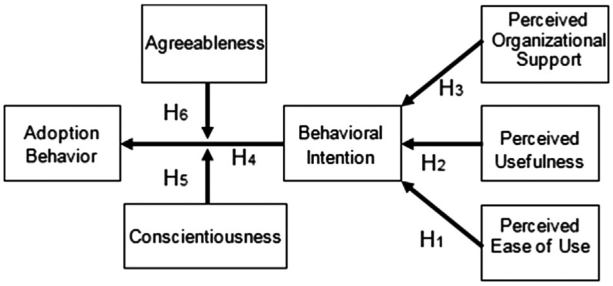


Fig. 1 – **Research model.**

H1. perceived ease of use is positively associated with intention to adopt security software.

H2. perceived usefulness is positively associated with intention to adopt security software.

Perceived Organizational Support (POS) strengthens the belief that the organization recognizes and rewards expected behavior, which in return encourages employees to be dedicated and loyal to the organization and its goal (Rhoades and Eisenberger, 2002). There have been numerous studies that have found a positive relationship between POS and employees' willingness to fulfill conventional job responsibilities that typically are neither formally rewarded nor contractually enforceable (Settoon et al., 1996). In IS field, perceived organizational support has been shown to have a positive impact on security compliance intention of the employees (D'Arcy and Greene, 2009). Therefore, this study posits the following:

H3. perceived organizational support is positively associated with intention to adopt security software.

The correlation between adoption intention and initial software use is also of interest. In the past, technology adoption studies have focused mainly on behavioral intent without actually measuring initial use. While there have been abundant IS research studies that have measured intention of people to comply or violate norms, laws or policies, there have been very few studies that have measured actual behavior of the users because of the level of difficulty in its measurement

(Warkentin et al., 2012b). Recent findings have questioned the strength of the relationship between behavioral intent and behavior outcome in various situational contexts (Abraham et al., 1999; Norman et al., 2003; Paulin et al., 2006). As such, it is necessary to test the relationship between adoption intention and initial use of security software:

H4. adoption intention is positively associated with initial use of security software.

Although intentions are commonly used to predict behavioral outcomes, dispositional factors such as personality may account for even more variance (Ilies et al., 2006; Karahanna et al., 1999; Mowen et al., 2007; Zhang et al., 2007). Personality has been theorized to significantly impact the relationship between intentions and behaviors, although few studies have yielded conclusive evidence (Ajzen, 2005; Endler, 1997; Gountas and Gountas, 2007). Therefore, this research investigates the role of personality as a moderator of the intention–behavior relationship:

H5. the higher the level of conscientiousness, the stronger the relationship between adoption intention and initial use of security software.

H6. the higher the level of agreeableness, the stronger the relationship between adoption intention and initial use of security software.

4. Method

4.1. *Procedure*

Subjects were introduced to a new web-based security program, called Perimeter Check, in a twenty minute presentation (see Fig. 2). Perimeter Check is unique in that it provides security measures that are not commercially available. It analyzes the user's computing environment, identifies potential vulnerabilities, and recommends actions that might improve the safety level for various computer activities (See Appendix A for a more complete description of this security program). Because it is web-based, Perimeter Check does not need to be loaded onto a computer - users may simply visit the Perimeter Check website to utilize the program's security features. During the presentation, Perimeter Check's features and benefits were explained, and directions for its use were given.

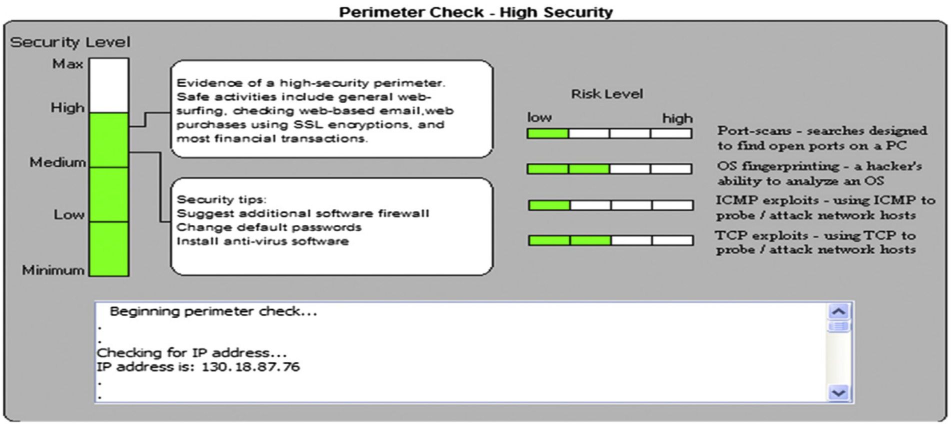
Because the IT governance structure of the university where this experiment is performed is decentralized, students, faculty, and staff members are provided significant autonomy to utilize and protect information resources. Accordingly, each individual user must actively secure his or her own computer and data. Because Perimeter Check provides several unique security features not available in other security programs, its advantages are quite salient. This web-based tool's functionality exceeds the feature sets of traditional security suites. The traditional security suites that are automated by personal computer lack the extensive feature of perimeter check such as identifying all the potential vulnerabilities in the user's computing environment, identifying the security level of existing software, risk level based on port scans, etc.

The subjects were asked to complete a survey regarding their personality and their attitudes toward the software (see Appendix B). They were also asked to provide their ID in order to assign extra credit for completing the survey. The subjects were given the web address of the security application (on a piece of paper), and were encouraged to use the security program regularly over the next four weeks. The twenty minute presentation was focused on motivating the users to use this security program along with the existing traditional security software in their computer to achieve comprehensive security.

In order to use the security program, subjects were required to log in using their IDs. The server maintained a log of subject IDs for those who had used the software at least once – this recorded actual initial adoption behavior.

4.2. *Subjects*

For this research, the sample pool consisted of undergraduate students enrolled in an introductory economics course at a large university in the southeastern United States. The decision to utilize students is supported by the findings of Agarwal and Karahanna (2000) and also by Gefen (2003), who found that a pool consisting of student subjects that come from diverse culture can be generalized to a larger population, especially when the phenomenon of interest is not social



Evidence of a high-security perimeter. Safe activities include general web-surfing, checking web-based email,web purchases using SSL encryptions, and most financial transactions.

Security tips:
Suggest additional software firewall
Change default passwords
Install anti-virus software

Port-scans - searches designed to find open ports on a PC

OS fingerprinting - a hacker's ability to analyze an OS

ICMP exploits - using ICMP to probe / attack network hosts

TCP exploits - using TCP to probe / attack network hosts

```
 Beginning perimeter check...
.
.
Checking for IP address...
IP address is: 130.18.87.76
.
.
```

Fig. 2 – The security software program – “perimeter check”.

context (the study participants did not socialize in our experiment – the adoption process is an individual one). Of 196 registered students in the course (sample population), 180 subjects viewed the demonstration and completed the survey. Ten incomplete surveys were discarded, leaving an N of 170 usable surveys. Of this number, 54 visited the Perimeter Check website and used the software (initial use). Background data were compiled to create a demographic profile of respondents. Most were male (65.88%), with an average age of 21. The respondents were experienced computer users – they had a collective average of five or more years' experience using a computer to perform important tasks, and used computers frequently. In addition, they all reported having access to a personal computer on which they could save documents and files and indicated the belief that they possess valuable electronic data they wished to protect.

