Journal of International Technology and Information Management

Manuscript 1588

Does Personality Traits and Security Habits Influence Security of Personal Identification Numbers? The Context of Mobile Money Services in Tanzania.

Daniel Ntabagi Koloseni

Does Personality Traits and Security Habits Influence Security of Personal Identification Numbers? The Context of Mobile Money Services in Tanzania

Daniel Ntabagi Koloseni
(*The Institute of Finance Management, Tanzania*)

ABSTRACT

Security is an important ingredient in financial transactions; as such, it is imperative that attention should be paid to enhancing the security habits and user behaviours of mobile payment services. Establishing a link between security habits, personality characteristics, and security behaviours provides a new dimension to studying security behaviours regarding mobile money services. Therefore, this study investigates how personality traits affect security behaviours and habits and how security habits mediate the link between personality traits and PIN security practices. The study found that conscientiousness, openness to experience, extroversion and security habits influence PIN security practices, while conscientiousness, agreeableness, and neuroticism influence security habits. Further, the study found security habits mediate the relationships between conscientiousness, agreeableness, neuroticism and PIN security practices. The study has managerial consequences for the players in the mobile money services domain in addition to its theoretical ramifications.

Keywords: Personality traits, Security habits, Mobile Money Services, PIN codes, Mediation effects

ISSN: 1941-6679-On-line Copy

INTRODUCTION

The world, in general, and the financial sector, in particular, has recently witnessed an increase in the number of information security incidences(Anderson *et al*., 2019; Kovalchuk *et al*., 2021). The economic losses and psychological anguish caused by these incidences are massive to society, individuals, and organizations. These incidents are primarily caused by the failure of users of financial information systems to abide by acceptable information security practices, among other factors (Parsons et al., 2014). It is well documented that simple security habits such as using a strong password, changing passwords regularly, using up-to-date software, regular back up and using anti-malware (Hong & Furnell, 2021; Zwilling *et al*., 2022) could massively reduce information system vulnerabilities, thus shielding the information system from attacks.

Personal Information Number (PIN) is a dominant approach for authenticating users in mobile money transactions. Unfortunately, the current security design in mobile money services and apps does not address many aspects of PIN management. For instance, many mobile money systems do not force users to change their PIN after a specified time. Also, most mobile money service systems do not encipher the PIN codes when keyed into the smartphone, making the shoulder surfing attack plausible. Therefore, the responsibility to secure the PIN codes lies on the shoulders of the user. In smartphones, PIN codes are securely stored in the hardware circuit called the secure element (Ogata et al., 2020; Reveilhac & Pasquet, 2009). PIN codes can be stolen and used to commit financial fraud, including phishing, farming, smishing, vishing, and shoulder surfing (Pathak et al., 2015). These attacks can be prevented by adopting acceptable security practices (Jamil et al., 2018; Shankhwar et al., 2020). Users should be security aware and develop security habits to counter these attacks. Security habit is an influential factor in several security behaviours, as illustrated in (Hong & Furnell, 2021 Koloseni *et al*., 2019; Nord *et al*., 2020; Zhang *et al*., 2023). Developing security habits is essential to users as it will enable them to practice security behaviour effortlessly and automatically. Security habit has been largely studied as a direct predictor of security behaviours in previous studies(Koloseni, 2017; Pahnila *et al*., 2007; Vance *et al*., 2012). However, the mediation and moderating effects of security habits on the practice of security behaviour have received less academic attention. This study focuses on the mediation effects. Habit has been illustrated as a mediator of human behaviours in different contexts. For example, it has been proven to mediate self-control and positive life outcomes in nighttime mobile phone use and well-being indicators (Galla & Duckworth, 2015; Urrila et al., 2017; Vernon et al., 2018).

ISSN: 1941-6679-On-line Copy

Human behaviours are closely linked with personal characteristics (Ajzen, 2005). Several research studies have been conducted to validate this link using the big five-factor model (FFM). For instance, prominently, the model has been utilized in research to assess threats and security of context-aware applications, security policy compliance, individual differences in cyber security behaviours, and smartphone security measures (Bouhnik *et al*., 2021; Condori-Fernandez *et al*., 2021; Padayachee, 2022; Power & Bello, 2022; Shropshire *et al*., 2006) to mention a few. However, the model has not been used to investigate individual PIN code security practices in mobile money services. The PIN codes' security concept, coupled with the mediation effects of personality traits and security habits in the context of mobile money services, is distinctive and, therefore, adds value to the field of information security. Against this backdrop, this study addresses the scant research on the mediation effects of security habits and the influence of personality traits on PIN code management among mobile money users.

LITERATURE REVIEW

Personality Traits and Human Behaviour

Empirical results from human psychology research have confirmed the relationships between personality traits and human behaviours when interacting with each other, systems or the environment (Changchit *et al*., 2022; Hinds & Joinson, 2019; Volk *et al*., 2020). Even though there are numerous personality characteristics, FFM evolved into a superior model for studying personality (Chang et al., 2012; Shropshire et al., 2006). The model comprises conscientiousness, agreeableness, neuroticism, openness, and extraversion as its core determinant factors (Goldberg, 1993; Widiger & Trull, 1997). In connection to information security behaviours, these traits have been demonstrated to correlate with security behaviours as reported by (Bawack *et al*., 2021, Gratian *et al*., 2018; Junglas *et al*., 2008; Pattinson *et al*., 2012; Peng & Dutta, 2022; Tang *et al*., 2020). However, the information systems literature has rarely looked into the relationship between these attributes and habits.

Habits are part and parcel of the personality development process (McCloskey & Johnson, 2021). Previous studies have indicated that the FFM influence individual habits (Kuijpers et al., 2019; Pfeiler & Egloff, 2020; Yazdanpanah & Hosseinlou, 2017), such that a person's patterns of emotion, behaviors, or thoughts impact habit formation.

ISSN: 1941-6679-On-line Copy

Theoretical Framework and Hypotheses

This study employs personality characteristics and security habits as the backbone of the theoretical framework. The theoretical framework depicts how security habits mediate the hypothetical relationships between the FFM on the intention to adopt PIN code security practices and the direct impacts of the FFM on the desire to adopt PIN code security, as shown in Figure 1.

