A quantitative diary study of perceptions of security in mobile payment transactions

Jiaxin Zhang and Yan Luximon (Corresponding author)
School of Design, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong SAR
yan.luximon@polyu.edu.hk

Abstract

While mobile payment services have been flourishing in China, users have continually questioned the security of these transactions. Although customization has been proposed as a vital factor for mobile commerce, minimal knowledge exists regarding how it affects users' perceived security in mobile payment transactions. A quantitative diary study was therefore conducted to provide insight into the personality traits that motivate customization behaviors in security, and how such behaviors influence perceived security under different use contexts in relation to mobile payments. First, an instrument for the diary study was developed through an interview. Then, 134 responses from mobile payment users were used to examine the relationships between personality traits and customization behaviors. Among them, the diary was completed by 67 mobile payment users who reported their perceived security for 1094 recoded payment events across various use contexts for periods ranging between 5 and 15 days. The results showed that the personality traits of extraversion and intellect influence users' customization behaviors and these behaviors have a positive effect on perceived security. Additionally, the relationship between customization behaviors and perceived security was moderated by the task and technical contexts. Based on these findings, design implications and opportunities for mobile payment services are described.

Keywords

Perceived Security; Customization Behaviors; Mobile Payment; Use Contexts; Quantitative Diary Study.

1. Introduction

Ubiquitous mobile technologies have produced new methods of economic exchange. Mobile payment, defined as “payments for goods, services, and bills with a mobile device by taking advantage of wireless and other communication technologies” (Dahlberg, Guo & Ondrus, 2015) is a convenient and effective payment method. Numerous mobile payment systems, such as Apple Pay, Samsung Pay, PayPal, Google Wallet, Alipay, and WeChat Pay, have been introduced to mass markets worldwide. However, levels of acceptance of these payment services are unevenly distributed. Studies have shown that perceived security is a crucial predictor of mobile payment acceptance in developing markets (Dahlberg et al., 2015; Goeke & Pousttchi, 2010; Mallat, 2007), and this in turn is equally vital to post-adoption usage in mature markets. For a substantial number of mobile payment users in China (502 million in 2017), security remains a prominent challenge in the development of mobile payment methods because 71.8% of users have security concerns (iiMedia Research, 2017). In 2018, a survey in China reported that 64.7% users stated that security was a main concern around mobile payment usage. In addition, 50% of users required there to be better security management of mobile payment services (Payment & Clearing Association of China, 2019). Recent security issues related to mobile payments have revealed that various improvements to the security experience pertaining to mobile payment services are still required. For example, in 2017, Alipay experienced problems with security holes in the interaction design of its authentication methods, and in 2018, Alipay’s visual design for privacy caused a scandal, inciting numerous user complaints (Global Web, 2018; He, 2018). Due to the inadequate design of mobile payment services, many users still regard mobile payment as an insecure payment method, even though it has been proven to be more secure than traditional payment methods (Johnson, Kiser, Washington & Torres, 2018). This situation has revealed the importance of understanding how to design mobile payment services to enhance perceived security.

Research into mobile-commerce-user interfaces has indicated that customization is an important element of interface design (Lee & Benbasat, 2004). Customization can refer to the sites or devices that are capable of being tailored by users (Lee & Benbasat, 2004; Nilashi, Ibrahim, Reza Mirabi, Ebrahimi & Zare, 2015). Users can tailor aesthetic features such as the interface layout out, background color or font, as well as functional features including information settings and system settings (Kim et al., 2015). Customizations are also available in mobile payment services (Shao, Zhang, Li & Guo, 2019). On the other hand, users are considered to be the weakest link when it comes to information security as they are generally reluctant to comply with security suggestions and do not understand security mechanisms (Safa et al., 2015; Tam, Glassman & Vandenwauver, 2010). However, studies have also found that users have developed their own security strategies to protect their accounts based on the contexts of use (Gross & Rosson, 2007; Radke, Boyd, Nieto & Buys, 2013). Different online activities require different levels of security, with financial accounts requiring the highest level of security. Therefore, if users perceive security protection to be insufficient, they will develop their own approaches to protect their security (Radke et al., 2013). Since users are allowed to tailor security functions in mobile payment services, they could take security actions by customizing their security settings to improve their perceived security. This paper focuses on the functional customization provided to users and investigates the functional customization behaviors of users. While users may take action to fulfill their security needs and enhance their perceived security, personality traits remain an importance predictors of user behavior (Shropshire, Warkentin & Sharma, 2015; Zhang, Reithel & Li, 2009). However, personality patterns in m-commerce security behavior are still rarely discussed. This study attempts to expand the body of knowledge around personality patterns and customization behaviors in m-commerce.

Even though customization behaviors are vital to perceived security, use context is another important factor when studying user interaction with mobile devices (Korhonen, Arrasvuori & Väänänen-Vainio-Mattila, 2010). Use context involves information that influences interactions between users and systems (Dey, 2001), and has various dimensions according to the research fields (Belk, 1974; Korhonen et al., 2010; Tarasewich, 2003; Wigelius & Väätäjä, 2009). For example, researchers have proposed social, spatial, temporal, infrastructural, and task contexts to describe interactions between an individual and a mobile device. User behaviors vary according to contextual conditions, as conditions can influence a user’s priorities and abilities during such interactions (Barnard, Yi, Jacko & Sears, 2007). Additionally, researchers (Barnard et al., 2007; Kjeldskov & Skov, 2014) have suggested that contextual factors should be studied using field studies that cater to specific domains.

As security is an essential concern for mobile payment users and mobile services are ubiquitous, it is important to gain a better understanding of user customization behaviors in relation to security settings and perception of security. This research therefore addresses the relationships that exist between personality traits, customization behaviors, and perceived security, and investigates how these relationships change according to different use contexts. By applying the Big Five Personality Trait Theory, this study advances knowledge of the relationships between user customization behaviors and personality traits. It also combines Protection Motivation Theory (PMT) and Risk Compensation Theory to examine how customization behaviors (security behaviors) influence users' perceived security (threat appraisal) in different use contexts.

This study began by interviewing 14 mobile payment users to gain an understanding of their mobile payment service customization behaviors and to categorize payment contexts in daily life. Subsequently, based on the interview results, research instruments were developed for use in a quantitative diary study to assess the relationships between personality traits and customization behaviors, as well as the moderating effects of use context on the relationships between customization behaviors and perceived security. A total of 134 mobile payment users participated in reporting their personality traits and customization behaviors in relation to security settings for mobile payments in the initial phase of the quantitative diary study. Of the 134 participants, 67 participated in recording payment events with their perceived security and description of use context within the task context, technical context and social context for periods ranging from 5 to 15 days. The results answered the following research questions: "How do users customize their mobile payment services? Which personality traits influence users' customization behaviors in relation to security settings? How does use context influence the effect of customization behaviors on perceived security?"

2. Literature review and development of research model

2.1 Theoretical background of the research model

Many studies have attempted to understand users' behaviors in relation to information technology (Menard, Bott & Crossler, 2017; Das & Khan, 2016; Safa et al., 2015; Anderson & Agarwal, 2010; Rhee, Kim & Ryu, 2009; Zhang et al., 2009). Most of them were conducted by grounding in psychological and predictive behaviour theories, including the PMT (Roger, 1975, 1983), Social Cognitive Theory (Bandura, 1986), Self-Determination Theory (Deci & Ryan, 2012) and Theory of Planned Behavior (Ajzen, 1991). Of these models, PMT places a particular focus on user security behaviors and highlights the influences that result from an individual's evaluation of threats and their capability to deal with these threats. PMT was initially developed to explain how fear affects people's attitude and behavior around public health (Roger, 1975, 1983). Many researchers in the field of information security have utilized PMT as a theoretical framework to explain and predict users' security behaviors in relation to information security threats (Hanus & Wu, 2016; Johnston & Warkentin, 2010; Tsai et al., 2016). According to PMT, a person's security protection behavior is influenced by two cognitive processes: threat appraisal and coping appraisal. Threat appraisal involves two factors: perceived severity and perceived vulnerability (Floyd, Prentice-Dunn & Rogers, 2000). Threat appraisal thus describes the level at which users evaluate the severity of a threat, as well as the possibility that they are vulnerable to a threat (Crossler & Bélanger, 2014). Coping appraisal is an evaluation process whereby the user assesses whether they are capable of protecting oneself, if such action is effective, and if there is value in applying such a protection (Crossler & Bélanger, 2014). Coping appraisal comprises three factors: response efficacy, self-efficacy, and response cost (Floyd et al., 2000). Both threat appraisal and coping appraisal are triggered by information from different sources: environmental and intrapersonal. Environmental information involves verbal persuasion and observational learning, while intrapersonal information involves personality variables and prior experience (Floyd et al., 2000).

Despite the fact that well-developed theories have been applied to explain the drivers of undertaking security behaviors, researchers have found that Risk Compensation Theory could provide new insights into explaining user attitudes toward risks after they had taken the security measurements in information technology (Kearney & Kruger, 2016; Zhang et al., 2009). This idea was inspired by the paradox that people who pursue high-level security measures are more likely to perceive themselves as highly secure and therefore take more risks. For example, users might feel more secure if they engage in a higher number of customization behaviors, even when they send money to an untrustworthy account. According to Risk Compensation Theory, users initially appraise a threat to their transactions and financial systems based on their previous experience in mobile payment usage. Users will customize security settings in their applications to compensate for threats and to obtain an acceptable level of perceived security. However, users use mobile payment services in various situations, which may present new risks. Therefore, perceived security levels will be lower or higher depending on the context (Kearney & Kruger, 2016).