4.3. *Measures and instrumentation*

The present study involves the measurement of six latent constructs, including perceived ease of use, perceived usefulness, perceived organizational support, adoption intention, conscientiousness, and agreeableness. Perceived ease of use was operationalized using six formative scale items. The items were adopted and modified from Davis (1989) to fit the context of this study. Perceived usefulness was operationalized using six formative scale items. The items were adapted for this research. Perceived organizational support was operationalized using eight formative items. The items were modified from Eisenberger et al. (2002) for the present study. Behavioral intent was represented by three reflective items. These items were originally developed for a similar study (Fishbein and Ajzen, 1975), and have since been used to predict a range of human behaviors. Conscientiousness was operationalized using seven word pairs. The items were developed and validated by Goldberg (1992). Agreeableness was represented in terms of seven word pairs. The items for this construct were also borrowed from Goldberg (1992). Finally, actual use was operationalized in terms of the number of times each subject used the security program. Actual server data was used for this measure; this was possible because subjects were required to log in each time they used the program.

Items for perceived ease of use, perceived usefulness, perceived organizational support, and behavioral intent were measured using five-point Likert scales, were '1' corresponded with 'strongly disagree' and '5' corresponded with 'strongly agree.' The word pairs for conscientiousness and agreeableness were measured using five-point Likert scales. For each word pair, '1' indicated strong association with the first word and '5' indicated strong association with the second word in the pairing.

Following established guidelines (Jarvis et al., 2003; Petter et al., 2007), several of the constructs and corresponding scales used in this study were determined to be formative as opposed to reflective. As previously indicated, perceived ease of use, perceived usefulness, and perceived organizational support were identified as formative, while behavioral intent, conscientiousness, and agreeableness were recognized as reflective. Because biases may occur when formative constructs are mis-specified as reflective (Mackenzie et al., 2005), the constructs were classified according to the four decision rules outlined by (Petter et al., 2007). In summary, these rules concern the direction of causality among constructs and items, and the interchangeability, covariation, and nomological net of the scale items.

Content validity for all instrument scales was established through both literature review and an expert panel comprised of 3 researchers with experience in scale development and 2 information security experts. Particularly for formative constructs, content validity is critical, as removal of items from formative scales must be theoretically driven and must not compromise scale robustness by removing items that capture critical dimensions of the latent variables (Diamantopoulos and Winklhofer, 2001; Straub et al., 2004).

5. Results

Once the data were collected, a two-step analysis was conducted to ensure the validity and reliability of measures prior to testing the proposed relationships (Gefen et al., 2000). The analysis followed a components-based approach to structural equation modeling with the smartPLS software package because the research model contains both formative and reflective constructs (Ringle et al., 2005) and allows simultaneous usage of reflective and formative measurement even under condition of non-normality and small to medium sample sizes (Chin et al., 2003). This paper conducted tests of significance for all paths using the bootstrap re-sampling procedure (Cotteman and Senn, 1992) and used the standard approach for evaluation that requires path loadings of each construct to exceed 0.70. The paper follows with the convergent and discriminant validity check of reflective scale and then the validity and reliably checks of formative measures. Indicator weights were used in the analysis (Gefen et al., 2000) because loadings for formative indicators may be misleading (Chin et al., 2003).

5.1. *Convergent validity*

The convergent validity of the reflective constructs was assessed by considering individual item reliability and construct reliability (Barclay et al., 1995). Item reliability was determined by examining the degree to which items load on their corresponding latent constructs. An item was judged to be sufficiently reliable if its loading was greater than or equal to 0.70 (Fornell and Bookstein, 1982). As such, all the items for behavioral intent and conscientiousness exhibited convergent validity. However, two of the items of our construct called "agreeableness" had item loadings less than 0.7. Thus, these two items "AGREE1" (i.e. Selfish…Unselfish) and "AGREE6" (i.e. Distrustful… Trustful, see Appendix B) were found to be lacking in reliability; these items were not included in subsequent analysis. As depicted in Table 1, the remaining scale items for the reflective constructs exceeded the recommended threshold for item reliability.

Construct reliability was determined by examining the internal consistency measure for each construct. Constructs which exceeded the 0.70 level of internal consistency were

Table 1 – Convergent validity of measurement model.

Construct	Item	Item reliability	Internal consistency	Cronbach's alpha[b]
Behavioral intent (BINT)	BINT1[a]	.936	.9604	.9381
	BINT2	.967		
	BINT3	.998		
Conscientiousness (CONS)	CON1	.779	.8239	.8142
	CON2	.796		
	CON3	.735		
	CON4	.717		
	CON5	.853		
	CON6	.762		
Agreeableness (AGREE)	AGREE2	.906	.8054	.7962
	AGREE3	.937		
	AGREE4	.844		
	AGREE5	.898		
	AGREE7	.764		

[a] Note: BINT1 implies item 1 under construct Behavioral Intent, while BINT2 implies item 2 under Behavioral Intent and so on. Please see Appendix B for details.
[b] For illustrative purposes only.

judged to possess sufficient reliability (Barclay et al., 1995; Fornell and Larcker, 1981). As shown in Table 1, behavioral intent, conscientiousness, and agreeable possessed internal consistency measures above the recommended threshold for construct reliability. For purposes of comparison, the Cronbach's alpha score was also computed for each of the constructs. Because the scale items and constructs possessed sufficient reliability, the requirements for convergent validity were met.

5.2. *Discriminant validity*

At the indicator level, discriminant validity was assessed by analyzing item cross-loadings; at the construct level discriminant validity was considered by reviewing relationships between constructs and the square root of the average variance extracted (AVE) (Bollen, 1989). Individual items were assumed to possess sufficient discriminant validity if they loaded higher on their own respective construct than on any other latent variable (Gefen et al., 2000; Straub et al., 2004). As depicted in Table 2, each item loaded highest on its respective latent construct.

Discriminant validity was assessed at the construct level by comparing the square root of each construct's AVE against its correlation with other constructs (Barclay et al., 1995), (Fornell and Larcker, 1981). As depicted in Table 3, the square root of each AVE is greater than the correlations between the constructs, indicating that more variance is shared between the construct and its indicators and then with other constructs. Based on the assessment of the reflective items and constructs, the requirements for discriminant validity were satisfied.

5.3. *Validity and reliability of formative measures*

The validity of formative measures was assessed by considering the results of a principal components analysis (PCA), and examining item weightings (Chin et al., 2003). As suggested by Diamontopoulos and Winklhofer (2001), items were assumed to be valid if their weightings were significant. Several items were not found to be significant, including item number 5 for perceived ease of use (i.e. PEOU5), item numbers 1, 2, and 4 for perceived usefulness (i.e. PU1, PU2, and PU4), item number 2, 5, 7, and 8 for perceived organizational support (i.e. POS2, POS5, POS7, and POS8) (see Table 4 and Appendix B for details). These items were not found to be sufficiently valid as their item weightings were nonsignificant, and thus were removed from the analysis. Formative constructs constitute different aspects of a construct, the items shouldn't have a higher correlation with each other (Diamantopoulos and Winklhofer, 2001). Thus, reliability was assessed by considering multicollinearity among scale items.