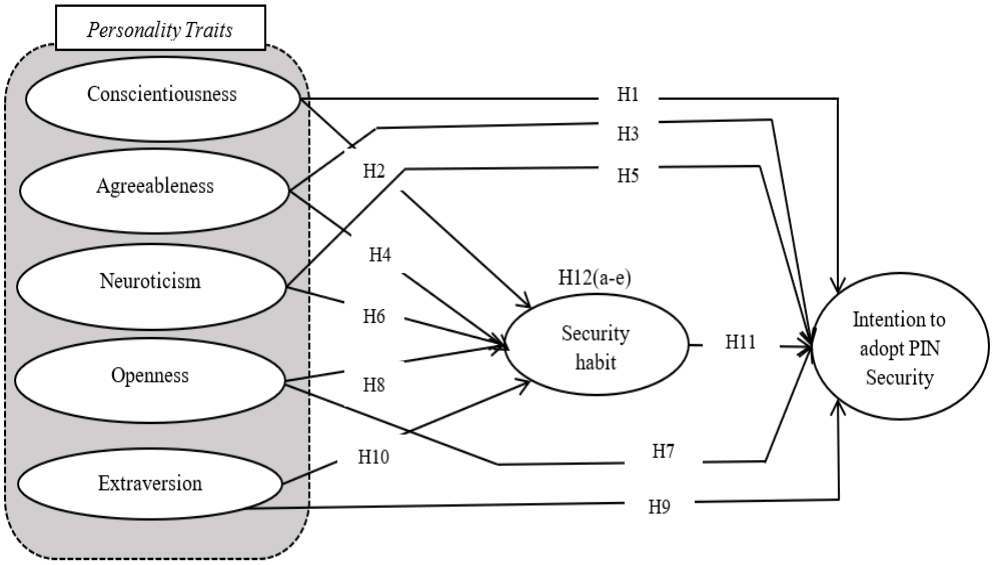

Figure 1. The Research Model

Individual conscientiousness describes the degree to which someone indicates probable care and feels responsible for protecting the interest of others (Costa Jr & McCrae, 2008; John & Srivastava, 1999). A high inclination to conscientiousness suggests an individual's awareness, self-control, and the tendency to take others' interests with dignity and responsibly (Goldberg, 1990). Because of these characteristics, they tend to act in a manner that could protect and shield others from danger. Further, conscientious individuals are highly motivated and likely to persist longer at a task than others (Sansone et al., 1999). In relation to the information security domain, conscientious individuals are characteristically motivated to practice information security behaviour repeatedly as long as this behaviour will impact the well-being of others. It is anticipated that a person high with conscientiousness is likely to develop a habit of regularly practising acceptable information security behaviours because of the tendency to avoid risky behaviours and the possession of an inner desire to protect others.

ISSN: 1941-6679-On-line Copy

Hence the hypotheses:

H1: Conscientiousness positively influences the intention to adopt PIN security practices.
H2: Conscientiousness positively influences security habits.

Agreeableness indicates an individual's readiness to interact and collaborate with others, sympathy, and eagerness to help them (Costa Jr & McCrae, 2008). An individual with this personality is ready to compromise their interests for the sake of creating harmony among parties involved in a given context (Lim *et al*., 2023). Agreeableness is for shaping social attitudes, philosophy of life and habits in general (Bosnjak *et al*., 2007; Costa Jr *et al*., 1991). It is expected that highly agreeable individuals pay little attention to appraising information security. This relationship has also been empirically confirmed by (Junglas et al., 2008; Matt & Peckelsen, 2016) in the context of privacy-protective behaviour. Some evidence indicates that agreeableness may be related to specific habits. One study found that agreeable individuals have more positive health habits, including eating a healthy diet and involving in regular bodily exercise (Intiful et al., 2019). Cooperativeness and consideration of agreeable individuals may translate into security practices relating to PIN security.

Hence the hypothesis:

H3: Agreeableness positively influence the intention to adopt PIN security practices.
H4: Agreeableness positively influence security habits.

Neurotic individuals are depressed, impulsive, tense and generally emotionally unstable (Goldberg, 1993; John & Srivastava, 1999). Also, they tend to experience more threats and anxieties as compared to emotionally stable individuals (Goldberg, 1990). Thus, individuals with neuroticism are likely to participate in actions that can help to avoid falling victim to cyber-attacks. Accordingly, previous research has shown that neurotic individuals are positively associated with acceptable information security behaviours such as (Peng & Dutta, 2022) and (Škrinjarić et al., 2018). Additionally, previous studies indicated that neuroticism is associated with various health and computer-related behaviours and habits. For instance, Cao and Su (2007) and Donnellan *et al*. (2000) found that neuroticism is linked to internet addiction. Reasonably, neuroticism increases the likelihood of engaging in habitual security practices. Hence, the hypothesis:

H5: Neuroticism positively influences the intention to adopt PIN security practices.
H6: Neuroticism positively influences security habits.

Curiosity, readiness to explore new things, imagination, and intelligence are common traits of individuals who are open to experience (John & Srivastava, 1999). Based on these characteristics, these individuals have a more profound sense of awareness resulting from exposure to a variety of learning environments and contexts (Junglas et al., 2008). These individuals are, therefore, likely to embrace security and adopt information security measures when using information systems. Junglas *et al*. (2008) argue that people who exhibit openness to experience are likely to evaluate security threats. On the same note, curiosity and an open mind are avenues for developing habits. Thus, open-minded people tend to form good information security habits. Further, these traits have links with e-mail habits, as illustrated by (Vishwanath et al., 2015). Hence, the study hypothesizes that:

H7: Openness to experience positively influences the intention to adopt PIN security practices.
H8: Openness positively influences security habits.

Extraversion is a personality trait characterized by an outgoing and social nature, while habit is a term used to describe a pattern of behaviour that happens frequently and often unconsciously(Verplanken & Aarts, 1999). The proclivity to riskier behaviour is higher in extroverts than in their counterparts because of their need for excitement (Goldberg, 1993). As such, they are likely to delve into improper riskier behaviours, such as ignoring the advice to cover PIN when using mobile gadgets to make payments and repeatedly avoiding exercising security habits, as long as these actions may not impact their relationship with others. There is proof to support the links between extraversion and habit. Lucas and Baird (2004) revealed that people who scored high on extraversion were inclined to participate in physical activity regularly, which suggests that they may have developed a habit of exercising.
Additionally, a study conducted by Hughes *et al*. (2012) found that a person who scored high on extraversion was more inclined to engage in the habit of using the Internet for social services and Twitter and Facebook frequently. This implies that extroverts are also likely to engage in security-related habits positively or negatively based on optimism, enthusiasm, affection, and social nature traits they possess. Hence the hypothesis:

H9: Extraversion influences the intention to adopt PIN security practices.
H10: Extraversion influences security habits.

Habits are defined as automaticity in performing a particular action or behaviour (Verplanken & Aarts, 1999). Habits are recurring, habitual security behaviors that people engage in when dealing with information systems. The role of security habits in information systems has been thoroughly investigated in the IS literature. For instance, security habits have been confirmed to impact the desire to adhere to security policy (Nord, 2020; Pahnila *et al*., 2007; Vance *et al*., 2012) and to adopt cyber security behaviours (Koloseni, 2017; Tsai *et al*., 2016). Using findings from earlier studies as support, this makes the following hypothesis:

H11: Security habits positively influence the intention to adopt PIN security practices.

Since personality traits influence the intention to adopt PIN code security practices and security habits and, in turn, security habits could influence the intention to adopt PIN security practices, it means security habits have mediating effects. Based on the argument, personality traits could indirectly impact the intention to adopt PIN security practices through the security habits construct. Therefore, the hypotheses:

H12a: The relationship between conscientiousness and the intention to adopt PIN security is mediated by security habits.
H12b: The relationship between agreement and the intention to adopt PIN security is mediated by security habits.
H12c: The relationship between neuroticism and the intention to adopt PIN security is mediated by security habits.
H12d: Security habits mediate the relationship between openness and the intention to adopt PIN security.
H12e: Security habits mediate the relationship between extroversion and the intention to adopt PIN security.

METHODS

Development of Data Collection Instrument

A questionnaire was utilized to gather information, which was then used to assess the study's hypotheses. The questionnaire was created using verified items from past research. The source of each measurement item is reported in the appendix. The design of the measurement scale is essential in addressing measurement errors. Previous studies have indicated that design features of the response scale affect how the respondents process the response scale and use it to respond to the questionnaire (Stefkovics, 2022; Yan et al., 2018). To reduce the possibility of potential measurement errors borne out of questionnaire design issues, all measurement

items used in this study employed previously validated interval scales with the same direction, similar to the previous studies. However, modifications were made in the constructs of security habits and the intention to adopt PIN security to contextualize the measurement items to reflect the focus of the study.