PMT claims that threat appraisal affects users' security behaviors, while Risk Compensation Theory proposes that users' security practices will have a response to users' evaluation to the threats. One interpretation of PMT is that environmental sources exist as a trigger within the threat and coping appraisal process. This study combines PMT and Risk Compensation Theory, and investigates how an individual's security behaviors could compensate for their threat appraisal of a situation (see Figure 1). This study assumes that users' security behaviors will have a response to their threat appraisal, and that this effect is influenced by environmental sources. In other words, if users had customize more security settings, they might feel more secure, and this effect will be particularly distinct in some use contexts.

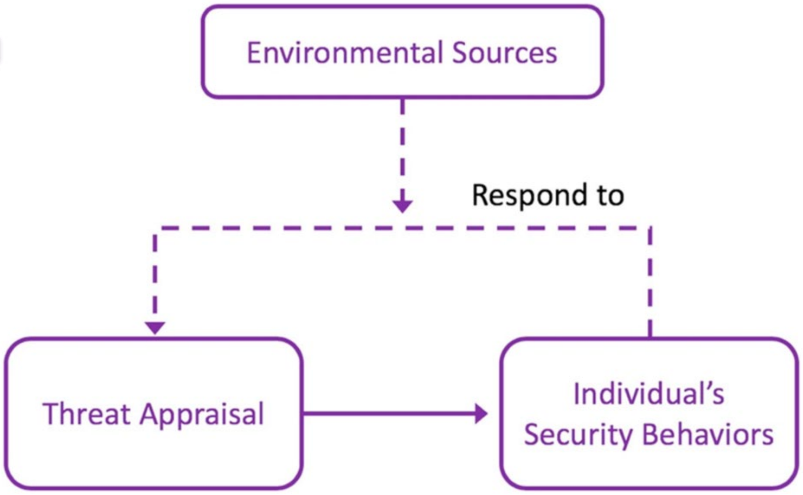

Figure 1. The theoretical background relationship based on PMT and Risk Compensation Theory.

2.2 Development of the research model

2.2.1 Perceived security and threat appraisal

Perceived security has been studied by many information technology researchers. However, definitions of perceived security are often adapted to fit the research context. Perceived security in information technology was initially defined as the degree to which an individual believes that transmitting sensitive information is secure on the web (Salisbury, Pearson, Pearson & Miller, 2001). Adapting this definition to the mobile payment research context, perceived security can be defined as the extent to which one can transact sensitive information securely over mobile payment platforms (Fan, Shao, Li & Huang, 2018; Hartono, Holsapple, Kim, Na & Simpson, 2014; Khalilzadeh, Ozturk & Bilgihan, 2017). Since perceived security plays an important role in the use of information technology, researchers have attempted to measure the perceived security of users. For example, Huang, Rau and Salvendy (2010) have indicated that perceived security should be measured in relation to threats, and have revealed six constructs of perceived security, namely perceived knowledge, perceived impact, perceived severity, perceived controllability, perceived possibility and perceived awareness. Colobran (2016) believes that perceived security refers to the level security that one feels, ranging from "complete security" to "no security at all". As users evaluate the severity of threats and the possibility of vulnerability in threat appraisal of PMT, this research views perceived security to represent these two factors in threat appraisal. This is because users' subjective evaluation of the security of personal and financial information mainly relates to threats in mobile payment transactions. It has been proven that perceived security is constructed by perceived knowledge, perceived impact, perceived severity, perceived controllability, perceived possibility and perceived awareness, when in regard to user information technology threats (Huang et al., 2010). Therefore, perceived security is a more comprehensive indicator for reflecting user's appraisal of risky situations.

2.2.2 Environment sources and use context

Environment sources are proposed to have effects on threat appraisal, according to PMT. They consist of verbal persuasion and observational learning, which implies that environmental sources involve any information within the threat appraisal process (Floyd et al., 2000). In the field of human-computer interaction, environmental sources can be regarded as use context, which has been generally described as "any information that can be used to characterize the situation of entities that are considered relevant to the interaction between a user and an application, including the user and the application themselves" (Dey, 2001). Environmental sources can also be specifically defined as any environmental conditions within a mobile interaction. For example, Barnard et al. (2007) have claimed that a context is “a set of conditions or users’ states that influence the ways in which a human interacts with a mobile computing device”. Liang and Yeh (2011) have defined use context as “people who use their mobile devices in diverse environments”.

Based on the definition of use context, it is a vital aspect of user behavior during mobile interactions. Many researchers have also explored specific contextual factors when studying user behavior or when designing general mobile services. Belk (1974) initially defined five situational factors that influence consumer behaviors: physical surroundings, social surroundings, temporal perspective, task definition, and antecedent states. Tarasewich (2003) has proposed a context model comprising three dimensions: environment, participants, and activity. Wigelius and Väätäjä (2009) have suggested five contextual factors that influence mobile use: social, spatial, temporal, infrastructural, and task context. Finally, Korhonen et al. (2010) have proposed eight contextual factors, namely environment, personal, task, social, spatio-temporal, device, service, and access network, to analyze the mobile user experience. In terms of security, different dimensions of use context influence user behaviors. For instance, Wolf, Kuber and Aviv (2018) have proposed that applying context-sensitive technology could enhance security. Mallat (2007) has studied the influence of context on mobile payment usage and found that users’ security and privacy concerns are associated with authentication and confidentiality. These studies have discussed the influence of use context from a technology-based perspective. Dourish, Grinter, De La Flor and Joseph (2004) have proposed that users’ perceptions of security depend not only on the nature of the task but also on who they interact with. This illustrates the influence of context from the perspective of social relationships.

2.2.3 Personality traits, security behaviors and customization behaviors

Numerous studies have investigated factors influencing users’ security behaviors (Zhang et al., 2009). Personality traits constitute one of the most important predictors. Nicholson, Soane, Fenton-O’Creevy and Willman (2015) have identified the personality patterns of risk takers using six categories, namely “recreation, health, career, finance, safety, and social” (p. 160). They found that risk takers tend to have high extraversion and openness, and low neuroticism, agreeableness, and conscientiousness. Nevertheless, the link between personality patterns and security behaviors is based on research domains. In other words, although a specific personality pattern might lead to more security behaviors in one domain, it may not necessarily predict security behaviors in another domain. For instance, Shropshire et al. (2015) have found that agreeableness and conscientiousness can moderate the relationship between intention and behaviors in security software adoption to protect organizational security. Junglas, Johnson and Spitzmüller (2008) have found that agreeableness and openness to experience are significantly related to concerns for privacy security in location-based services. Korzaan and Boswell (2008) have found that agreeableness and intellect can indirectly and directly affect a user's intention to retaliate against the personal collection practices of an organization. Therefore, according to research, the influence of personality traits on security behaviors is context-based.

On the other hand, the use of phone settings is an important security behavior related to smartphone use (Zhang, Li and Deng, 2017). In mobile payment services specifically, security customization is provided where users are allowed to improve the security of their accounts by tailoring their security settings (Shao et al., 2019). In this case, to customize security settings is a way to undertake security behaviors in mobile payment services. Therefore, this research approaches users' security behaviors by investigating their customization behaviors in relation to security settings.

2.2.4 Proposed research model

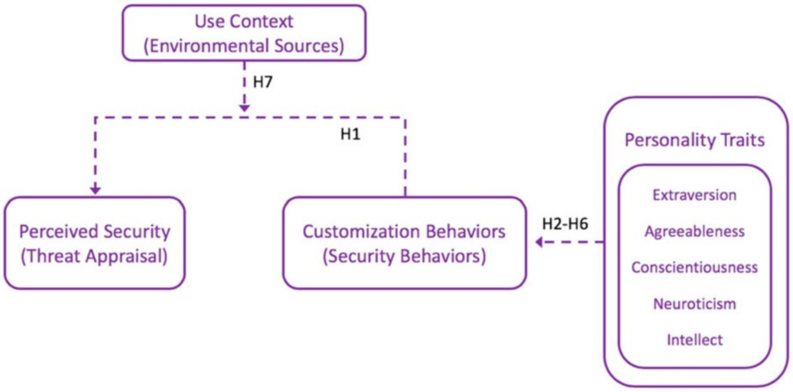

Figure 2. The proposed research model

Based on the initial research model derived from PMT, Risk Compensation Theory (see Figure 1), and other literature, a research model was proposed (see Figure 2). This model assumes that user personality traits will influence customization behaviors, that these behaviors have an impact on perceived security, and that use context has a moderating effect on the relationship between customization behaviors in security settings and perceived security. Detailed hypotheses were then developed from these assumptions.