Multicollinearity is not a desirable trait among formative indicators, and may decrease reliability (Petter et al., 2007). The variance inflation factor (VIF) was used to measure multicollinearity; the items were judged to be sufficiently reliable if the VIF statistics were less than or equal to 3.3

Table 2 – Loading and cross-loading matrix.

Construct	Item	Latent construct		
		BINT	CONS	AGREE
Behavioral Intent (BINT)	BINT1	.9398	.1490	.1703
	BINT2	.9342	.2142	.2016
	BINT3	.9558	.1516	.1699
Conscientiousness (CONS)	CONS1	.1888	.8803	.3483
	CONS2	.0876	.6508	.3573
	CONS3	.1111	.5471	.3543
	CONS4	.0514	.4217	.2378
	CONS5	.1024	.6527	.3337
	CONS6	.1172	.7594	.3722
Agreeableness (AGREE)	AGREE2	.1401	.4228	.8076
	AGREE3	.0835	.1567	.4259
	AGREE4	.1780	.3281	.7496
	AGREE5	.1489	.3742	.7353
	AGREE7	.0901	.2812	.6962

Table 3 – Correlations among reflective constructs.

Construct	BINT	CONS	AGREE
Behavioral intent (BINT)	.9433		
Conscientiousness (CONS)	.1818	.6707	
Agreeableness (AGREE)	.1912	.4873	.6849

Note: Square-rooted AVE on diagonal.

(Diamantopoulos and Winklhofer, 2001). The calculated VIF statistics were all within the recommended threshold for reliability (Table 4). As evidenced by these assessments, the formative constructs were found to be sufficient, valid and reliable.

5.4. *Model relationship testing*

The bootstrap sampling procedure was used to test the proposed relationships among the constructs (Gefen et al., 2000). This approach to structural equation modeling was necessary as the model included formative constructs. Path coefficients and t-values were obtained through this procedure (Table 5). Of the three determinants of behavioral intent, perceived ease of use and perceived usefulness were supported while perceived organizational support was not found to be significant. A possible explanation for this outcome regards the study context – undergraduates at a large university. Because the university did not officially adopt the security program, it is conceivable that the subjects assumed the software did not have the university's support. Thus, expectations of organizational support would be low, even if subjects intended to use the software. Finally, the path between behavioral intent and actual use was found to be significant. The model's explanatory power was considered by observing the R^2 of endogenous constructs (Chin et al., 2003). As shown in Fig. 3, perceived ease of use and perceived usefulness accounted for over 30% of the variance in behavioral intent. However, behavioral intent, without the assistance of personality moderators, only explained 10.4% of the variance in actual use.

The moderating effect of conscientiousness and agreeableness was then tested. The R^2 values between the main and interaction effects were compared (see Table 6) and Cohen's f2 was calculated, following Chin (1998). Interaction effect sizes were considered small if 0.02, medium if 0.15, and large if 0.35 (Cohen, 1988). The results of this analysis support the role of conscientiousness and agreeableness as moderators of the relationship between behavioral intent and actual use. Conscientiousness has a medium sized moderating effect; agreeableness had a small/medium effect. Together, they increase the amount of variance explained by 14%. Finally, Table 7 presents the results of the hypotheses tests; with the exception of H3, all the proposed relationships were supported.

Table 5 and Fig. 3 show the beta scores and t-values for the relationships displayed in the research model. Fig. 3 also shows that the R-squared values for both the dependent constructs are greater than 0.10 (Falk and Miller, 1992). All the paths are significant except the path between perceived organizational support and behavioral intention to adopt security software ($\beta = 0.105$, $t = 1.06$, $p < 0.150$). Thus, H3 was not supported. Perceived ease of use was found to have a significant relationship with PU supporting H1 ($\beta = 0.322$, $t = 3.554$, $p < 0.001$). Perceived usefulness has a significant relationship with behavioral intention to adopt security software, supporting H2 ($\beta = 0.314$, $t = 3.433$, $p < 0.001$). H4 was also supported ($\beta = 0.252$, $t = 3.625$, $p < 0.001$) implying that behavioral intention has a significant relationship with extent of use. Also, as shown by Table 6, conscientiousness and agreeableness both moderate the relationship between behavioral intent and extent of use, supporting H5 and H6. In this study, conscientiousness was found to have a moderate size moderating impact as the interaction effect size is 0.146 and agreeableness has small/medium effect on moderating impact as the interaction size is 0.093 (Cohen, 1988).

6. Discussion

6.1. *Key findings and implications*

Consistent with earlier research, perceived ease of use and perceived usefulness were found to be significant predictors of

Table 4 – Validity and reliability of formative measures.

Construct	Item	Weight	t-Value	Significance	VIF
Perceived ease of use (PEOU)	PEOU1[a]	.3692	2.8260	$\rho < .001$	2.99
	PEOU2	.2029	2.2748	$\rho < .010$	2.83
	PEOU3	.4164	3.1477	$\rho < .001$	3.17
	PEOU4	.0132	2.5549	$\rho < .005$	2.78
	PEOU6	.0615	3.1198	$\rho < .001$	2.89
Perceived usefulness (PU)	PU3	.1904	2.1693	$\rho < .050$	3.03
	PU5	.0293	3.0056	$\rho < .001$	2.85
	PU6	.4455	2.6942	$\rho < .005$	2.94
Perceived organizational support (POS)	POS1	.2144	2.9732	$\rho < .001$	2.89
	POS3	.4431	2.6063	$\rho < .005$	3.22
	POS4	.0681	1.9771	$\rho < .050$	2.86
	POS6	.2917	2.4488	$\rho < .010$	3.08

[a] Note: PEOU1 implies item 1 for Perceived ease of use and so on. Please see Appendix B for details.

Table 5 – Path coefficients and their t-Values.

Hypothesis	Path from	Path to	Path coefficient (β)	t-Value	Significance
H_1	PEOU	BI	.322	3.554	ρ < .001
H_2	PU	BI	.314	3.433	ρ < .001
H_3	POS	BI	.105	1.063	ρ < .150
H_4	BI	USE	.252	3.625	ρ < .001

software adoption intention. In contrast to the extant literature on general software adoption behavior, however, perceived usefulness was not found to be the most important factor in forming an adoption intention. Rather, the present study's findings are consistent with earlier security software adoption studies which suggested that computer users have perceptions of security software which differ from perceptions of other information technologies, and that the attitudes included in the technology adoption model do not fully reflect user motivation to adopt security software, (Warkentin et al., 2004; Woon et al., 2005). For traditional office automation and personal productivity software, the functionality of the software contributes directly to task efficiency and/or effectiveness. Increased perception of usefulness are likely to result from increased ability to sort data, generate reports, compile graphs, attach documents to email, etc. But users may not perceive security software as supporting work activities directly. More effective virus scanning, for example, is not likely to be perceived as increasing productivity; it contributes to the establishment of a secure technological work platform, but does not directly support work activities. Therefore, PU (which measures improved job performance productivity) may not be appropriate.