Subjects, Sampling, and Data Collection Procedures

The respondents were selected using a purposeful sampling approach to ensure only respondents with experience in mobile money services were included in the study, and the data collected reflected the situation under study. In total, 600 questionnaires were disseminated between September 2022 and February 2023, and 434 responses were received, indicating a response rate of 72.3%. Prior to data processing, the questionnaires that were collected were checked for missing data. Fifty-one (51) questionnaires had substantial missing information and were thus discarded. As a result, the subsequent data analysis used 383 valid questionnaires. The questionnaires were created in two languages, Kiswahili and English. The majority of the study population uses these two languages. An approved linguist performed the translation between the two languages to ensure that information was not distorted. Additionally, two experts from the information systems domain (IS) verified the translated questionnaire's content. Table 1 lists the respondents' demographic characteristics.

Table 1. Profile of respondents' demographics

Variable	***Category***	***Frequency***	***Percentage (%)***
Gender	Male	209	54.6
	Female	174	45.4
Educational level	Informal Education	12	3.1
	Primary	25	6.5
	Secondary	74	19.3
	Diploma	83	21.7
	Bachelor	127	33.2
	Masters	53	13.8
	PhD	9	2.3
Experience in Using Computer/ Smartphones/ATM	Less than one Year	73	19.1
	2 -5 Years	109	28.5
	Above 5 Years	201	52.5

RESULTS

The structural equation modelling (SEM) technique was applied to examine the connections between variables. Smart PLS4, a partial least squares (PLS)-based SEM program, was employed for the task. The assessment of the measurement model was accomplished first, followed by the evaluation of the structural model as per Anderson and Gerbing's (1988) recommendation. This two-step process is essential since it allows for a more thorough examination of the measurement model, to attain a more rigorous test of the structural model, to improve the precision of the estimates and the ability to detect significant effects (Anderson & Gerbing,1988).

Evaluation of the Measuring Model

The reliability was determined by gauging the internal consistency of the individual indicators of each construct. Cronbach's alpha and composite reliability were used for that purpose. The Cronbach's alpha and composite reliability values are equivalent to or above 0.70, indicating that the reliability has been attained (Cronbach, 1970). The results show that indicators of the constructs are trustworthy because both Cronbach's alpha and composite reliability ratings are higher than 0.70. Table 2 presents the reliability assessment's findings.

Table 2. Indictor's Reliability Assessment

Construct	Cronbach's alpha	Composite reliability	AVE
AG	0.855	0.857	0.698
CONS	0.810	0.814	0.725
EXV	0.841	0.844	0.676
NEU	0.877	0.890	0.731
OPE	0.868	0.871	0.792
PSP	0.863	0.864	0.709
SHA	0.897	0.900	0.764

Key

AG:	Agreeableness	EXV:	Extraversion	NEU: Neuroticism	OPE: Openness
SHA	Security Habits	CONS	Conscientiousness	PSP:	PIN Security Practices

Both discriminant validity and convergent validity were evaluated to determine the validity of the measuring items. Convergent validity is an indication of whether an indicator is related to other indicators that it should be related to. To evaluate convergent validity, the study examined the AVE. Hair *et al.* (2010) stated that the

ISSN: 1941-6679-On-line Copy

appropriate threshold values for AVE are equal to or above 0.50. The findings demonstrated that AVEs for all constructs were above 0.50, as shown in Table 3, suggesting that convergent validity has been achieved satisfactorily.

Table 3. Average Value Extracted Results

Construct	The average variance extracted (AVE)
AG	0.698
CONS	0.725
EXV	0.676
NEU	0.731
OPE	0.792
PSP	0.709
SHA	0.764

Heterotrait Monotrait (HTMT) ratios and the indictor's cross-loadings were primarily used to assess the construct's discriminant validity. Cross loadings indicate that factor loadings for all indicators exceed all of their respective cross-loadings, supporting the fact that discriminant validity has been demonstrated (Hair *et al*., 2015), as indicated in Table 4.

Table 4. Constructs Cross Loadings

Construct	*Items/Construct*	*Cross loadings*						
AG	AGR1	0.867						
	AGR2	0.861						
	AGR3	0.859						
	AGR4	0.748						
CONS	CONS1		0.805					
	CONS2		0.897					
	CONS3		0.850					
EXV	EXT1			0.820				
	EXT2			0.838				
	EXT3			0.811				
	EXT4			0.818				
NEU	NE1				0.886			
	NE2				0.894			
	NE3				0.865			
	NE4				0.769			
OPE	OP1					0.876		
	OP2					0.924		
	OP3					0.869		

ISSN: 1941-6679-On-line Copy

PSP	PSP1						0.835	
	PSP2						0.883	
	PSP3						0.855	
	PSP4						0.793	
SHA	SHA1							0.868
	SHA2							0.875
	SHA3							0.882
	SHA4							0.872

The HTMT scores need to be 0.90 or less to establish the discriminant validity (Henseler *et al*., 2015). The study found that HTMT values for all constructs were within the acceptable range, supporting the discriminant validity. Table 5 displays the results of the HTMT ratios of correlations.

Table 5. Results of Discriminant Validity Assessment using HTMT ratios

Construct	AG	CONS	EXV	NEU	OPE	PSP	SHA
AG							
CONS	0.695						
EXV	0.669	0.833					
NEU	0.781	0.857	0.821				
OPE	0.707	0.832	0.825	0.896			
PSP	0.738	0.924	0.849	0.811	0.840		
SHA	0.706	0.767	0.670	0.841	0.683	0.830	

Structural Model Analysis

The following aspects should be taken into consideration as part of the process of evaluating the structural model: explanatory power, model predictive relevance, and significance and path coefficients (Hair *et al*., 2019).

Explanatory Power, Predictive Power and Effect Size

Model explanatory power was evaluated through coefficient of determination (R^2) and predictive power (Q^2). Q^2 estimates the model out of sample predictive power, while R^2 estimates the model on sample explanatory power (Hair *et al*., 2019; Shmueli & Koppius, 2011). Findings indicated that personality attributes accounted for 61.2% of the variation in security habits. The R^2 was estimated when the model was without and with the mediating variable (security habits) to gain insight into its impact in terms of the model's explanatory power. According to the study's findings, the model was able to account for 71.7% (i.e. R^2 of 71.7%) of the variation in the intention to implement PIN code security measures in the absence of security

habits. It accounted for 75% (i.e. R^2 of 75%) of the variation in the intention to adopt PIN security practices. The findings indicate an increase in the model's explanatory power. According to (Henseler et al., 2009), the obtained R^2 values indicate the model explanatory power is moderate and substantial, respectively.

Q^2 in this study was estimated using the *PLSpredict* method (Ringle et al., 2022). According to Hair *et al*. (2019), if a minority of dependent variables indicators have the root means square (RMSE) values higher than the naïve linear model (LM) benchmark, the model has medium predictive power. Hence, *PLSpredict* results reported in Table 6 indicate that the model has medium predictive power. Table 7 indicates the results of the effect sizes. The interpretation of the effect sizes follows the guidelines devised by Cohen (1988), where small, medium, and large effect sizes correspond to f^2 values of at least or equal to 0.02, 0.15, and 0.35, respectively.