2.3 Hypotheses

2.3.1 Customization behaviors and perceived security

Customization is a notable factor in mobile interface design (Lee & Benbasat, 2004; Mahatanankoon, Wen & Lim, 2005; Nilashi, Ibrahim, Reza Mirabi, Ebrahimi & Zare, 2015). Previous studies have shown that customization is one of the most important interface design features of m-commerce, particularly in the enhancement of users' trust in the system (Lee & Benbasat, 2004; Li & Yeh, 2010; Schwiderski-Grosche & Knospe, 2002). For mobile payment services in particular, customization behaviors refer to a user's ability to tailor a payment system to meet their needs and personal habits. These include behaviors such as customizing the information function, payment methods and security settings (Li & Yeh, 2010; Shao et al., 2019; Tossell, Kortum, Shepard, Rahmati & Zhong, 2012). For instance, users are able to add or delete icons from the home page of Alipay to create a personal interface. They can also change authentication methods by modifying their security settings. In terms of the psychological aspect, researchers have also found that customization has a strong connection to users' psychological needs (Kim et al., 2015; Marathe & Sundar, 2011). As this paper has proposed that security behaviors could have a positive effect on perceived security, and that users undertake security behaviors through functional customization, we hypothesized that users' customization behaviors have a positive influence on perceived security. Thus, users who have more customized security settings in a mobile payment system will exhibit a higher level of perceived security.

H1: Customization behaviors in relation to security settings will have a positive effect on perceived security.

2.3.2 Personality traits and customization behaviors

Many personality theories have been developed to measure the traits of an individual. This study applied constructs from Big Five Personality traits, namely extraversion, agreeableness, conscientiousness, neuroticism, and intellect.

Extraversion refers to people who are energetic, active and sociable (Donnellan, Oswald, Baird, & Lucas, 2006; Halevi, Lewis & Memon, 2013). People with high extraversion are expected to be more energetic and outgoing. Gratian, Bandi, Gukier, Dykstra and Ginther (2018) have suggested that extraversion is positively related to device securement behavioral intention. In other words, people who exhibit energetic and outgoing traits are more likely than introverted people to have the intention to lock their devices. However, other researchers have indicated that users with higher extraversion scores are more likely to take risks and become vulnerable to phishing (Halevi et al., 2013; Nicholson, Soane, Fenton-O'Creevy & Willman, 2005). As customizing the settings will be a burden on the interaction with payees, this study expected that extraverted users would take risks for a more active payment interaction. Thus, it was hypothesized that:

> H2: Extraversion will have a negative effect on customization behaviors in relation to security settings of mobile payment services.

Conscientiousness indicates the level of organization, systematization, efficiency, and dutifulness when performing tasks; agreeableness describes people's willingness to trust others, consider others' feelings, and help others (Donnellan et al., 2006; Halevi et al., 2013; Zhou & Lu, 2011). Conscientiousness and agreeableness are more likely to have a positive effect on security management behaviors. For example, Uffen, Kaemmerer and Breitner (2013) found that conscientiousness has a positive effect on the intention to take security measures when using smartphones; Shropshire, Warkentin, Johnson and Schmidt (2006) and Shropshire et al. (2015) found that both agreeableness and conscientiousness have a positive influence on IT security-compliant behaviors and could moderate the actual use of security software. Therefore, two hypotheses were proposed:

> H3: Agreeableness will have a positive effect on customization behaviors in relation to security settings of mobile payment services.

> H4: Conscientiousness will have a positive effect on customization behaviors in relation to security settings of mobile payment services.

Neuroticism refers to people who are prone to emotional instability, nervousness, and anxiety (Donnellan et al., 2006; Halevi et al., 2013; Zhou & Lu, 2011). Neurotic users feel a lack of control and are concerned about potential risk and loss (Zhou & Lu, 2011). This could therefore be a positive personality trait in relation to security practices, because computer anxiety may encourage users to engage in security behaviors (Korzaan & Boswell, 2008). Therefore, the following hypothesis was proposed:

> H5: Neuroticism will have a positive effect on customization behaviors in relation to security settings of mobile payment services.

The fifth personality trait in this study is intellect, with characteristics such as imaginative, creative, abstract thinking, curious and knowledgeable (Donnellan et al., 2006; Halevi et al., 2013; Korzaan & Boswell, 2008). Therefore, people who exhibit high levels of intellect would tend to realize the risks and take security measurements. For example, Korzaan and Boswell (2008) found that intellect could affect a user's behavioral intention to retaliate against personal collection practices that are undertaken by some organizations. Thus, it was hypothesized that:

> H6: Intellect will have a positive effect on customization behaviors in relation to security settings of mobile payment services.

2.3.3 Use context

The critical role of use context has also been acknowledged in interface design and mobile security. Blom and Monk (2003) revealed that contextual factors are an important factor in explaining why users change the appearance of their mobile devices. Tarasewich (2003) also argued that the complexities of context and interaction should be considered in the design of m-commerce applications. Different dimensions of the use context may play a role in user behaviors, and this context has specific categories according to the research domain (Barnard et al., 2007; Kjeldskov & Skov, 2014). This study regards use context as "any feature that describe the situation related to the interaction between humans and mobile devices", and defines it as a moderator (Dey, Abowd & Salber, 2001; Liang & Yeh, 2011). It focused on the influence of use context on the relationships between user perceived security and customization behaviors in mobile payment services. This meant that the direction and the strength of the relationship between two variables could vary based on each dimension of the moderator (Baron & Kenny, 1986; Shin, 2009). Therefore, the moderated effect of use context was proposed in H7. The specific dimensions of use context (contextual factor) in relation to perceived security in mobile payment systems were then identified and the sub-hypotheses were proposed in the interview study (Section 3 of this paper).

H7: Use context moderates the relationship between customization behaviors in relation to security settings and perceived security.

3 Interview study of customization behaviors and contextual factors

The previous section had proposed a research model and hypotheses to address the relationships that exist between personality traits, customization behaviors, perceived security, and use context. Due to minimal available knowledge of users' customization behaviors and contextual factors surrounding the use of mobile payment services, a semi-structured interview study was first conducted to explore users' customization behaviors, as well as contextual factors to develop research instruments for the quantitative diary study.

3.1 Interview participants and procedure

A snowball sampling method was applied to recruit interviewees in China. The aim was to select experienced mobile payment users in order to elicit various attitudes and perceptions toward security, diverse use contexts, and customization behaviors in regard to mobile payment systems.

Interviewees were regular mobile payment users and none were information security experts. They comprised six males and eight females, all aged between 21 and 29 (mean = 25.642; standard deviation = 1.823), of whom 11 had more than 3 years' experience using mobile payments, two had 1 to 3 years' experience, and one had 0.5 to 1 years' experience. The guidelines for the semi-structured interview incorporated three sections: 1) participants discussed their security concerns; 2) they reported their need for security protection, security practices, and customization in mobile payment services; and 3) they described their previous secure or insecure experiences of using mobile payment services. All interviews were audio recorded. Ten interviews were conducted face-to-face, and four interviews were conducted via telephone. Each interview lasted between 25 and 45 minutes.

3.2 Data analysis and results

The audio recordings of the interviews were transformed into text data. Using ATLAS.ti software, the interview data was coded by performing thematic analysis. The similarities and meanings in the texts were compared and grouped (Saldaña, 2015). Table 1 and Table 2 lists some example codes and quotations from the interviewees.

Table 1. Example of interview coding in customization behaviors

Category	**Customization behaviors (selection)**	**Interview quotation(example)**
Enhance control of the payment system	Set a daily payment limit;	I set a daily payment limit for my mobile payment account in case my account is hacked (Participant No.8)
	Decline the billing agreements with merchants;	I didn't agree to "the billing agreement with merchants" that was proposed by the system. This is because I want to manually confirm every payment by myself (Participant No.11)

Table 2. Example of interview coding in use context

Category	Types of contextual factors (selection)	Interview quotation(example)
Task context	QuickPay;	I feel insecure when merchants scan my QR code to pay. In this circumstance, the payment amount is input by the merchant, and I am worried that they would input a larger sum. (Participant No.2)
	QR code pay	I feel worried when I scan the QR code displayed on the shared bike, because it might be a fake QR code.(Participant No.5)

3.2.1 Users 'customization behaviors in mobile payment system

Text segments in regard to users' customization behaviors were grouped into three codes (categories of customization behaviors) and six sub-codes (customization behaviors) (see Table 3). The frequencies of the codes were also counted. Most participants said they had attempted to enhance their control of the system (N = 9), and around half of them (N = 6) said they had changed the payment authentication methods. These two categories of customization behaviors were aimed at improving the security usage. However, three participants said they had modified the layout of the mobile payment system, but that they only did so for the convenience or to improve the aesthetic appearance of the interface.

Table 3. Classification of customization behaviors

Category	Customization behaviors
Change payment authentication methods	Disable the one-step payment (pay without authentication) function;
	Set a login authentication;
	Set both login and payment authentications.
Enhance control of the payment system	Set a daily payment limit;
	Decline the billing agreement with the merchant;
Layout modification	Remove functions from the home page of the mobile payment system.

3.2.2 Contextual factors related to perceived security

Previous studies have reported several contextual factors in various situations related to mobile and mobile payment usage (Arrasvuori, Boberg & Korhonen, 2010; Belk, 1974; Engl & Nacke, 2013; Mallat, Rossi, Tuunainen & Anssi, 2009). These served as a basis for developing an appropriate classification of contextual factors in this study. The coding results indicated that interviewees perceived security in different ways according to the task context, technical context, and social context. Therefore, these three contextual factors were used as the three main themes. Subsequently, eleven sub-codes (types of contextual factors) were also identified from the interviews.