As a predictor of initial use, adoption intention was significant, although it explained less variance than expected. The majority of the sample population indicated an intention to adopt the security measure, but less than a quarter actually followed through on their intentions. Thus, it appears that factors other than intention play a significant role in determining behavioral outcomes. The lack of explanatory power also supports the assertion that intention should not be used as a surrogate for actual behavior unless its explanatory power has been vetted within the associated adoption context (Chandon et al., 2005). Thus, this study provides additional value by providing a basis for further research in security adoption.

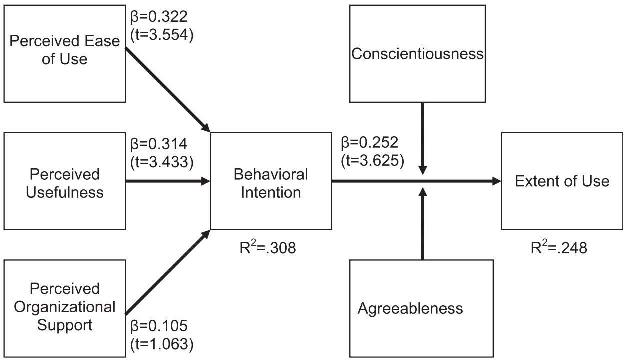


Fig. 3 – Structural model.

The present study offers several unique contributions that inform the research foundation for academics as well as practicing information security managers. First, this research analyzed the relationship between perceived ease of use, perceived usefulness, perceived organizational support, and intention to adopt security software and established statistically valid findings in this area. Second, this project tested the link between intention and actual initial use, which has not been previously analyzed within the context of secure user behaviors. In this regard, this research has avoided the problems related to common methods bias by collecting actual usage behavior. Finally, this project explored the role of personality as a moderator of intention and identified important findings. This research can help the practitioners as well. Practicing information security managers may also take notice of this predictor of secure behavior. Perhaps personnel selection, training, and retention policies might be informed by the findings of this research.

6.2. *Limitation and future research*

McGrath (1981) describes the "three horned dilemma" to highlight the trade-offs between various research designs, and argues that all empirical designs are subject to inherent limitations. Various research designs may result in greater or less (1) generalizability to the target population, (2) precision in measurement and control of the behavioral variables, and (3) realism of context. Our experimental design slightly favored realism (actual field study with a real security tool, not a contrived lab experiment) and precision (using established, previously-validated instrument items with a statistically significant sample size) over generalizability (using college student volunteers with demographic characteristics that do not perfectly match the entire population of computer users).

The sampling frame for this study was students, most of who were between the ages of 18 and 21. Characteristics of computer users were once very different from the overall population, but the differences are disappearing as the digital

Table 6 – Test of training recency as a moderator.

Interaction term	Cohen's f^2	Effect size
Conscientiousness x behavioral intent on extent of usage	.146	Medium
Agreeableness x behavioral intent on extent of usage	.093	Small/medium

Table 7 – Outcome of the hypotheses test.

	Hypothesis	Outcome
H_1	Perceived ease of use will have a positive influence on behavioral intent	Supported
H_2	Perceived usefulness will have a positive influence on behavioral intent	Supported
H_3	Perceived organizational support will have a positive influence behavioral intent	Not supported
H_4	Behavioral intent will have a positive influence on extent of use	Supported
H_5	Conscientiousness will moderate the relationship between behavioral intent and extent of use	Supported
H_6	Agreeableness will moderate the relationship between behavioral intent and extent of use	Supported

divide is closing and as universal access to technology is becoming a reality. Computer users are young and old, rich and poor, and male and female of all ethnic groups. Our sample population was younger, but other characteristics were similar to the broad spectrum of computer users in this important regard. More importantly, they reported being experienced computer users, as would be expected. They reported frequent computer usage and possession of data they valued. In short, they were motivated to protect valuable information resources, and therefore closely matched the population of computer users. Although previous research has shown that computer related behaviors doesn't change significantly between different age groups, ethnic groups, sex or level of richness, the student sample represents a limitation of this design.

The present study could be extended in the future by several ways. First, an expanded research sample could include a broader spectrum of computer users, perhaps in a diverse set of organizational environments. Second, the role of conscientiousness and agreeableness (and personality in general) should be explored as an interesting avenue for further research in information security behavior adoption. Third, other secure behaviors (password selection, data backup procedures, scanning activity, etc.) could be analyzed to further establish the relationships evident in this project. Fourth, post-adoption activity (continuance or discontinuance, for example) could be explored with a longitudinal research design. Fifth, time perspective theory could be used to understand variance in the actual behavior as behavior is influenced by how individuals link their behavior to their past, present, and future along with their personality (Zimbardo and Boyd, 1999).

7. Conclusion

Although IS research are focused on measuring the actual behaviors based on behavioral intention, there has been intention-behavior discrepancy due to present of unknown variables that exist in between the behavioral intention and actual behavior. This has led to lower accuracy among researchers to predict security compliance behavior. One such factor that may help researchers to bridge this gap is to understand the “Big Five” personality of the users. Based on earlier research on organizational safety, two personality factors from the five factor model, conscientiousness and agreeableness, were included in the present paper as moderators of intention. Perceived ease of use, Perceived Usefulness and Perceived Organizational Support were the three constructs used as attitudinal constructs affecting behavioral intention. With the help of 170 undergraduate responses from a large US university, we performed empirical test on the proposed model. The result suggested that perceived usefulness and perceive ease of use has a positive influence on behavioral intention while perceived organizational support doesn't have a positive influence on behavioral intention. The behavioral intention was found to have positive effect on extent of use. Conscientiousness and agreeableness were both supported as moderators and independent predictors of initial use.

Appendix A. Description of perimeter check

Perimeter Check is a web-based security tool which was developed exclusively for research purposes. It is not available for commercial distribution. The purpose of this security application is to assess a PC's susceptibility to attacks from third parties. The program performs an analysis of a PC's security profile and provides feedback.

This information security utility combines an executable program written in ANSI-standard C++ with the LAMP architecture (Linux operating system, Apache server, MySQL, and PHP) (see Figure A-1). Perimeter Check can be accessed via the internet through a secured webpage. PHP scripts are used for authentication and for passing a user's IP address is to the C++ component. This component uses many of the network and probe features found in open source hacking tools (such as NMAP). Packets are crafted for identifying host characteristics, such as operating system, browser type, services available, ports open, firewall/configuration, and susceptibility to various TCP, ICMP, and IP attacks.

The returned packets are examined via the C++ component of Perimeter Check, and the results are conveyed to the end user via PHP-generated webpage content. Along with diagnostic information, suggestions for improving the security of a host PC are provided. In the design of Perimeter Check, much care was taken to avoid providing network and host details which, in the wrongs, might be used to damage systems and networks.