Table 6. PLS Predict results

Indicators			PLS-SEM		Linear Model Benchmark	
		Q^2predict	RMSE	MAE	RMSE	MAE
PIN Security Behaviors	PSP1	0.481	0.841	0.618	0.836	0.617
	PSP2	0.564	0.745	0.571	0.720	0.514
	PSP3	0.483	0.847	0.656	0.877	0.669
	PSP4	0.420	0.863	0.643	0.940	0.709
Security Habits	SHA1	0.391	0.878	0.638	0.931	0.688
	SHA2	0.349	0.916	0.650	0.988	0.695
	SHA3	0.435	0.791	0.572	0.858	0.624
	SHA4	0.547	0.724	0.513	0.715	0.513

Table 7. Effect Sizes

Constructs	PIN Security Practices	Security Habits
AG	0.024	0.038
CONS	0.149	0.042
EXV	0.073	0.001
NEU	0.017	0.199
OPE	0.053	0.004
SHA	0.146	

***Note**: PSP is an endogenous construct*

Important Map Analysis (IPMA)

IPMA enables pinpointing the areas where managerial or practical intervention is necessary. To put it another way, one could spot important areas yet perform poorly and adopt the appropriate management tools to make improvements. IPMA results indicate that the most important construct is conscientiousness (0.379). In terms of performance, the construct with the highest performance is agreeableness (68.483). Based on these findings, managerial interventions should be extended to conscientious individuals to enhance their intention to practice PIN code security behaviours. Notably, the level of importance did not match the level of performance for this construct. Table 8 displays the IPMA's results in tabular form, while Figure 2 displays them in graph form.

Table 8. IPMA Results for intention to practice PIN security behaviours

Endogenous Construct	***Constructs***	***Importance (Total Effects)***	***Performance (Index Value)***
PIN Security Behaviours	Agreeableness	0.165	**68.483**
	Conscientiousness	**0.379**	57.028
	Extraversion	0.222	65.428
	Neuroticism	0.025	61.134
	Openness	0.182	55.822
	Security Habit	0.306	64.43

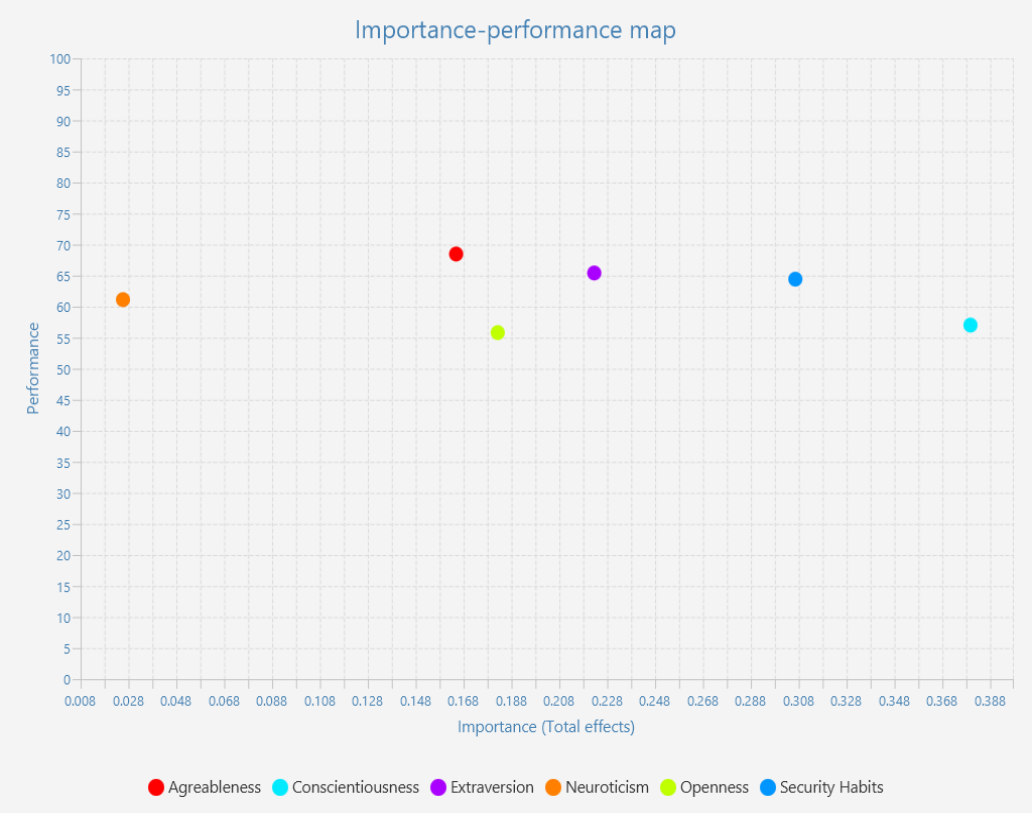

Figure 2. IPMA results for the endogenous construct for intention to practice PIN security behaviours

Assessment of the Path Coefficients

The significance level, as represented by the *p*-values, *t*-values, and path coefficient values (β), was considered while evaluating the path coefficients. Out of the eleven hypothetical relationships, seven (7) were supported. Specifically, the study found that conscientiousness influences both PIN code security practices (*H1*) and security habits *(H2)*, and agreeableness influences security habits (*H4*). Further, the study found that neuroticism influences security habits *(H6)*, openness has an influence on PIN code security practices (*H7*), extraversion has an impact on PIN code security practices *(H9)*, and PIN code security habits have an influence on PIN code security practices *(H11)*. On the contrary, the study found that agreeableness *(H3)* and neuroticism *(H5)* do not influence PIN code security practices, while openness *(H8)* and extroversion *(H10)* do not influence PIN code security habits. Table 9 and Figure 3 display the findings of the hypothesis testing.

Table 9. Direct Relationships Results

Hypotheses and Paths				*β*	*t- values*	*p-values*	*Remarks*
H1	CONS	⟶	PSP	0.079	3.998	0.000	Supported
H2	CONS	⟶	SHA	0.093	2.201	0.028	Supported
H3	AG	⟶	PSP	0.061	1.838	0.066	Not Supported
H4	AG	⟶	SHA	0.084	2.048	0.041	Supported
H5	NEU	⟶	PSP	0.082	1.647	0.100	Not Supported
H6	NEU	⟶	SHA	0.118	4.409	0.000	Supported
H7	OPE	⟶	PSP	0.072	2.815	0.005	Supported
H8	OPE	⟶	SHA	0.092	0.712	0.477	Not Supported
H9	EXV	⟶	PSP	-0.067	3.203	0.001	Supported
H10	EXV	⟶	SHA	0.092	0.276	0.783	Not Supported
H11	SHA	⟶	PSP	-0.082	3.751	0.000	Supported