The task context, defined as the interaction involved in the payment process, comprised five sub-codes; the technical context, defined as the authentication method applied in the payment process, also comprised five sub-codes; and the social context, defined as the degree of trust in the payee, comprised one sub-code. Classifications and definitions of the contextual factors are presented in Table 4.

Consequently, hypothesis H7 was then be further specified with three sub-hypotheses:

H7: Use context moderates the relationship between customization behaviors and perceived security.

H7.1: Task context moderates the relationship between customization behaviors and perceived security.

H7.2: Technical context moderates the relationship between customization behaviors and perceived security.

H7.3: Social context moderates the relationship between customization behaviors and perceived security.

Table 4. Classification and definition of Contextual factors

Contextual factors	**Types of contextual factors**	**Definition**
Task context	QR code pay	Quick response (QR) code pay is a payment method that requires consumers to use a mobile payment application (such as Alipay or WeChat Pay) to scan a merchant's mobile payment QR code. In this method, the consumer must open a mobile payment application and select the QR code scan function to scan the merchant's QR code. The consumer must then enter or confirm the payment amount and authorize the transaction.
	QuickPay	In QuickPay, a consumer provides a QR code to pay. In this method, the consumer must open a mobile payment application to display their payment QR code to the merchant. The merchant then completes the transaction by entering the payment amount into a reader device and then scanning the consumer's QR code through a barcode scanner.
	M-payment platform pay	Mobile payment (M-payment) platform pay includes various types of payment options embedded in mobile payment applications where no third parties are involved. Currently, mobile payment platforms provide numerous functions, such as peer-to-peer transfer, bill payment, and payment in mobile applets.
	In-app pay	In-app pay refers to payment transactions conducted in third-party apps, such as DiDi, Meituan-Dianpin, and Taobao. In this method, vendors must use M-payment platform software development kits and integrate third-party code into their apps. Specifically, when a consumer makes a purchase in a third-party app, the app requires authorization from an external mobile payment app to process the transaction.
	NFC pay	NFC pay refers to payment methods based on near field communications technology. This payment method requires a physical tag to be installed into users' mobile devices; a software app installation is not required. As with credit card payments, a reader device is required to complete the transaction.
Technical context	Fingerprint	Users apply their fingerprint to authorize the payment.
	Password	Users enter a password to authorize the payment.
	No authentication	Users do not use any authentication method when making a payment.

	Face ID	Users show their face to the phone to authorize the payment.
	Both password and fingerprint	Users apply both password and fingerprint to authorize the payment.
Social context	Trust level	This refers to the degree to which the payer trusts the payee during the payment process.

*The definition of task context was modified based on current popular payment methods in China (Payment products of Alipay, n.d.; Multiple Payment Methods of WeChat Pay, n.d.).

3.3 Interview results used for the development of an instrument for the quantitative diary study

The interview study had helped to identify customization behavior categories and possible contextual factors regarding perceived security in mobile payment services. These were expected to be used to design a questionnaire instrument for the quantitative diary study. In term of user customization behaviors, this research only focused on the effects of functional customization behaviors in relation to security. Therefore, the customization behaviors in the categories of “change payment authentication methods” and “enhance control of the payment system” are selected for the design of the instrument. However, “layout modification” is related to aesthetic customization behaviors and is not considered in this study. Three contextual factors, namely task context, technical context and social context, were identified in the data analysis. The effects of contextual factors are still unclear to the researchers. As such, these three factors are all involved in the development of the questionnaire instrument for the quantitative diary study. The influences of contextual factors will be examined through the quantitative diary study.

4 The diary study design

A quantitative diary study was selected to fulfill the aims of this research. Namely, to determine the relationships between personality traits and customization behaviors in relation to security settings, and to investigate the moderating effects of use context on the relationships between customization behaviors in relation to security settings and perceived security. An advantage of using this method is that data was sourced from real service adoption scenarios rather than from laboratory scenarios with hypothetical settings (Ohly, Sonnentag, Niessen & Zapf, 2010), and was therefore more appropriate for studying the influence of use context. The quantitative diary method also involves an event-based design, whereby the features of a situation and users' responses to the situation are points of focus rather than variations over time (Bolger, Davis & Rafaeli, 2003). Moreover, participants were required to use a pre-coded diary questionnaire instead of free text to record an event, thus ensuring that they described a payment event in relation to the contextual factors that were the focus of this study. Using this method, participants were asked to complete a diary questionnaire immediately after any payment event for a period of 5 to 15 days. Each participant reported at least 10 payment events during their recording period.

4.1 Instrument development

All variables are recorded using two questionnaire instruments in the quantitative diary study including a pre-test questionnaire and a pre-coded diary questionnaire (Appendix A). Users' customization behaviors in relation to security settings and contextual factors pertinent to perceived security identified in the interview study were used to design the pre-test questionnaire and the pre-coded diary questionnaire, respectively.

The pre-test questionnaire was designed to collect data on user characteristics, including demographic information, personality traits, and customization behaviors in relation to security settings to test the hypotheses H2 to H6. Numerous instruments have been developed to measure personalities, including the 50-item International Personality Item Pool-Five Factor Model (the 50-item IPIP FFM) (Goldberg, 1999), the 20-item Mini International Personality Item Pool (the 20-item Mini-IPIP) (Donnellan et al., 2006), and the Ten-Item Personality Inventory (Gosling, Rentfrow & Swann, 2003). The 50-item IPIP-FFM has frequently been used to explain users' security behaviors (Korzaan & Boswell, 2008; Shropshire, Warkentin & Sharma, 2015). The 20-item Mini-IPIP is the short form of the 50-item IPIP-FFM (Cooper, Smillie & Corr, 2010; Donnellan et al., 2006; Goldberg, 1999). A long questionnaire with 50 items is more precise than a shorter instrument, but may lead to careless responses because it is time-consuming to complete (Donnellan et al., 2006). Conversely, although a short questionnaire with 10 items is brief, it may be unreliable (Donnellan et al., 2006). The 20-item Mini-IPIP has been shown to be a more efficient replacement, with similar reliability and validity compared to the 50-item IPIP-FFM (Donnellan et al., 2006), and is a reasonable choice in balancing the trade-off between precision and brevity (Kortum & Oswald, 2018). Therefore, the 20-item Mini-IPIP was used to measure personality traits in the pre-test questionnaire. In term of users' customization behaviors, the categories of "change payment authentication methods" and "enhance control of the payment system", which are related to security behaviors, were selected to create a multiple-choice question to observe users customization behaviors in relation to security.

The pre-coded diary questionnaire was developed to record payment events, and then to test the hypotheses H1 and H7 (H7.1, H7.2 and H7.3). At each payment events, participants recorded the perceived security level with one question and described the use context with three questions. The perceived security level was measured using a semantic differential rating scale ranging from 0 (perceive completely unsecure) to 100 (perceive completely secure) (Abrazhevich, Markopoulos & Rauterberg, 2009). The three questions designed for describing use context are: a single choice question for the task context, a single choice question for the technical context, and a semantic differential rating scale question which is ranging from 0 (completely untrustworthy) to 100 (completely trustworthy) for the social context.

4.2 Recruitment

To optimize the validity of the study, users were expected to exhibit various demographic traits and usage experiences. Hence, non-random-internet (convenience) sampling (Hays, Liu & Kapteyn, 2015; Martens, De Wolf & De Marez, 2019) was utilized to target participants with the following demographic characteristics: aged above 18, non-expert in mobile payment security, and experience in using mobile payment services. The recruitment link was distributed via social media. A financial reward was offered to participants to incentivize their participation. To avoid fake responses, participants were informed that they would not receive the financial reward until their payment diaries had been examined by the researchers.

4.3 Procedure

Mobile payment users who chose to participate in this study were required to follow "Msurvey," which was a social network account created for this research. Links to the pre-test questionnaire and the pre-coded diary questionnaire could be accessed in the "Msurvey". After following the "Msurvey" and reading information regarding the diary study, participants reported their demographic information, personality traits, and customization behaviors in mobile payment usage by answering the pre-test questionnaires. In so doing they registered to participate in the study. The researchers examined the submitted pre-test questionnaires and informed participants regarding their suitability for the diary study. Qualified participants were then required to record all their payment events with the pre-coded diary questionnaire for a period of 5 to 15 days. Each participant was expected to report approximately 15 and no less than 10 events during their recording period. Daily reminders to record payment events were also sent through the social network account. The data collection process covered a period of 2 months.

5 Data Analysis and Results

5.1 Participants

A total of 179 participants registered for this quantitative diary study and finished the pre-test questionnaires. Of these participants, a total of 45 did not meet the participation requirements, leaving 134 valid responses to the pre-test questionnaire for analyzing the impacts of personality traits on customization behaviors. Of the134 participants, there were 60 males and 74 females. Most of the participants were aged between 18 and 30 (85.075%) and used mobile payment services daily (70.149%). The participants held various occupations, but none claimed to be experts in mobile payment security. An overview of the customization behaviors of the 134 participants was also provided. The distribution of the number of customization behaviors exhibited by each participant was as follows: 0 (44.776%), 1 (23.134%), 2 (17.164%), 3 (9.701%), 4 (3.731%), and 5 (1.493%). Among 134 participants, 67 (27 males and 40 females) had recorded at least 10 valid payment events during the 5 to 15-day period. In total, 1094 payment events were collected with the pre-coded diary questionnaire and used to analyze the influences of use context on the relationship between customization behaviors and perceived security. The age distribution is similar to that of the 67 participants: 18 to 25 (35.821%), 26 to 30 (46.269%), 31 to 40 (11.940%), and above 41 (5.970%). The majority (64.179%) of participants used mobile payment services daily, 32.836% used such services weekly, and 2.985% used such services monthly. In term of customization behaviors, more than 60% of participants had customized at least one security setting to protect the security of their mobile payment accounts. Table 5 shows the frequency and percentage of gender, age distribution, frequency of use, and customization behaviors of the sample size.