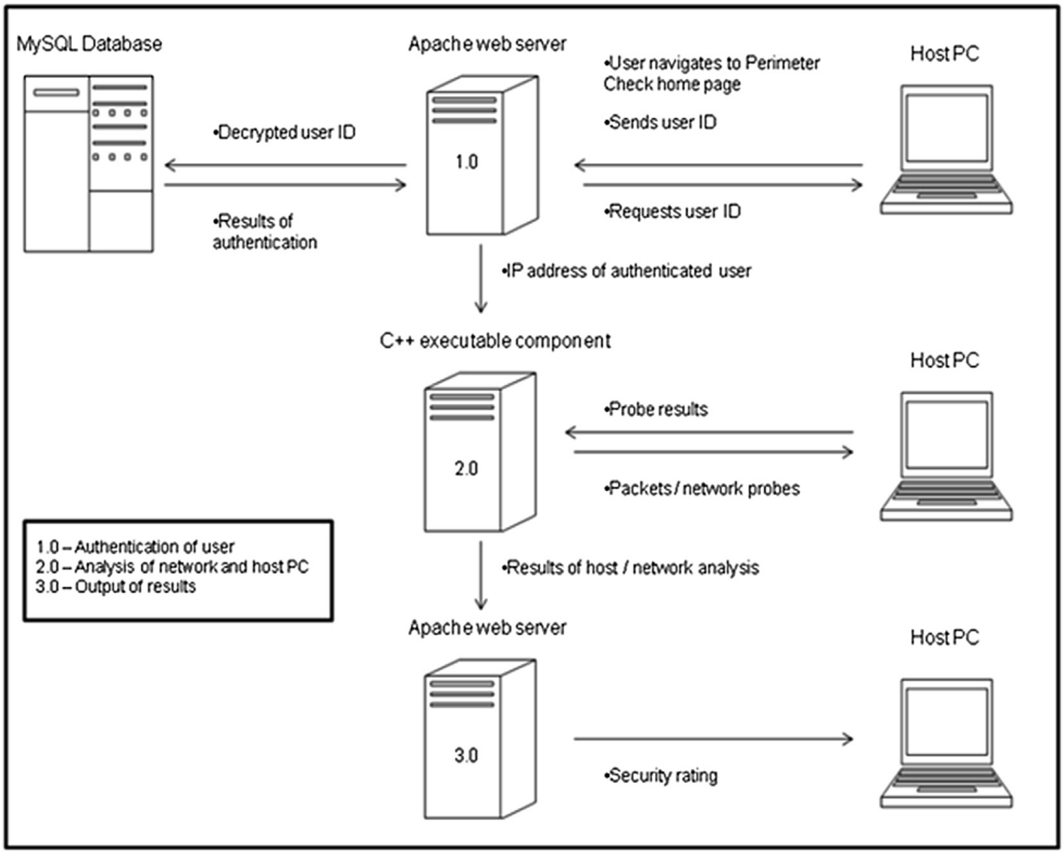

MySQL Database
Apache web server
•User navigates to Perimeter Check home page
•Sends user ID
Host PC
•Decrypted user ID
1.0
•Results of authentication
•Requests user ID
•IP address of authenticated user
C++ executable component
Host PC
•Probe results
2.0
•Packets / network probes
1.0 – Authentication of user
2.0 – Analysis of network and host PC
3.0 – Output of results
•Results of host / network analysis
Apache web server
Host PC
3.0
•Security rating

Figure A-1 – Data flow – perimeter check.

Appendix B. Scales and items

Items	Perceived ease of use (five-point agreement scale) – Adapted from Davis (1989).
PEOU1	My interaction with Perimeter Check would be clear and understandable.
PEOU2	I would find Perimeter Check to be flexible to interact with.
PEOU3	I would find it easy to Perimeter Check to do what I want it to do.
PEOU4	Learning to operate Perimeter Check would be easy for me.
PEOU5	It would be easy for me to become skilled at using Perimeter Check.
PEOU6	I would find Perimeter Check easy to use.
Items	**Perceived Usefulness (five-point agreement scale) – Adapted from Davis (1989)**
PU1	Using Perimeter Check in my job would enable me to accomplish tasks more quickly.
PU2	Using Perimeter Check would improve my job performance.
PU3	Using Perimeter Check would improve increase my productivity.
PU4	Using Perimeter Check would enhance my effectiveness on the job.
PU5	Using Perimeter Check would make it easier to do my job.
PU6	I would find Perimeter Check useful in my job.
Items	**Perceived Organizational Support (five-point agreement scale) – Adapted from Eisenberger et al. (2002)**
POS1	The organization values my contribution to its well-being.
POS2	The organization fails to appreciate any extra effort from me. (R)
POS3	The organization would ignore any complaint from me. (R)
POS4	The organization really cares about my well-being.
POS5	Even if I did the best job possible, the organization would fail to notice. (R)
POS6	The organization cares about my general satisfaction at work.
POS7	The organization shows very little concern for me. (R)
POS8	The organization takes pride in my accomplishments at work.

(continued on next page)

(continued)	
Items	**Agreeableness (five-point word pair scale) – Adapted from Goldberg (1992)**
AGREE1	Selfish … Unselfish
AGREE2	Unkind … Kind
AGREE3	Uncooperative … Cooperative
AGREE4	Cold … Warm
AGREE5	Disagreeable … Agreeable
AGREE6	Distrustful … Trustful
AGREE7	Stingy … Generous
Items	**Conscientiousness (five-point word pair scale) – Adapted from Goldberg (1992)**
CON1	Disorganized … Organized
CON2	Irresponsible … Responsible
CON3	Negligent … Conscientious
CON4	Impractical … Practical
CON5	Careless … Thorough
CON6	Lazy … Hardworking
CON7	Extravagant … Thrifty
Items	**Intention (five-point agreement scale) – Adapted from Fishbein and Ajzen (1975)**
BI1	I intend to use Perimeter Check
BI2	I plan to use Perimeter Check
BI3	I predict I will use Perimeter Check
Note: Items marked (R) are reverse-coded. (plus demographic questions, computer usage questions, and ID).	

REFERENCES

Abraham C, Sheeran P, Norman M, Conner M, Wries ND, Otten W. When good intentions are not enough: modeling post-decisional cognitive correlates of condom use. J Appl Soc Psychol 1999;29(2):2591–612.

Adams A, Sasse M. Users are not the enemy. Commun ACM 1999;42(12):40–6.

Agarwal R, Karahanna E. Time flies when you're having fun: cognitive absorption and beliefs about information technology. MIS Q 2000;24(4):665–94.

Ajzen I. Attitudes, personality, and behavior. 2nd ed. Chicago, IL: McGraw-Hill; 2005.

Ajzen I, Fishbein M. Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice Hall; 1980.

Ajzen I, Thomas CB, Franklin C. Explaining the discrepancy between intentions and actions: the case of hypothetical bias in contingent valuation. Personal Soc Psychol Bull 2004;30(9):1108–21.