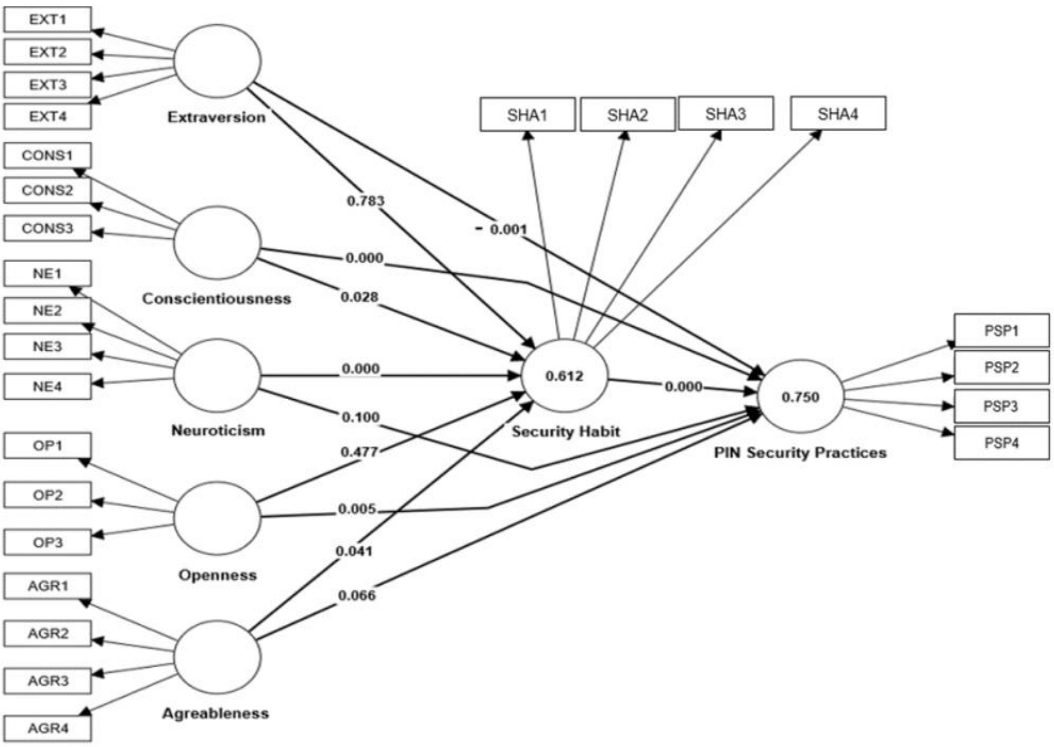

Figure 3. Structural Model with Coefficients

-

Mediation Effects

Out of five hypothesized mediation relationships, three were supported. Notably, the study found that security habits mediate the relationships between conscientiousness, agreeableness, neuroticism and the intention to practice PIN security behaviours donated as H12b, H12c and H12e, respectively. The rest of the mediation relationships were not supported. The results of the mediation effects are reported in Table 10.

Table 10. Hypotheses Testing for the Mediation Relationships.

Hypotheses and Paths						*β*	*t- values*	*p- values*	*Remarks*
H12a	EXV	⟶	SHA	⟶	PSP	0.030	0.260	0.795	Not Supported
H12b	CONS	⟶	SHA	⟶	PSP	0.031	2.002	0.045	Supported
H12c	AG	⟶	SHA	⟶	PSP	0.029	1.993	0.065	Supported
H12d	OPE	⟶	SHA	⟶	PSP	0.031	0.657	0.511	Not Supported
H12e	NEU	⟶	SHA	⟶	PSP	0.059	2.686	0.007	Supported

DISCUSSION

The study examined the roles of personality traits and security habits in the intention to adopt PIN security practices and of information security habit's mediating effects on the association between personality traits and the user's desire to adopt PIN security practices. The study found that conscientiousness influences both security habits and PIN code security practices. This finding is not surprising since conscientious individuals are likely to avoid unsecured behaviour, such as sharing passwords and using unsecured wireless access (Russell et al., 2017). Further, this finding supports (Jiaxin Zhang et al., 2019), who found that conscientious people are motivated to be involved in fine-tuning the user interface to enhance the security of mobile gadgets when accessing mobile money services. Further studies which support these findings include McCormac *et al*. (2017) and Shropshire *et al*. (2015). Moreover, the finding that conscientiousness influences PIN code security practices is particularly noteworthy since PIN codes are a crucial part of protecting sensitive information, such as banking or financial data. The study suggests that people high in conscientiousness are inclined to follow best practices when it comes to creating and using PIN codes, which can help to reduce the risk of unauthorized access.

Findings revealed positive effects of agreeableness on security habits. Agreeable individuals are likely to follow the rules without being monitored (Organ & Paine, 1999) because they are cooperative and considerate (Costa Jr & McCrae, 2008). Moreover, agreeable individuals can learn a habit because they are cooperative and can adhere to acceptable habits or behaviours exercised in society, such as security habits when accessing mobile money services using mobile gadgets. Contrarily, the research revealed that agreeability had no bearing on the intention to engage in PIN security behaviors. This finding suggests that a person's proclivity to collaborate, be mindful of others' feelings, and be sympathetic towards others does not necessarily influence their information security habits. Thus, at least in the context of this study, highly agreeable people may be less inclined to participate in security behaviours. The finding that neuroticism influences security habits suggests that individuals who are more anxious and worrisome tend to exhibit more cautious and security-conscious behaviours to reduce their anxiety and worry about potential security threats (Li et al., 2019). Also, this finding suggests that these individuals engage in secure habits out of anxiety or fear of negative consequences. As a result, they may be more likely to use and protect their PIN when accessing mobile money services by shielding against shoulder sufferers and regularly changing the PIN code, among other security habits. These results are in harmony with (Li et al., 2019), who found that neurotic individuals are extra-sensitive to privacy when using social networks.

Interestingly, the findings indicate that neuroticism does not influence PIN code security practices. The utility of intention diminishes as the strength of habits increases (Neal et al., 2006). In light of this, the significant relationship between neuroticism and security habits has probably oppressed the intention to practice PIN security practices. As a result, this hypothesis turned insignificant.

The study also found that openness and PIN code security practices were associated, indicating that, curious and open to new experiences, individuals may be more enthusiastic about experimenting with new security measures or be more receptive to learning about security best practices. This result validates the research conducted by (Li et al., 2019) (Dreibelbis, 2016), who discovered that open individuals are inclined to practice acceptable security behaviours such as changing passwords regularly and adhering to principles of creating strong passwords. Nevertheless, the study found being flexible, adaptable, creative, curious, and willing to try new things may not necessarily translate into acceptable security habits. As a result, openness does not influence security habits.

ISSN: 1941-6679-On-line Copy

Unsurprisingly, the study found that extraversion significantly impairs an individual's intention to practice PIN security practices. Probably, because extroverts are naturally social and have the tendency to seek out stimulation and excitement, they are likely to participate in risky behaviours, such as sharing private information or employing flimsy passwords, hence compromising the security of their PIN codes. This result contrasts with that of (Gratian *et al.*, 2018), who discovered that extroverts have a strong and positive intention to practice appropriate security behaviours. However, there was no proof of a connection between extraversion and security habits. This finding suggests that an individual's level of extraversion may not necessarily have an impact on their information security habits in relation to PIN code security. The finding that PIN code security habits influence PIN code security practices highlights the importance of cultivating good security habits to ensure the safety of sensitive information. This finding is congruent with (Aigbefo et al., 2022), who observed a similar trend, such that as the strength of the security habits intensifies, the desire to engage in information security increases. This finding suggests that interventions aimed at improving security habits may have a favorable influence on overall PIN code security practices in the mobile payment context.