Table 5. Demographic information of participants

	N=134		N=67	
	Frequency	Percentage (%)	Frequency	Percentage (%)
Gender				
Male	60	44.776	27	40.299
Female	74	55.223	40	59.701
Age distribution				
18-25	56	41.791	24	35.821
26-30	58	43.284	31	46.269
31-40	15	11.194	8	11.940
above 41	5	3.731	4	5.970
Frequency of use				
Daily	94	70.149	43	64.179
Weekly	33	24.627	22	32.836
Monthly	7	5.223	2	2.985
Customization behaviors (number of behaviors)				
0	60	44.776	26	38.806
1	31	23.134	13	19.403
2	23	17.164	13	19.403
3	13	9.701	9	13.433
4	5	3.731	4	5.970
5	2	1.493	2	2.985

5.2 Personality traits and customization behaviors

A total of 134 responses in the pre-test questionnaires were used to examine the relationship between personality traits and customization behaviors. Since the 20-item Mini-IPIP scale has been seldom used within the Chinese population, the scale may need to be refined for use in specific cultures (Zheng et al., 2008). Therefore, the exploratory factor analysis (EFA) was conducted with principal-axis factoring (PAF) to validate the number of latent structures existing in the Mini-IPIP scale in the Chinese context. A new scale, an adapted Mini-IPIP scale, was refined in this study (Wieland, Durach, Kembro & Treiblmaier, 2017; Worthington & Whittaker, 2006).

The reliability of the adapted Mini-IPIP scale was assessed using Cronbach's alpha. The relationships between personality traits and customization behaviors were examined by the Multiple Linear Regression.

The Kaiser-Meyer-Olkin (KMO) test and the Bartlett sphericity test were applied to measure the sampling adequacy of conducting a factor analysis. The KMO test produced a value of 0.678 and Bartlett's test of sphericity was 901.892, with the degree of freedom at 190 (p<0.001), indicating that the scale is suitable for a factor analysis (Nunnally, 1978; Worthington & Whittaker, 2006). In this study, seven components were extracted with principal-axis factoring. All seven components have eigenvalues higher than 1, accounting for a 70.384% variance in total (see Table 6). The correlations among all components are displayed in Table 7.

Table 6. Results of the factor analysis

Pattern Matrix

			Factor							
	Items	Description	1	2	3	4	5	6	7	Communalities
extraversion	e1	I am the life of the party.			0.151		0.210	**0.860**	-0.123	0.545
	e2	I don't talk a lot. (R)	-0.170		**0.745**			0.122		0.532
	e3	I talk to a lot of different people at parties.			0.284			**0.591**	0.122	0.342
	e4	I keep in the background. (R)			**0.864**	0.161		0.248		0.568
agreeableness	a1	I sympathize with other's feelings.	-0.153	**0.656**	-0.335					0.582
	a2	I am not interested in other people's problems. (R)	0.112	**0.820**	0.276			-0.156	-0.101	0.633
	a3	I feel other's emotion.		0.453	-0.230			0.149		0.465
	a4	I am not really interested in others. (R)	0.339	0.497	0.121					0.404
conscientiousness	c1	I get chores done right away.	0.437		-0.148		-0.324	0.492		0.587
	c2	I often forget to put things back in their proper place.	**0.738**							0.584
	c3	I like order.	0.167		-0.118	0.107	-0.438		0.279	0.356
	c4	I make a mess of things. (R)	**0.550**	0.176	-0.100	-0.103		-0.114	0.180	0.560
neuroticism	n1	I have frequent mood swings.	-0.206		0.114	**0.622**		0.251		0.566
	n2	I am relaxed most of the time. (R)	0.366		-0.117	0.397	0.267		-0.307	0.472
	n3	I get upset easily.	-0.221	-0.122	-0.153	**0.636**	-0.133			0.702
	n4	I seldom feel blue. (R)		0.149	0.125	**0.731**		-0.316		0.566
intellect	i1	I have a vivid imagination.	-0.192		-0.128	0.158		0.167	**0.617**	0.586
	i2	I am not interested in abstract ideas. (R)	0.138				**0.746**	0.150	0.146	0.550
	i3	I have difficulty understanding abstract ideas. (R)	0.157	0.117		-0.137	**0.659**		0.174	0.645

	i4	I do not have a good imagination. (R)	0.187	-0.167	0.142		0.159	-0.128	**0.921**	0.764
	Variance %		19.131	15.109	10.128	8.330	6.529	5.980	5.177	
	Eigen values		3.826	3.022	2.026	1.666	1.306	1.196	1.035	

Note: Extraction method: principal-axis factoring; rotation method: Promax with Kaiser Normalization; R refers to the reverse scored item.

Table 7. Results of factor correlations among seven components

Factor	1	2	3	4	5	6
2	0.179					
3	0.010	-0.194				
4	-0.215	-0.255	-0.174			
5	0.339	0.019	0.312	-0.278		
6	-0.257	0.106	-0.431	0.018	-0.442	
7	0.153	0.550	-0.218	-0.193	-0.077	0.296

There are some criteria for factor loadings and cross loadings to determine that the items should be retained or removed in the adapted scale: 1) there should be at least 4:1 items of each factor with a factor loading higher than 0.6, when the sample size consist of 134 responses in this study (Worthington & Whittaker, 2006); 2) To ensure acceptable correlations among items within a construct, the factor loading value should be greater than 0.5 (Hair Jr, Black, Babin and Anderson, 2014); 3) there should be no variable with a cross-loading less than a 0.15 difference from an item's highest factor loading (Farrell, 2010; Farrell & Rudd, 2011; Worthington & Whittaker, 2006). According to these criteria, the result of the factor analysis (see Table 6) suggests that both the extraversion and intellect items are divided and loaded highest in two different components in the Chinese context, respectively. They are extraversion_1 with items of e1 and e3 in component 6, extraversion_2 with items of e2 and e4 in component 3, intellect_1 with items of i2 and i3 in component 5, and intellect_2 with items of i1 and i4 in component 7 (see Table 6 and Table 8). Three items of neuroticism loaded highest in component 4 (neuroticism_1 with items of n1, n3, and n4). There are two items (c2 and c4) constructing conscientiousness_1 in component1 and two items constructing (a1 and a2) agreeableness_1 in component2. Because the loading of the items a3 and a4 from agreeableness, items c1 and c3 from conscientiousness, and the item n2 from neuroticism are relatively smaller in each component, these four items were removed from the adapted Mini-IPIP scale (Wieland et al., 2017). The correlations among all components are lower than 0.71 also indicating a sufficient discriminant validity (Jia & Jia, 2009) (see Table 7).

Table 8. The constructs and Cronbach's alpha of the adapted Mini-IPIP for the Chinese context

Construct	Cronbach's Alpha	Results
extraversion_1		
e1	0.544	Removed
e3		
extraversion_2		
e2	0.677	Retained
e4		
agreeableness_1		
a1	0.497	Removed
a2		
conscientiousness_1		
c2	0.647	Retained
c4		
neuroticism_1		
n1		
n3	0.701	Retained
n4		
intellect_1		
i2	0.727	Retained
i3		
intellect_2		
i1	0.596	Removed
i4		

A Cronbach's alpha value of 0.6 or more is considered acceptable (Hair, Ringle & Sarstedt, 2011; Nunnally, 1978). In this study, Cronbach's alpha values for extraversion_2, conscientiousness_1, neuroticism_1, and intellect_1 were between 0.647 and 0.727 (Table 8). Cronbach's alpha values for extraversion_1 (0.544), agreeableness_1 (0.497), and intellect_2 (0.596) were lower than 0.6. Therefore, this study retained extraversion_2, conscientiousness_1, neuroticism_1, and intellect_1 in the adapted Mini-IPIP scale in the Chinese context for further analysis and removed extraversion_1, agreeableness_1 and intellect_2.

The relationships between personality traits and customization behaviors were examined. A Multiple Linear Regression was calculated to predict customization behaviors based on personality traits with the adapted Mini-IPIP scale in the Chinese context (extraversion_2, conscientiousness_1, neuroticism_1, and intellect_2). The results are shown in Table 9. A significant regression equation was found (F(4, 129)=4.659, $p<0.005$), with an R^2 of 0.126. Both extraversion_2 (β= -0.227, p=0.008) and intellect_2 (β=0.275, p=0.005) were found to have significant effects on customization behaviors, and together they explained 12.6% of the variability of the dependent variable. However, no significant coefficients were found between conscientiousness_1, neuroticism_1, and customization behaviors. Thus, H2 and H6 were all supported, and H3, H4, and H5 were not supported.