Amireault S, Godin G, Vohl MC, Pérusse L. Moderators of the intention-behaviour and perceived behavioural control-behaviour relationships for leisure-time physical activity. Int J Behav Nutr Phys Activity 2008;5(1):7.

Anderson CL, Agarwal R. Practicing safe computing: a multimethod empirical examination of Home computer user security behavioral intentions. MIS Q 2010;34(3):613–44.

Assadi V, Hassanein K. Continuance intention to use high maintenance information systems: the role of perceived maintenance effort. In: The 18th European conference on information systems, Pretoria, South Africa; 2010.

Bagozzi R. The legacy of the technology acceptance model and a proposal for a paradigm shift. J Assoc Inf Syst 2007;8(4):244–54.

Barclay D, Higgins C, Thompson R. The partial least squares approach to causal modeling: personal computer adoption and use as an illustration. Technol Stud 1995;2(2):285–309.

Bollen K. Structural equations with latent variables. New York, NY: Wiley; 1989.

Booth-Kewley S, Vickers RR. Associations between major domains of personality and health behavior. J Personal 1994;62(3):281–98.

Bosnjak M, Brakto D, Galesic M, Tuten T. Consumer personality and individual differences: revitalizing a temporarily abandoned field. J Bus Res 2007;60(6):590–6.

Brecht F, Fabian B, Kunz S, Müller S. Communication anonymizers: personality, internet privacy literacy and their influence on technology acceptance. Eur Conf Inf Syst 2012;214:1–13.

Burnett J, Oliver R. Fear appeal effects in the field: a segmentation approach. J Mark Res 1979;16(2):181–90.

Campbell DT. Social attitudes and other acquired behavioral dispositions. Chichester: Wiley; 1963.

Capelli D, Desai A, Moore A, Shimeall T, Weaver E, Wilke B. Management and education of the risk of insider threat. In: Proceedings of the 24th international system dynamics conference, Netherlands; 2006.

Cellar D, Nelson Z, Yoke C. The five factor model: investigating the relationships between personality and accident involvement. J Prev Interv Community 2001;22(1):43–52.

Chandon P, Morwitz V, Reinartz W. Do intentions really predict behavior? Self-generated validity effects in survey research. J Mark 2005;69(2):1–14.

Chenoweth T, Minch R, Tabor S. Expanding views of technology acceptance: seeking factors explaining security control adoption. In: Proceedings of AMCIS; 2007. p. 321–32.

Chin W. The partial least squares approach to structural equation modeling. In: Marcoulides M, editor. Modern methods for business research. Mahwah, NJ: Lawrence Erlbaum Associates; 1998. p. 295–336.

Chin W, Marcolin B, Newsted P. Modeling approach for measuring interaction effects: results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. Inf Syst Res 2003;14(2):189–217.

Cohen J. Statistical power analysis for the behavioral sciences. Hillsdale, NJ: Lawrence Erlbaum Associates; 1988.

Conner M, Abraham C. Conscientiousness and the theory of planned behavior: toward a more complete model of the antecedents of intention and behavior. Personal Soc Psychol Bull 2001;27(11):1547–61.

Conner M, Armitage CJ. Extending the theory of planned behavior: a review and avenues for further research. J Appl Soc Psychol 1998;28(15):1429–64.

Cotteman W, Senn J. Challenges and strategies for research in systems development. John Wiley & Sons, Inc; 1992.

Courneya KS, Bobick TM, Schinke RJ. Does the theory of planned behavior mediate the relation between personality and exercise behavior? Basic Appl Soc Psychol 1999;21(4):317–24.

Crossler R, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. Comput Secur Comput Secur 2013;32(1):90–101.

D'Arcy J, Greene G. The multifaceted nature of security culture and its influence on end user behavior. In: Proceedings of IFIP TC8 international workshop on information systems security research, May 29-30, Cape Town, South Africa; 2009. p. 145–57.

Da Veiga A, Eloff J. A framework and assessment instrument for information security culture. Comput Secur 2010;29(2):196–207.

Davis F. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q 1989;13(3):319–39.

Davis F. User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. Int J Man-Machine Stud 1993;38(3):475–87.

Davis F, Bagozzi RP, Warshaw PR. User acceptance of computer technology: a comparison of two theoretical models. Manag Sci 1989;35(8):982–1002.

Davis F, Bagozzi RP, Warshaw PR. Extrinsic and intrinsic motivation to use computers in the workplace. J Appl Soc Psychol 1992;22(14):1111–32.

Devaraj S, Easley R, Crant J. How does personality matter?, Relating the five-factor model to technology acceptance and use. Inf Syst Res 2008;19(1):93–105.

Diamantopoulos A, Winklhofer H. Index construction with formative indicators: an alternative to scale development. J Mark Res 2001;38(2):269–77.

Dinev T, Hu Q. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J Assoc Inf Syst 2007;8(7):386–408.

Duxbury L, Haines G. Predicting alternative work arrangements from salient attitudes: a study of decision makers in the public sector. J Bus Res 1991;23(1):83–97.

Eisenberger R, Huntington R, Hutchinson S, Sowa D. Perceived organizational support. J Appl Psychol 1986;71(3):500–7.

Eisenberger R, Stinglhamber F, Vandenberghe C, Sucharski I, Rhodes L. Perceived organizational support: contributions to perceived organizational support and employee retention. J Appl Psychol 2002;87(4):698–714.

Endler N. Evolution of personality construct in marketing and its application to contemporary personality research. J Consum Res 1997;6(1):55–66.

Falk RF, Miller NB. A Primer for Soft Modeling. Akron, OH: University of Akron Press; 1992. p. 103. xiv.

Fishbein M, Ajzen I. Belief, attitude, intention and behavior: an introduction to theory and research. Reading, MA: Addison-Wesley; 1975.

Fornell C, Bookstein F. Two structural equation models: Lisrel and Pls applied to consumer exit-voice theory. J Mark Res 1982;19(1):440–52.

Fornell C, Larcker D. Evaluating structural equation models with unobservable variables and measurement error. J Mark Res 1981;18(1):39–50.

Fu JR, Farn CK, Chao WP. Acceptance of electronic tax filing: a study of taxpayer intentions. Inf Manag 2006;43(1):109–26.

Funder D. Global traits: a Neo-Allportian approach to personality. Psychol Sci 1991;2(1):31–9.

Furnell P, Gennatou M, Dowland P. A prototype tool for information security awareness and training. Logist Inf Manag 2002;15(6):352–7.

Furnell S, Bryant P, Phippen A. Assessing the security perceptions of personal internet users. Comput Secur 2007;26(5):410–7.

Gefen D, Straub DW. The relative importance of perceived ease of use in IS adoption: a study of e-commerce adoption. J Assoc Inf Syst 2000;1(8):1–30.

Gefen D, Straub D, Boudreau M. Structural equation modeling techniques and regression: guidelines for research practice. Commun AIS 2000;7(7):1–78.

Gefen D, Karahanna E, Straub D. Trust and tam in online shopping: an integrated model. MIS Q 2003;27(1):51–90.