Regarding mediation relationships, the mediation effect of security habits on the relationship between conscientiousness, agreeableness and neuroticism, and the intention to practice PIN information security behaviours suggest that security habits contribute significantly to understanding the connection between conscientiousness and the desire to partake in information security behaviours. Accordingly, boosting the desire to practice PIN information security behaviours is among the interventions to increase security habits. Because security habits in this instance provided full mediating effects, these interventions are crucial for the mediation relationships between agreeableness and intention to practice PIN information security behaviors and extraversion and intention to practice PIN information security behaviors. Thus, for these two variables to impact the practice of PIN information security behaviours, security habits should play a mediation role.

IMPLICATIONS

Theoretical Implications

The results of this study have significant theoretical and practical ramifications for both academics and practitioners alike. For the theory, this study investigates an area which is underexplored in the information security literature, thus bridging the knowledge gap on information security and the FFM. Additionally, this study has

modelled personality traits as both direct predictors and indirect predictors of security behaviours, whereas security habits play a role as a mediating construct. To the best of the researcher's understanding, this research is the first to examine how the FFM and security habits interact in this fashion. The obtained R^2 is relatively better in comparison with previous studies such as (Junglas *et al.*, 2008; Peng & Dutta, 2022; Shropshire *et al.*, 2015 and Tang *et al.*, 2020), which had integrated personality traits in their model to investigate various information security behaviours. This implies this model could provide an adequate prediction of security behaviours as compared to the previous model in a situation whereby personality traits have been considered. In the absence of security habits as a mediating variable, the model R^2 was 71.7%. After the introduction of security habits as a mediating variable, the R^2 increased to 75 % (an increase of 3.3%). This further justifies the inclusion of security habits as a mediating construct on the links between personality traits and the adoption intention of acceptable PIN security practices.

Practical Implications

Notably, to enhance the PIN code's security during mobile money services, the service providers should focus on extroverts because their tendency to be involved in risky security behaviours, including revealing passwords to others, could negatively impact the security of the PIN codes. Additionally, the study confirmed that security habits mediate the relationships between conscientiousness, agreeableness and neuroticism. Hence, it is also crucial for mobile money service providers to ensure that the security habits of conscientiousness, agreeableness, and neuroticism of individuals are shaped to practice acceptable PIN security behaviours positively. It is crucial to remember that agreeableness and neuroticism initially had no direct impact on the intention to adopt PIN code security practices; instead, their impact became apparent after the security habits were added as a mediator. The resulting proposed model educates practitioners about the significant impact personality factors and security habits have on how PIN security measures are adopted by individuals.

CONCLUSION, LIMITATIONS AND FURTHER STUDIES

The results offer empirical proof of the role of the big five personality traits and security habits in determining an individual's security behaviours in light of mobile money services. Despite the contributions offered by this study, it is without limitations. First, the study was carried out in Tanzania, but it might be replicated in other countries to increase its generalizability. Second, investigations into the moderation and mediation role in the realm of information security are scarce. The

association between personality factors and the adoption of PIN security practices has been investigated in this study to see how security habits may operate as a mediator. To deepen our understanding of personality features in this area, future studies could explore its potential as a moderator of personality traits. Third, future research may examine longitudinal data in addition to the cross-sectional survey data utilized to assess changes in PIN security practices over time.

REFERENCES

Aigbefo, Q. A., Blount, Y., & Marrone, M. (2022). The influence of hardiness and habit on security behaviour intention. *Behaviour and Information Technology*, *41*(6), 1151–1170. https://doi.org/10.1080/0144929X.2020.1856928

Ajzen, I. (2005). *Attitudes, Personality and Behaviour*. McGraw-hill education.

Amichai-Hamburger, Y., & Ben-Artzi, E. (2003). Loneliness and Internet use. *Computers in Human Behavior*, *19*(1), 71–80.

Analytica, O. (2021). African corporates face rising cybercrime risks. *Emerald Expert Briefings*, *oxen-db*.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modelling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*(3), 411.

Anderson, R., Barton, C., Rainer, B., Clayton, R., Ga, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the Changing Cost of Cybercrime. *Workshop on the Economics of Information Security (WEIS)*, 1–32. http://orca.cf.ac.uk/id/eprint/122684

Bosnjak, M., Galesic, M., & Tuten, T. (2007). Personality determinants of online shopping: Explaining online purchase intentions using a hierarchical approach. *Journal of Business Research*, *60*(6), 597–605.

Bouhnik, D., Reich, N., & Aharony, N. (2021). Willingness to information security as a function of personality characteristics and threat assessment among adolescents. *Online Information Review*, *45*(5), 912–929. https://doi.org/10.1108/OIR-06-2020-0218

Cao, F., & Su, L. (2007). Internet addiction among Chinese adolescents: prevalence and psychological features. *Child: Care, Health and Development*, *33*(3), 275–281.

Chang, L., Connelly, B. S., & Geeza, A. A. (2012). Separating Method Factors and Higher Order Traits of the Big Five : A Meta-Analytic Multitrait-Multimethod Approach. *Journal of Personality and Social Psychology*, *102*(2), 408–427.

Changchit, C., Cutshall, R., & Pham, A. (2022). Personality and Demographic Characteristics Influence on Consumers' Social Commerce Preference. *Journal of Computer Information Systems*, *62*(1), 98–108. https://doi.org/10.1080/08874417.2019.1709229

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.). Hillsdale.

Condori-Fernandez, N., Suni-Lopez, F., Muñante, D., & Daneva, M. (2021). How Can Personality Influence Perception on Security of Context-Aware Applications? In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 12812 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-030-79318-0_1

Costa Jr, P. T., & McCrae, R. R. (2008). The Revised Neo Personality Inventory (neo-pi-r). In J. Boyle, G. Matthews, & D. . Saklofske (Eds.), *The SAGE Handbook of Personality Theory and Assessment* (Vol 2, pp. 179–198). Sage Publications, Inc. https://doi.org/https://doi.org/10.4135/9781849200479.n9

Costa Jr, P. T., McCrae, R. R., & Dye, D. A. (1991). Facet scales for agreeableness and conscientiousness: A revision of the NEO Personality Inventory. *Personality and Individual Differences*, *12*(9), 887–898.

Donnellan, M. B., Oswald, F. L., Baird, B. M., & Lucas, R. E. (2006). The Mini-IPIP Scales : Tiny-Yet-Effective Measures of the Big Five Factors of Personality. *Psychological Assessment*, *18*(2), 192–203. https://doi.org/10.1037/1040-3590.18.2.192

Dreibelbis, R. C. (2016). *It's more than just changing your password: Exploring the nature and antecedents of cyber-security behaviors*. University of South Florida.

Galla, B. M., & Duckworth, A. L. (2015). *More Than Resisting Temptation : Beneficial Habits Mediate the Relationship Between Self-Control and Positive Life Outcomes*. *109*(3), 508–525.

Goldberg, L. R. (1990). An alternative" description of personality": the big-five factor structure. *Journal of Personality and Social Psychology*, *59*(6), 1216.

Goldberg, L. R. (1993). The structure of phenotypic personality traits. *American Psychologist*, *48*(1), 26.

Goldberg, L. R. (1999). A broad-bandwidth, public-domain personality inventory measuring the lower-level facets of several five-factor models. *Personality Psychology in Europe*, *7*(1), 7–28.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behaviour intentions. *Computers & Security*, *73*, 345–358.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2015). PLS-SEM : Indeed, a Silver Bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy-related behaviour and personality traits. *Proceedings of the 22nd International Conference on World Wide Web*, 737–744.