Table 9. Standardized coefficients beta of the Multiple Regression Analysis regarding the customization behaviors and personality traits

	Dependent variable	
	Customization behaviors	
	Beta (β)	p
Independent variables		
extraversion_2	-0.227**	0.008
conscientiousness_1	0.034	0.730
neuroticism_1	0.074	0.427
intellect_2	0.275**	0.005

Note: *p < 0.050, **p < 0.010, ***p< 0.005

5.3 Influences of use contexts

A total of 67 participants with 1094 payment events were used to analyze the influence of use context on the relationship between customization behaviors and perceived security. A descriptive analysis was conducted to determine the categories of use context applied in further data analysis by illustrating the distribution of payment events in four perceived security levels. Then, a Spearman's Rank Correlation was conducted to examine the relationship between customization behaviors and perceived security in the overall context. The Spearman's Rank Correlation and the Linear Regression was then applied to evaluate the effects of use context on the relationships between customization behaviors and perceived security.

5.3.1 Perceived security and payment events

A descriptive analysis was applied to determine the distribution of payment events at four levels of perceived security. The classification of levels of perceived security was based on the distribution of payment events. The low level ranged from 0 to 60 points, with 140 payment events; the medium level ranged from 61 to 75 points, with 287 payment events; the high level ranged from 76 to 85, with 368 payment events; and the very high level ranged from 86 to 100, with 299 payment events. Subsequently, the distribution of 1,094 payment events was described in relation to perceived security, according to the task and technical context.

The number of payment events reported by each participant ranged from 10 to 31 (mean = 16.323; standard deviation = 3.169). The mean score of perceived security in each event was 77.683, with a standard deviation of 15.342. Most payment events (87.202%) received a security score greater than 60; however, 12.797% of payment events received a security score of less than 60. This implied that at least one out of every 10 mobile payment events may have been less than satisfactory.

Table 10. Categorization of contextual factors and perceived security

Category	Payment context	Number of events	Percentage (%)	Mean of perceived security
Task context	QR code pay	450	41.133	76.158
	QuickPay	236	21.572	78.559
	M-payment platform pay	304	27.788	79.007
	In-app pay	98	8.958	77.898
	NFC pay	6	0.548	87.167
Technical context	Password	423	38.665	78.627
	Fingerprint	453	41.408	75.289
	No authentication	126	11.517	78.611
	Face ID	43	3.930	89.419
	Password and Fingerprint	34	3.108	73.471
	Others	15	1.371	89.333

Table 10 lists the numbers and percentages corresponding with payment events categorized by two context measures: the task context and the technical context. The data clearly indicates that most payment events occurred in the task context of QR code pay (n = 450), followed by M-payment platform pay (n = 304), QuickPay (n = 236), In-app pay (n = 98), and NFC pay (n = 6). This indicates that mobile payment services based on mobile applications are the most popular in China, but mobile payment services based on NFC technology are rarely used (Wang, Hahn & Sutrave, 2016). In terms of technical context, passwords and fingerprints were the most popular authentication methods, accounting for 38.665% and 41.408%, respectively. For 11.517% of payment events, users also had the option to pay without using any means of authentication. Face ID is still a new authentication method, and it is dependent on the model of mobile device used; the present results indicated that only 3.930% of payment events involved this method. Furthermore, in 34 payment events, users employed a method that combined passwords and fingerprints, which is a secure but inconvenient means of authentication.

The means of perceived security scores in all payment contexts are presented in Table 10. Users' perceived security level was average in most contexts. Except for contexts with low frequency (less than 50 events), the majority of payment contexts corresponded with mean scores between 76 and 79 for perceived security. In terms of task context, the mean scores of perceived security for QuickPay and M-payment platform pay were approximately two points higher than that for QR code pay, and approximately one point higher than that for In-app pay. Among the three most frequently-used authentications, the mean score of perceived security in the technical context of fingerprint authentication (75.289) was slightly lower than that for passwords (78.627) and no authentication (78.611). Surprisingly, users also felt secure when they paid without using any authentication. Payment contexts with less than 50 payment events exhibited either a relatively high perceived security score (above 85) or low perceived security score (below 74). This finding may have been related to the small sample size involved in the analysis.

Participants' perceived security levels may have been affected by the interrelationships between multiple contexts. The distributions of payment events with four perceived security levels in multiple contexts were analyzed using crosstab. To reduce the bias caused by the small sample size, only four task contexts (QR code pay, QuickPay, M-payment platform pay, and In-app pay) and three technical contexts (Fingerprints, Passwords, and No authentication) were selected for analysis. Each of these contexts corresponded with more than 90 payment events. Figure 3 denotes the proportions of payment events in terms of task context, technical context, and perceived security level. The proportions of payment events with fingerprints and passwords are similar in each task context. However, the level of password use grew as the perceived security level increased in QR code pay and QuickPay, whereas fingerprint use exhibited an opposite trend in these two task contexts. Only a minimal number of payments were made without using any authentication in the task contexts of QR code pay, M-payment platform pay, and In-app pay, whereas a large proportion of payments were made with no authentication in QuickPay. Furthermore, although users did not apply any authentication in the QuickPay context, most of these users still reported either a high or very high perceived security level.

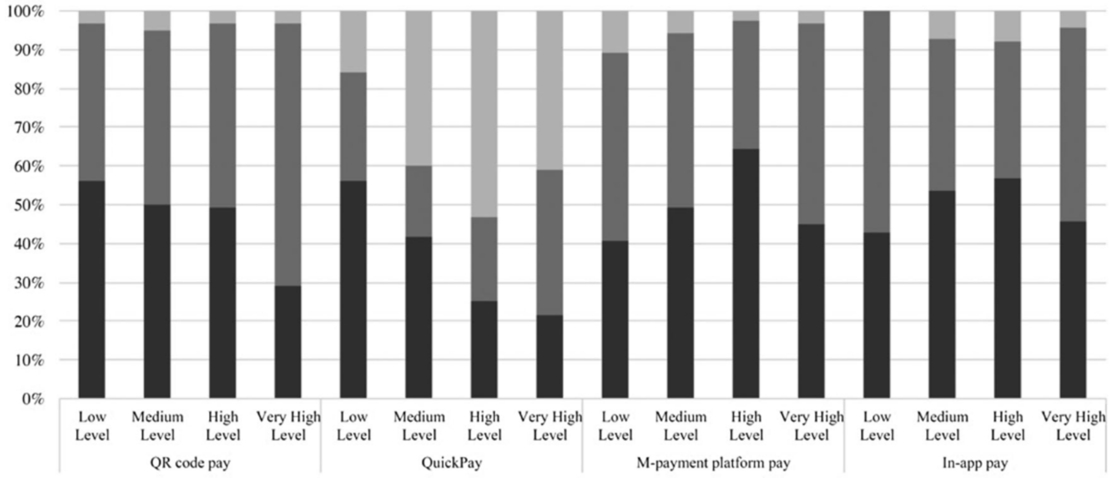

Figure 3. Comparison of the proportions of payment events distributed at four perceived security levels according to task context and technical context

5.3.2 The moderating effects of use context on the relationships between customization behaviors and perceived security

The Spearman's Rank Correlation test was applied to test the relationships between customization behaviors and perceived security in the overall context. A significant correlation was observed between customization behaviors and perceived security (r = 0.136, p = 0.000). Therefore, H1 was supported.

Because social context was recorded using a rating scale, the interaction between customization behaviors in security settings and social context was tested with Linear Regression. There is no significant interaction between the effect of social context and customization behaviors (p = 0.261), but social context has a significant impact on perceived security (see Table 11). The results therefore indicated that social context is a determinant of perceived security rather than a moderator. A Spearman's rank correlation test was conducted to further explore the coefficient between social context and perceived security. A significant correlation was observed between social context and perceived security (r = 0.538, p = 0.000). Thus, H7.3 was not supported.

Table 11. The results of the interaction between customization behaviors and social context

	Dependent Variables Perceived security
	Beta (β)
Independent Variables	
Customization behaviors	0.247*
Social context	0.527***
Customization behaviors × Social context	-0.135

Note: *p < 0.050, **p < 0.010, ***p< 0.005

To investigate the moderating effects of each level of task context and technical context on the influence of customization behaviors on perceived security, the payment events were divided into different groups according to the contextual factors. For instance, four types of task context, namely QR code pay, Quick pay, M-payment platform pay, and In-app pay, represented four moderator levels; three types of technical context, namely passwords, fingerprints, and no authentication method, represented three moderator levels. The moderating effects of each level of one contextual factor were tested by comparing the coefficients between customization behaviors and perceived security among each group in one contextual factor. Spearman's rank correlation test was used to explore the relationships between customization behaviors and users' perceived security (see Table 12).

In terms of the task context, significant correlations were revealed between customization behaviors and perceived security in the task context of QR code pay (r= 0.166, p = 0.000) and M-payment platform pay (r = 0.187, p = 0.001). No significant correlations were found in the task context groups of Quick pay (r = 0.026, p = 0.696) and In-app pay (r = 0.024, p = 0.817). In terms of the technical context, significant correlations were identified between customization behaviors and perceived security in the group of passwords (r = 0.153, p = 0.002) and no authentication (r = 0.435, p = 0.000). Specifically, the coefficient for customization behaviors to perceived security for the no authentication group is much larger than that for passwords. This implies that users who customized a greater number of security settings perceived the transactions to be more secure, particularly when they paid without using authentication methods. However, no correlation existed between customization behaviors and perceived security in the fingerprints group (r = 0.034, p = 0.470) (see Table 12). Therefore, H7.1 and H7.2 were supported.