Geller E, Wiegand D. People-based safety: exploring the role of personality in injury prevention. Prof Saf 2005;14(12):28–36.

Goldberg L. The development of markers for the big-five factor structure. Psychol Assess 1992;4(1):26–41.

Gollwitzer PM. The volitional benefits of planning. In: Gollwitzer PM, Bargh JA, editors. The psychology of action: linking cognition and motivation to behavior. New York: Guilford; 1996. p. 287–312.

Gountas J, Gountas S. Personality orientations, emotional states, customer satisfaction, and intention to repurchase. J Bus Res 2007;60(1):72–5.

Greene G, D'Arcy J. Assessing the impact of security culture and the employee-organization relationship on IS security compliance. In: Proceedings of the fifth annual symposium on information assurance, Albany, NY; 2010.

Guo KH, Yuan Y, Archer NP, Connelly CE. Understanding nonmalicious security violations in the workplace: a composite behavior model. J Manag Inf Syst 2011;28(2):203–36.

Han X, Kwortnik Jr JR, Wang C. Service loyalty: An integrative model and examination across service contexts. J Serv Res 2008;11(1):22–42.

Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organizations. Eur J Inf Syst 2009;18(2):106–25.

Hirschheim R. Introduction to the special issue on Quo Vadis Tam – issues and reflections on technology acceptance research. J Assoc Inf Syst 2007;8(4):204–5.

Hu Q, Dinev T, Hart P, Cooke D. Top management championship and individual behavior towards information security: an integrative model. In: Proceedings of the 16th European conference on information systems, Galway, Ireland, 54; 2008. p. 1–13.

Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput Secur 2012;31(1):83–95.

Ilies R, Scott B, Judge T. The interactive effects of personality traits and experienced States on intraindividual patterns of citizenship behavior. Acad Manag J 2006;49(3):561–75.

James L, Mazerolle M. Personality in work organizations. Thousand Oaks, California: Sage Publications; 2002.

Jarvis C, Mackenzie S, Podsakoff P, Mick D. A critical review of construct indicators and measurement model misspecification in marketing and consumer research. J Consum Res 2003;30(2):199–218.

John O, Srivastava S. The big five trait taxonomy. In: Pervin, John, editors. Handbook of personality theory and research. New York, NY: The Guilford Press; 1999.

Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS Q 2010;34(3):549–66.

Kajzer M, D'Arcy J, Crowell CR, Striegel A, Bruggen DV. An exploratory investigation of message-person congruence in information security awareness campaigns. Comput Secur 2014;43:64–76.

Karahanna E, Straub D, Chervany N. Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. MIS Q 1999;23(2):183–212.

Karahanna E, Agarwal R, Angst C. Reconceptualizing compatibility beliefs in technology acceptance research. MIS Q 2006;30(4):781–804.

Karim NSA, Zamzuri NHA, Nor YM. Exploring the relationship between internet ethics in university students and the big five model of personality. Comput Educ 2009;53(1):86–93.

Klein G, Jiang J, Tesch D. Wanted: project teams with a blend of is professional orientations. Commun ACM 2002;45(6):81–7.

Konovsky MA, Organ DW. Dispositional and contextual determinants of organizational citizenship behavior. J Organ Behav 1996;17(3):253–66.

Korzaan ML, Boswell KT. The influence of personality traits and information privacy concerns on behavioral intentions. J Comput Inf Syst 2008;48(4):15–24.

Lee Y, Kozar K. An empirical investigation of anti-spyware software adoption: a multitheoretical perspective. Inf Manag 2008;45(2):109–19.

Li Y, Tan CH, Teo HH, Tan BC. Innovative usage of information technology in Singapore organizations: do CIO characteristics make a difference? Eng Manag IEEE Trans 2006;53(2):177–90.

Limayem M, Hirt SG, Cheung CM. How habit limits the predictive power of intention: the case of information systems continuance. MIS Q 2007;31(4):705–37.

Lu J, Yao JE, Yu CS. Personal innovativeness, social influences and adoption of wireless internet services via mobile technology. J Strateg Inf Syst 2005;14(3):245–68.

Mackenzie S, Podsakoff P, Jarvis C. The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions. J Appl Psychol 2005;90(4):710–30.

Mahmood MA, Siponen M, Straub D, Rao HR, Raghu TS. Moving toward black hat research in information systems security: an editorial introduction to the special issue. MIS Q 2010;34(3):431–3.

Manstead AS, Parker D. Evaluating and extending the theory of planned behavior. Eur Rev Soc Psychol 1995;6(1):69–95.

Mazhelis O, Puuronen S. A framework for behavior-based detection of user substitution in a mobile context. Comput Secur 2007;26(2):154–76.

McCrae RR, John OP. An introduction to the five-factor model and its applications. J Personal 1992;60(2):175–215.

McGrath J. Dilemmatics: the study of research choices and dilemmas. In: McGrath J, Martin J, Kulka R, editors. Judgment calls in research. Beverly Hills, CA: Sage Publications; 1981. p. 69–103.

Meyerowitz B, Chaiken S. The effect of message framing on breast self examination attitudes, intentions and behavior. J Personal Soc Psychol 1987;52(3):500–10.

Milne S, Sheeran P, Orbell S. Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory. J Appl Soc Psychol 2000;30(1):106–43.

Mowen J, Park S, Zablah A. Towards a theory of motivation and personality with application to word-of-mouth communications. J Bus Res 2007;60(6):590–6.

Norman P, Sheeran P, Orbell S. Does state versus action orientation moderate the intention-behavior relationship? J Appl Soc Psychol 2003;33(3):536–53.

O'Brien TB, DeLongis A. The interactional context of problem-, emotion-, and relationship-focused coping: the role of the big five personality factors. J Personal 1996;64(4):775–813.

Organ DW, Paine JB. A new kind of performance for industrial and organizational psychology: recent contributions to the study of organizational citizenship behavior. Int Rev Ind Organ Psychol 1999;14:337–68.

Ouellette JA, Wood W. Habit and intention in everyday life: the multiple processes by which past behavior predicts future behavior. Psychol Bull 1998;124(1):54–74.

Paulin M, Ferguson R, Bergeron J. Service climate and organizational commitment: the importance of customer linkages. J Bus Res 2006;59(8):906–15.

Peele H. Reciprocating perceived organizational support through citizenship behaviors. J Manag Issues 2007;19(4):554–75.

Pemberton A, Pemberton J, Williamson J, Lounsbury J. Rim professionals: a distinct personality? Inf Manag J 2005;39(5):54–60.

Petter S, Straub D, Rai A. Specifying formative constructs in information systems research. MIS Q 2007;31(4):623–56.

Pfleeger SL, Caputo DD. Leveraging behavioral science to mitigate cyber security risk. Comput Secur 2012;31(4):597–611.

Podsakoff PM, MacKenzie SB, Paine JB, Bachrach DG. Organizational citizenship behaviors: a critical review of the theoretical and empirical literature and suggestions for future research. J Manag 2000;26(3):513–63.

Posey C, Bennett RJ, Roberts TL. Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes. Comput Secur 2011;30(6):486–97.