Hamburger, Y. A., & Ben-Artzi, E. (2000). Relationship between extraversion and neuroticism and the different uses of the Internet. *Computers in Human Behavior*, *16*(4), 441–449. https://doi.org/10.1016/S0747-5632(00)00017-0

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In *New challenges to international marketing*. Emerald Group Publishing Limited.

Hinds, J., & Joinson, A. (2019). Human and Computer Personality Prediction From Digital Footprints. *Current Directions in Psychological Science*, *28*(2), 204–211. https://doi.org/10.1177/0963721419827849

Hong, Y., & Furnell, S. (2021a). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, *57*, 102710. https://doi.org/10.1016/j.jisa.2020.102710

Hong, Y., & Furnell, S. (2021b). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, *57*, 102710.

Hughes, D. J., Rowe, M., Batey, M., & Lee, A. (2012). A tale of two sites: Twitter vs. Facebook and the personality predictors of social media usage. *Computers in Human Behavior*, *28*(2), 561–569.

Intiful, F. D., Oddam, E. G., Kretchy, I., & Quampah, J. (2019). *Exploring the relationship between the Big five personality characteristics and dietary habits among students in a Ghanaian University*. 1–7.

Jamil, A., Asif, K., Ghulam, Z., Nazir, M. K., Alam, S. M., & Ashraf, R. (2018). Mpmpa: A mitigation and prevention model for social engineering based phishing attacks on Facebook. *2018 IEEE International Conference on Big Data (Big Data)*, 5040–5048.

Jiaxin Zhang, J., Luximon, Y., & Song, Y. (2019). The role of consumers' perceived security, perceived control, interface design features, and conscientiousness in continuous use of mobile payment services. *Sustainability (Switzerland)*, *11*(23). https://doi.org/10.3390/su11236843

John, O. P., & Srivastava, S. (1999). *The Big-Five trait taxonomy: History, measurement, and theoretical perspectives*.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, *17*, 387–402.

Kim, E. J., Namkoong, K., Ku, T., & Kim, S. J. (2008). The relationship between online game addiction and aggression, self-control and narcissistic personality traits. *European Psychiatry*, *23*(3), 212–218.

Koloseni, D. N. (2017). *The practice of information security: an analysis of government employees in Tanzania using the Health Belief Model (HBM)* (pp. 1–241). Universiti Tunku Abdul Rahman.

Koloseni, D. N., Lee, C. Y., & Gan, M.-L. (2019). Understanding information security behaviours of Tanzanian government employees: A health belief model perspective. *International Journal of Technology and Human Interaction*, *15*(1). https://doi.org/10.4018/IJTHI.2019010102

Kovalchuk, O., Shynkaryk, M., & Masonkova, M. (2021). Econometric Models for Estimating the Financial Effect of Cybercrimes. *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)*, 381–384.

Kuijpers, M., Douglas, S., & Kuiken, D. (2019). Personality traits and reading habits that predict absorbed narrative fiction reading. *Psychology of Aesthetics, Creativity, and the Arts*, *13*(1), 74.

Li, Y., Huang, Z., Wu, Y. J., & Wang, Z. (2019). Exploring how personality affects privacy control behaviour on social networking sites. *Frontiers in Psychology*, *10*, 1–9. https://doi.org/10.3389/fpsyg.2019.01771

Lim, B.-C., & Ployhart, R. E. (2006). Assessing the convergent and discriminant validity of Goldberg's International Personality Item Pool: A multitrait-multimethod examination. *Organizational Research Methods*, *9*(1), 29–54.

Lim, S. L., Bentley, P. J., Peterson, R. S., Hu, X., & Prouty McLaren, J. (2023). Kill chaos with kindness: Agreeableness improves team performance under uncertainty. *Collective Intelligence*, *2*(1), 263391372311585. https://doi.org/10.1177/26339137231158584

Limayem, M., Hirt, S. G., & Cheung, C. M. K. (2007). How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance. *Mis Quarterly*, *31*(4), 705–737.

Lucas, R. E., & Baird, B. M. (2004). Extraversion and emotional reactivity. *Journal of Personality and Social Psychology*, *86*(3), 473.

Matt, C., & Peckelsen, P. (2016). Sweet idleness, but why? How cognitive factors and personality traits affect privacy-protective behaviour. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 4832–4841.

McCloskey, K., & Johnson, B. T. (2021). You are what you repeatedly do: Links between personality and habit. *Personality and Individual Differences*, *181*(June), 111000. https://doi.org/10.1016/j.paid.2021.111000

Mccormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual Differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156.

Neal, D. T., Wood, W., & Quinn, J. M. (2006). Habits - A repeat performance. *Current Directions in Psychological Science*, *15*(4), 198–202. https://doi.org/10.1111/j.1467-8721.2006.00435.x

Nord, J. H. (2020). Impact of Habits on Information Security Policy Compliance. *Issues In Information Systems*, *21*(3), 217–226. https://doi.org/10.48009/3_iis_2020_217-226

Nord, J. H., Koohang, A., Floyd, K., & Paliszkiewicz, J. (2020). Impact of habits on information security policy compliance. *Issues in Information Systems*, *21*(3), 217–226.

Novakovic, L., McGill, T., & Dixon, M. (2009). Understanding user behaviour towards passwords through acceptance and use modelling. *International Journal of Information Security and Privacy (IJISP)*, *3*(1), 11–29.

Ogata, H., Ishikawa, T., Miyamoto, N., & Matsumoto, T. (2020). An ATM security measure to prevent unauthorized deposit with a smart card. *IEICE Transactions on Information and Systems*, *E103D*(3), 590–601. https://doi.org/10.1587/transinf.2019EDP7143

Organ, D. W., & Paine, J. B. (1999). *A new kind of performance for industrial and organizational psychology: Recent contributions to the study of organizational citizenship behaviour.*

Padayachee, K. (2022). Understanding the effects of situational crime prevention and personality factors on insider compliance. *Journal of Information Security and Applications*, *70*, 103338.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behaviour towards IS security policy compliance. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 156b-156b.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*(May), 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Pathak, S. K., Pathak, S. K., Mishra, M. K., Kesharwani, L., & Gupta, A. K. (2015). Automated teller machine (ATM) fraud and security. *The Indian Police Journal*, *62*(3), 192–206.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, *20*(1), 18–28.

Peng, M. H., & Dutta, B. (2022). Impact of Personality Traits and Information Privacy Concern on E-Learning Environment Adoption during COVID-19 Pandemic: An Empirical Investigation. *Sustainability (Switzerland)*, *14*(13). https://doi.org/10.3390/su14138031

Pfeiler, T. M., & Egloff, B. (2020). Personality and eating habits revisited: Associations between the big five, food choices, and Body Mass Index in a representative Australian sample: a*ppetite*, *149*, 104607.

Power, V., & Bello, A. (2022). Individual differences in cyber security behaviour using personality-based models to predict susceptibility to sextortion attacks. In *Cybersecurity and Cognitive Science* (pp. 89–113). Elsevier.

Reveilhac, M., & Pasquet, M. (2009). Promising secure element alternatives for NFC technology. *Proceedings - 2009 1st International Workshop on Near Field Communication, NFC 2009*, *June*, 75–80. https://doi.org/10.1109/NFC.2009.14

Ringle, C. M., Wende, S., & Becker, J.-M. (2022). *SmartPLS 4*. Smart PLS 4.