Table 12. Moderating effects of tasks and technical contexts: significant correlations between customization behaviors and perceived security in different contexts

Moderators		**Correlation between Customization behaviors and perceived security**
Task contexts	QR code pay	0.166***
	Quick pay	0.026
	M-payment platform pay	0.187***
	In-app pay	0.024
Technical contexts	Passwords	0.153***
	Fingerprints	0.034
	No authentication	0.435***

Note: *p < 0.050, **p < 0.010, ***p< 0.005

Table 13 presents the results of the Linear Regression Analysis in the overall context, task context and technical context. Linear relationships were observed among social context, customization behaviors, and perceived security in the overall context (R^2 = 0.268), the task contexts of QR code pay (R^2 = 0.302) and M-payment platform pay (R^2 = 0.282); however, linear relationships only existed between social context and perceived security in the task contexts of QuickPay (R^2 = 0.272) and In-app pay (R^2 = 0.112). The results suggested that in the overall context, the context of QR code pay and M-payment platform pay, users' perceptions of security were influenced by both the social context and customization behaviors, whereas in the task contexts of QuickPay and In-app pay, users' perceptions of security were only influenced by the social context. Additionally, linear relationships were observed among the social context, customization behaviors, and perceived security in the technical context of Passwords ($R^2 = 0.258$) and No authentication ($R^2 = 0.323$), but only between social context and perceived security in the technical context of Fingerprints ($R^2 = 0.216$).

Table 13. Standardized coefficient Beta (β) of the Multiple Regression Analysis regarding perceived security, customization behaviors and social context

			Dependent Variable Perceived security		
			Independent Variable		
			Social context	Customization behaviors	R^2
Overall Effect	Overall context		0.499***	0.120***	0.268
Moderating Effect	Task context	QR code pay	0.516***	0.172***	0.302
		Quick pay	0.522***		0.272
		M-payment platform pay	0.485***	0.187***	0.282
		In-app pay	0.338***		0.112
	Technical context	Passwords	0.481***	0.120**	0.258
		Fingerprints	0.461***		0.216
		No Authentication	0.462***	0.337***	0.323

Note: *p < 0.050, **p < 0.010, ***p< 0.005

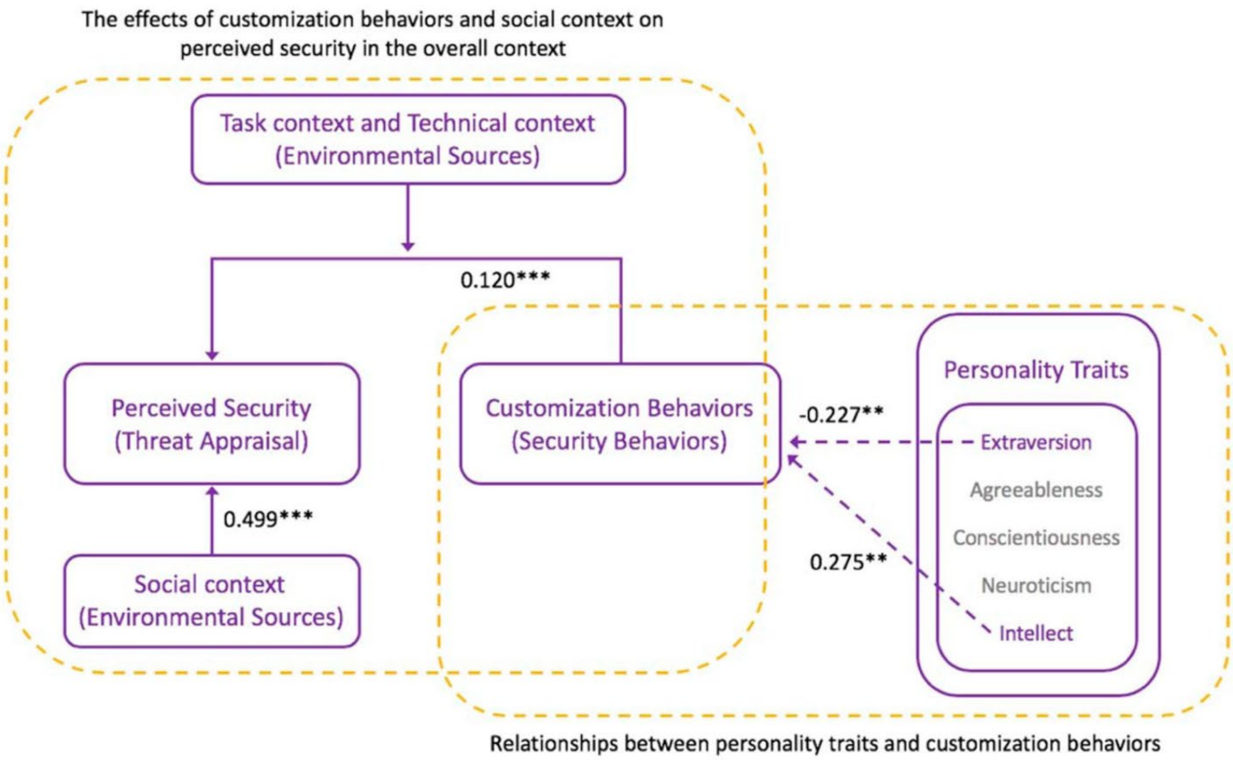
The effects of customization behaviors and social context on perceived security in the overall context
Task context and Technical context (Environmental Sources)
0.120***
Perceived Security (Threat Appraisal)
Customization Behaviors (Security Behaviors)
0.499***
Social context (Environmental Sources)
-0.227**
0.275**
Personality Traits
Extraversion
Agreeableness
Conscientiousness
Neuroticism
Intellect
Relationships between personality traits and customization behaviors

Figure 4. The final result

6 Discussion

6.1 Personality traits to customization behaviors

Although the influence of personality traits on user behaviors has gained increasing attention in recent years, a few studies have discussed its influence on security behaviors in mobile payment services. In this study, extraversion and intellect were found to influence users' customization behaviors in relation to the security settings of mobile payment services. Extraversion has a negative effect on customization behaviors (H2 supported with β= -0.227, p=0.008). This means that users who are introverted tend to customize security settings to protect their accounts, whereas users who are extraverted tend to modify their security settings less in mobile payment services. This may be explained by the fact that users with high scores for extraversion are more likely to be risk takers (Nicholson et al., 2005). They might prefer more convenient payment interactions to ensure an active transaction process. By contrast, introverted people are more likely to be anxious and depressed (Junglas, Johnson & Spitzmüller, 2008), which means that they prefer more complex payment processes to ensure security. Conversely, intellect positively affects customization behaviors (H6 supported with β=0.275, p=0.005). Users with high intellect indicated that they customized more security settings to protect their accounts in mobile payment services and vice versa. In previous studies, many researchers have used the term “openness to experience” rather than “intellect” when measuring personality traits (Donnellan et al., 2006). Also, past research has reported an inconsistent influence of openness on information security, particularly in relation to privacy. For example, some scholars (e.g., Halevi et al., 2013) have suggested that openness could encourage users to disclose privacy information, which leads to an increased privacy risk; however, others (Junglas et al., 2008) have proposed that openness to experience has a positive influence on the concern for privacy, as users with high openness to experience scores are more likely to be aware of risks. However, the measurement items in this study only emphasized users’ intelligent aspects. It is suggested that users with high intelligence scores would perform better in terms of security management. Notably although the personality traits of conscientiousness was found to be statistically significant with regard to security behaviors in previous research (Shropshire et al., 2006; Shropshire et al., 2015; Uffen et al., 2013), it did not have a significant impact on customization behaviors in this study (H4 rejected with β=0.034, p=0.346). This may be because users were expected and even required to take security measures on their personal computer devices or workplace devices in the context of previous studies. In these circumstances, users with higher scores for conscientiousness were more likely to conform to the security rules and implement security practices (Shropshire et al., 2015). Nevertheless, in the context of mobile payment services, customizing security settings is an optional behavior for users. Users generally only undertake such actions when they have higher security needs. Whether users implement security practices thus depends on these security needs rather than obedience to rules, and this may explain why conscientiousness have no effect on customization behaviors in relation to security settings. It was also observed that neuroticism did not have an impact on customization behaviors in mobile payment services (H5 rejected with β=0.074, p=0.427). Whereas previous research has demonstrated that neurotic people experience higher computer anxiety or phishing vulnerability (Halevi et al., 2013; Korzaan & Boswell, 2008), there is minimal evidence to suggest that neuroticism directly influences users’ security practices. Further research could therefore investigate the effects of neuroticism on security behaviors in mobile commerce.

6.2 Customization behaviors and perceived security in relation to use context

The study revealed that the factors that influence perceived security varied according to context. Customization behaviors in relation to security settings only enhance perceived security in the task contexts of QR code pay and M-payment platform pay, or in the technical contexts of passwords and no authentication to pay, whereas the social context predicted users' perceptions of security in each type of task context and technical context. This may be because both QuickPay and In-app pay involve verified payees, and users are more willing to trust merchants. Consequently, the social context takes up all the effect on perceived security. By contrast, QR code pay and M-payment platform pay involve more private-account transactions (such as peer-to-peer payments). Users may have been slower to develop trust in private-account transactions, and extra security behaviors (customizing security settings) could have an effect on perceived security.