Reid M, Riemenschneider C, Allen M, Armstrong D. Information technology employees in state government: a study of affective organizational commitment, job involvement, and job satisfaction. Am Rev Public Adm 2008;38(1):41–61.

Rhee HS, Kim C, Ryu YU. Self-efficacy in information security: its influence on end users' information security practice behavior. Comput Secur 2009;28(8):816–26.

Rhoades L, Eisenberger R. Perceived organizational support: a review of the literature. J Appl Psychol 2002;87(4):698–714.

Rhodes RE, Courneya KS. Investigating multiple components of attitude, subjective norm, and perceived control: an examination of the theory of planned behaviour in the exercise domain. Br J Soc Psychol 2003;42(1):129–46.

Ringle C, Wende C, Will W. Smartpls 2.0. 2005. from, www.smartpls.de.

Rogelberg SG. The encyclopedia of industrial and organizational psychology, vol. 2. Thousand Oaks, California: Sage Publishing; 2006.

Rosenthal D. Intrusion detection technology: leveraging the organization's security posture. Inf Syst Manag 2002;19(1):35–44.

Settoon RP, Nathan B, Robert CL. Social exchange in organizations: Perceived organizational support, leader–member exchange, and employee reciprocity. J Appl Psychol 1996;81(3):219–27.

Sharma S, Crossler RE. Disclosing too much? Situational factors affecting information disclosure in social commerce environment. Electron Commer Res Appl 2014;13(5):305–19.

Shropshire J, Warkentin M, Johnston A, Schmidt M. Personality and IT security: an application of the five-factor model. In: Proceedings of the twelfth Americas conference on information systems Acapulco, Mexico; 2006. p. 3443–9.

Siponen M. Five dimensions of information security awareness. Comput Soc 2001;31(2):24–9.

Sparks P, Guthrie CA. Self-Identity and the theory of planned behavior: a useful addition or an unhelpful artifice? J Appl Soc Psychol 1998;28(15):1393–410.

Stanton J, Stam K, Guzman I, Caldera C. Examining the linkage between organizational commitment and information security. In: Proceedings of the 2003 IEEE systems, man, and cybernetics conference, Washington, DC; 2003.

Straub ET. Understanding technology adoption: theory and future direction for informal learning. Rev Educ Res 2009;70(2):625–49.

Straub D, Boudreau M, Gefen D. Validation guidelines for is positivist research. Commun AIS 2004;13(1):380–427.

Triandis HC. Interpersonal behavior. Monterey, CA: Brooks/Cole Publishing Company; 1977.

van der Pligt J, De Vries NK. Expectancy-value models of health behaviour: the role of salience and anticipated affect. Psychol Health 1998;13(2):289–305.

Vance A, Sippenon M, Pahnila S. How personality and habit affect protection motivation. In: Workshop on information security and privacy, Phoenix AZ; 2009.

Venkatesh V, Bala H. Technology acceptance model 3 and a research agenda on interventions. Decis Sci 2008;39(2):273–315.

Venkatesh V, Davis F. A theoretical extension of the technology acceptance model: four longitudinal field studies. Manag Sci 2000;46(2):186–204.

Venkatesh V, Morris M, Davis G, Davis F. User acceptance of information technology: toward a unified view. MIS Q 2003;27(3). 424–478.

Venkatesh V, Davis F, Morris M, Michael G. Dead or alive? The development, trajectory and future of technology adoption research. J Assoc Inf Syst 2007;8(4):268–86.

Vroom C, Solms RV. Towards information security behavioural compliance. Comput Secur 2004;23(3):191–8.

Wang W, Benbasat I. Trust in and adoption of online recommendation agents. J Assoc Inf Syst 2007;6(3):72–101.

Wansink B, Sobal J. Mindless eating the 200 daily food decisions we overlook. Environ Behav 2007;39(1):106–23.

Warkentin M, Willison R. Behavioral and policy issues in information systems security: the insider threat. Eur J Inf Syst 2009;18(2):101–5.

Warkentin M, Davis K, Bekkering E. Introducing the check-off password system (COPS): an advancement in user authentication methods and information security. J End User Comput 2004;16(3):41–58.

Warkentin M, McBride M, Carter L, Johnston A. The role of individual characteristics on insider abuse intentions. Proc Am Conf Inf Syst 2012a;28:1–10.

Warkentin M, Sharma S, Gefen D, Pavlou P, Rose G. Government of the people, by the people: A look at trust in eGovernment. In: Proceedings of the 18th Americas conference on information systems, Seattle, Washington; August 9, 2012. Paper 20.

Warkentin M, Straub D, Malimage K. Featured talk: measuring secure behavior: a research commentary. In: Proceedings of the annual symposium, Alabany, NY; 2012. p. 1–8.

Watson D, Hubbard B. Adaptational style and dispositional structure: coping in the context of the five-factor model. J Personal 1996;64(4):737–74.

Whitman M. Enemy at the gates: threats to information security. Commun ACM 2003;46(8):91–5.

Willison R, Warkentin M. Beyond deterrence: an expanded view of employee computer abuse. Manag Inf Syst Q 2013;37(1):1–20.

Wong JK, Sheth JN. Explaining intention-behavior discrepancy: a paradigm. Adv Consumer Res 1985;12(1):378–84.

Woon I, Tan G, Low R. A protection motivation theory approach to home wireless security. In: Proceedings of the twenty-sixth international conference on information systems, Las Vegas; 2005. p. 367–80.

Zhang X, Prybutok V, Strutton D. Modeling influence on impulse purchasing behaviors during online marketing transactions. J Mark Theory Pract 2007;15(1):79–89.

Zimbardo PG, Boyd JN. Putting time in perspective: a valid, reliable individual-differences metric 1999;77(6):1271–88.

Jordan Shropshire is an Associate Professor of CIS at the University of South Alabama. His research focuses on the technical and behavioral aspects of cyber security. His work is currently funded by the National Science Foundation. Dr. Shropshire writes articles and delivers presentations for the academic and IT professional communities. He has served as associate editor or reviewer for publications such as *MIS Quarterly*, *Decision Support Systems*, *Information Systems Research*, and various ACM and IEEE Transactions. Dr. Shropshire completed his PhD in MIS at Mississippi State University and his undergraduate degree in business at the University of Florida.

Merrill Warkentin is Professor and the Drew Allen Endowed Fellow in the College of Business at Mississippi State University. His research has appeared in MIS Quarterly, Decision Sciences, European Journal of Information Systems, Decision Support Systems, Computers & Security, Information Systems Journal, and others. He is the AIS Departmental Editor for IS Security & Privacy, the Chair of the IFIP Working Group on IS Security Research, and Track Co-Chair for the ICIS 2013 Security Track. His primary research focus is in behavioral IS security issues. He is an AE for *MIS Quarterly*, *Decision Sciences*, *European Journal of Information Systems*, and *Information & Management*.

Shwadhin Sharma is a PhD student in the College of Business at Mississippi State University. His primary research interest is in social media, information security behaviors, and research methods. He has presented his research at several academic conferences.