Russell, J. D., Weems, C. F., Ahmed, I., & Richard III, G. G. (2017). Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors. *Journal of Cyber Security*

Technology, *1*(3–4), 163–174. https://doi.org/10.1080/23742917.2017.1345271

Sansone, C., Wiebe, D. J., & Morgan, C. (1999). Self-Regulating Interest: The Moderating Role of Hardiness and Conscientiousness. *Journal of Personality*, *67*(4), 701–733. https://doi.org/10.1111/1467-6494.00070

Shankhwar, S., Pandey, D., & Khan, R. A. (2020). Phishing prevention guidelines. In *Big Data Analytics and Computing for Digital Forensic Investigations* (pp. 171–181). CRC Press.

Shmueli, G., & Koppius, O. R. (2011). Predictive analytics in information systems research. *MIS Quarterly*, 553–572.

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. *AMCIS 2006 Proceedings*, 415.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior. *Computers and Security*, *49*, 177–191.

Simola, P., Virtanen, T., & Sartonen, M. (2019). Information security is more than just policy; it is in your personality. *ECCWS 2019 18th European Conference on Cyber Warfare and Security*, 459–465.

Škrinjarić, B., Budak, J., & Žokalj, M. (2018). The Effect of Personality Traits on System Incorporation. *Ekonomski Pregled*, *69*(2), 106–130.

Stefkovics, Á. (2022). Are Scale Direction Effects the Same in Different Survey Modes? Comparison of a Face-to-Face, a Telephone, and an Online Survey Experiment. *Field Methods*, *34*(3), 206–222.

Tadesse, M. M., Lin, H., Xu, B., & Yang, L. (2018). Personality Predictions Based on User Behavior on the Facebook Social Media Platform. *IEEE Access*, *6*, 61959–61969. https://doi.org/10.1109/ACCESS.2018.2876502

Tang, J., Akram, U., & Shi, W. (2020). Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: based on personality traits. *Journal of Enterprise Information Management*, *34*(4), 1097–1120. https://doi.org/10.1108/JEIM-03-2020-0088

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150.

Uffen, J., Kaemmerer, N., & Breitner, M. H. (2013). Personality traits and cognitive determinants–an empirical investigation of the use of smartphone security measures. *Journal of Information Security 4 (2013), Nr. 4*, *4*(4), 203–212.

Urrila, A. S., Artiges, E., Massicotte, J., Miranda, R., Vulser, H., Bézivin-frere, P., Lapidaire, W., Lemaître, H., Penttilä, J., Conrod, P. J., Garavan, H., Martinot, M. P., & Martinot, J. (2017). Sleep habits , academic performance, and the adolescent brain structure. *Nature Publishing Group, April 2016*, 1–9. https://doi.org/10.1038/srep41678

Van Ouytsel, J. (2021). The prevalence and motivations for password sharing practices and intrusive behaviors among early adolescents' best friendships–a mixed-methods study. *Telematics and Informatics*, *63*, 101668.

Vance, A., Siponen, M., & Pahnila, S. (2012a). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3–4), 190–198.

Vance, A., Siponen, M., & Pahnila, S. (2012b). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198.

Vasilopoulos, N. L., Cucina, J. M., & McElreath, J. M. (2005). Do warnings of response verification moderate the relationship between personality and cognitive ability? *Journal of Applied Psychology*, *90*(2), 306.

Vernon, L., Modecki, K. L., & Barber, B. L. (2018). Mobile phones in the bedroom: Trajectories of sleep habits and subsequent adolescent psychosocial development. *Child Development*, *89*(1), 66–77.

Verplanken, B., & Aarts, H. (1999). Habit, Attitude, and Planned Behaviour: Is Habit an Empty Construct or an Interesting Case of Goal-directed Automaticity? *European Review of Social Psychology*, *10*(1), 101–134.

Vishwanath, A., Habit, E., Susceptibility, P., Habits, M., Processing, H., & Processing, S. (2015). Examining the Distinct Antecedents of E-Mail Habits and its Influence on the Outcomes of a Phishing Attack. *Journal of Computer-Mediated Communication*, *20*, 570–584. https://doi.org/10.1111/jcc4.12126

Volk, A. A., Brazil, K. J., Franklin-Luther, P., & Dane, A. V. (2020). The influence of demographics and personality on COVID-19 coping in young adults. *Personality and Individual Differences*.

Widiger, T. A., & Trull, T. J. (1997). Assessment of the five-factor model of personality. *Journal of Personality Assessment*, *68*(2), 228–250.

Yan, T., Keusch, F., & He, L. (2018). The impact of question and scale characteristics on scale direction effects. *Survey Practice*, *11*(2), 1–9.

Yazdanpanah, M., & Hosseinlou, M. H. (2017). The role of personality traits through habit and intention in determining future preferences of public transport use. *Behavioral Sciences*, *7*(1), 1–15. https://doi.org/10.3390/bs7010008

Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741–759.

Zhang, R., Bello, A., & Foster, J. L. (2023). BYOD Security: Using Dual Process Theory to Adapt Effective Security Habits in BYOD. *Proceedings of the Future Technologies Conference*, 372–386.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

  ISSN: 1941-6679-On-line Copy

APPENDIX

Constructs/ Item	*Source*
Conscientiousness	(Donnellan *et al.*, 2006; Goldberg, 1999)
CS1: I get chores done the right way.	
CS2: I like to keep things in order.	
CS3: I often forget to put things back in their proper place.	
CS4: Many times, I mess up things.	
Agreeableness	(Lim & Ployhart, 2006; Goldberg, 1999)
AG1: I sympathize with others frequently.	
AG2: I feel for others	
AG3: I don't care what others are doing.	
AG4: I go with the majority	
Neuroticism	(Lim & Ployhart, 2006;Vasilopoulos *et al.*, 2005)
NE:1 I experience frequent mood swings.	
NE:2 I get upset easily.	
NE:3 I am relaxed most of the time.	
NE:4 I seldom feel blue.	
Openness	(Donnellan et al., 2006)
OP1: I enjoy imagining new and different ideas.	
OP2: I experience difficulty in comprehending abstract ideas	
OP3: OPN3 I am not keen to engage myself in intellectual discussions.	
OP4: I do not enjoy daydreaming	
Extraversion	(Donnellan et al., 2006)
EXT1: I enjoy partying frequently.	
EXT2: I enjoy talking to new people who are different from me.	
EXT3: I do enjoy socializing.	
EXT4: I enjoy going out to help people in need.	
Security habit	(Koloseni, 2017; Limayem *et al.*, 2007; Vance *et al.*, 2012)
SEH1: I have a habit of changing my PIN code regularly.	
SHE 2: It is my habit to change my PIN code periodically	
SHE 3: It is a norm for me to change the PIN code	
SHE 4: I check for people around me when login into my account without being reminded to do so.	
SHE 5: Checking for people around me before accessing my account is something I feel weird if I do not do it.	
PIN Security Practices	
PSP 1: I change my PIN code frequently	

PSP2: I never re-use old PIN code	(Novakovic et al., 2009; Van Ouytsel, 2021; Yıldırım & Mackie, 2019)
PSP 3: I often hide my password when making financial transactions	
PSP 4: I never share my PIN code	