Passwords were perceived to be a more secure form of authentication than fingerprints in mobile payment transactions, although they are inconvenient and can be stolen by anyone who can observe them being typed. A previous study by Zimmermann and Gerber (2017) revealed that users were more comfortable using passwords than biometrics in the financial domain). This may be because passwords are not unique, and the textual information can be changed after an account has been hacked. Conversely, a fingerprint comprises unique personal information, which is compromised if an account is hacked (Zimmermann & Gerber, 2017). Notably, users also perceived a higher level of security on average when using no authentication than when using fingerprints in mobile payments. This could be because payments without authentication were mostly performed in the task context of QuickPay, which corresponded to a higher proportion of trustable verified payees. Furthermore, the results revealed that customization behaviors could enhance users' perceived security when they use passwords or no authentication methods, whereas customization behaviors have no impact on users' perceived security when they authorize payments with fingerprints. This explains why users have higher perceived security levels when using passwords and no authentication to pay, as the security behaviors of customizing security settings augment perceived security in these two technical contexts.

6.3 Social context and perceived security

Despite the variety of task contexts and technical contexts, the social context is always an effective predictor of perceived security level in payment transactions (see Table 13). Many studies have demonstrated relationships between trust and perceived security in different research fields, including online banking (Casaló, Flavián & Guinalíu, 2007), acceptance of mobile banking (Vaithilingam, Nair & Guru, 2013), selecting commerce websites (Nilashi et al., 2015), e-commerce systems (Carlos Roca, José García & José de la Vega, 2009; Chellappa & Pavlou, 2002), mobile commerce (Gao & Waechter, 2017), e-payment (Kim, Tao, Shin & Kim, 2010), and mobile payment adoption (Khalilzadeh et al., 2017). However, most of these studies have defined trust as users' perceptions of the trustworthiness of systems or service providers (Carlos Roca et al., 2009; Casaló et al., 2007; Chellappa & Pavlou, 2002; Kim et al., 2010; Vaithilingam et al., 2013; Xin, Techatassanasoontorn & Tan, 2015): few have investigated the relationship between users' trust in payees and perceived security (Gao, Waechter & Bai, 2015; Khalilzadeh et al., 2017; Xin et al., 2015). This study defined the social context as trust in payees and confirmed its influence on perceived security in both offline and online payment scenarios.

However, the findings regarding the relationship between customization behaviors and the social context (trustworthiness to payees) are inconsistent with previous research. The results revealed no statistically significant correlation between customization behaviors and the social context. In other words, the customizability of the interface has no impact on users' trust in payees. Nonetheless, past studies have not only indicated that trust can be enhanced by applying interface design elements, they have also shown that customization of the user interface is one of the trust-inducing factors in e-commerce and m-commerce (Shao et al., 2019; Lee & Benbasat, 2004; Li & Yeh, 2010; Mendoza-González, Martin, Muñoz-Arteaga, Rodríguez & Ochoa Ortíz Zezzatti, 2009; Muñoz-Arteaga, González, Martin, Vanderdonckt & Álvarez-Rodríguez, 2009; Nilashi et al., 2015; Rayport & Jaworski, 2002; Riegelsberger & Sasse, 2001; Wang & Emurian, 2005). The reason for this could be that "trust" in these studies mostly referred to users' trust in the e-commerce or m-commerce systems. Allowing customizability and encouraging customization behaviors are ways to improve user interface quality, which is important for enhancing trust in a system (Zhou, 2013). However, it is understandable that customizing security settings in the interface may not make payees more trustworthy. Further research should be conducted to explore the influencing factors of the social context in mobile payment services.

6.4 Design implications

Our results have three design implications for service providers and designers of mobile payment platforms. Firstly, designers can consider user preferences regarding mobile payment settings based on their personality traits. Currently, service providers can rapidly gather user data, such as demographic information, location, lifestyle, and use habits to improve mobile services or application design to enhance satisfaction (Eastin, Brinson, Doorey & Wilcox, 2016; Xu, Luo, Carroll & Rosson, 2011). To improve satisfaction in mobile use, personality traits are a more predictable factor when examining user behaviors (Nguyen, Maxwell Harper, Terveen & Konstan, 2018; Uffen et al., 2013). However, they are rarely used because personality traits are more intrinsic factors and are therefore difficult to identify. Because the results of this study indicate that personality traits have an influence on customization behaviors in relation to security settings in regard to mobile payments, an important design implication is that designers should consider the different needs of users with different personality traits. Users with higher scores in extraversion tend to modify security settings less because they might be risk takers who prefer convenience over security (Nicholson et al., 2005). By contrast, users with higher scores in intellect prefer to customize their security settings because they tend to pay more attention to security management. Therefore, designers could use personality traits to generate a recommended security system for mobile payments to improve perceived security and user satisfaction (Nguyen et al., 2018). For example, designers could create two default security settings: one with a high level of security, and the other with a high level of convenience. Consequently, users would be recommended appropriate default security settings based on their personality.

Although users with different personality traits make various degrees of effort to modify security in their mobile payment services, it is still beneficial to encourage users to adopt customization and security behaviors. Based on the evidence found in this study, 55.223% of 134 participants reported they had modified at least one security setting. The existence of active customization behaviors implies that users might not have been burdened with the inconvenience that authentication systems cause. Nevertheless, in most current mobile payment systems (such as Alipay and WeChat pay), the default security settings tend to be designed for convenience rather than security. Although these systems previously allowed users to modify authentication settings or privacy settings, users' ability to customize the settings is decreasing as the applications are updated. For example, before 2019 users could set a daily payment limit to protect their account in the mobile payment version; however, this setting was removed in the latest version (Jul, 2019).

The findings also revealed an inconsistency with published research regarding users' attitudes toward authentication systems vis-à-vis the balance between convenience and security. Previous studies have explored the use context of authentication strategy in relation to personal computers or web-based services, where users preferred to sacrifice security for usability and convenience (Hayashi & Hong, 2011; Tam et al., 2010; Weir, Douglas, Carruthers & Jack, 2009). However, in terms of mobile payments, it was observed in this study that most users made efforts to secure their money and privacy, and these efforts resulted in perceptions of greater security. Thus, we suggest that users should be afforded greater authority to customize security settings in mobile payment services, even though the mobile system may be sufficiently secure.

Additionally, the findings suggest that security could have priority over convenience based on the context of use, particularly in the task contexts of QR code pay and M-payment platform pay. This is because a greater number of private-accounts, which tend to gain a low level of trust, were involved in these two contexts. Thus, the effect of extra security management behaviors was exhibited in maintaining perceived security levels. Accordingly, designers should consider the provision of visual cues (such as text information and icon designs displayed during the payment) and to assist users to estimate the trustworthiness of payees in the payment interaction. Security settings could also be designed so that they can be altered by users according to the situation.

6.5 Limitations

This study has several limitations that must be addressed. First, this study was mainly based on a quantitative diary method, which required participants to record their payment events during a certain period. This may have resulted in data being underreported. For example, participants may have forgotten to report payment events on a particular day for various reasons. Ohly et al. (2010) have indicated that underreporting does not seriously cause bias in results. Nevertheless, participants were sent a daily reminder to avoid this possibility. Another problem was that participants may have completed the diary questionnaires long after the events occurred or may have reported multiple events simultaneously at the end of a day because recording events several times a day was perceived to be burdensome. Thus, a pre-coded diary questionnaire was developed based on the interviews to address this potential problem. Participants were asked to report events as promptly and as often as possible. However, the pre-coded diary questionnaire restricted the possibility of exploring information in greater depth (Rahman, 2017). For example, the reason why users perceived security to be higher when using passwords than when using fingerprints in mobile payments remained unclear. Future studies could address this question.

Second, this study applied non-random-internet sampling to recruit suitable participants, which may have led to a sampling bias. Nevertheless, the population value was not the main concern in this study and the convenience sampling method was able fulfil the needs of this research. Additionally, this study may have benefitted from a larger sample. The current sample prevented analysis of some contexts, such as the task context of NFC pay and the technical context of Face ID, due to a lack of data in these contexts.

Finally, some inappropriate items from the Mini-IPIP scale were deleted using the factor analysis. The scale (the adapted Mini-IPIP scale in the Chinese context) used to measure participants' personality traits in this study was adapted from the Mini-IPIP scale. This is because some items in the Mini-IPIP may not have cross-cultural concurrent validation. For example, both e1 ("I am the life of the party.") and e3 ("I talk to a lot of different people at parties.") were used to assess an individual's extraversion level, but these two items exhibited low factor loadings. This may be because the term "party" is an uncommon concept in Chinese culture. Even though an individual is energetic, active and sociable (Donnellan et al., 2006; Halevi et al., 2013), they may not necessarily have attended a party or been active and sociable at a party. Therefore, removing these inappropriate items is beneficial to ensure the internal consistency of the scale. The values of factor loadings, cross loadings and factor correlations provided by the Exploratory Factor Analysis (see Table 6 and Table 7) have supported the construct validity of the new scale (Farrell, 2010; Farrell & Rudd, 2011; Hair Jr, Black, Babin & Anderson, 2014; Jia & Jia, 2009; Worthington & Whittaker, 2006). Future studies could improve the scale for use in the Chinese context by involving other items from the 50-item IPIP-FFM to perform Confirmatory Factor Analysis for examining the model fit. Furthermore, this study did not examine the impact of agreeableness_1 on customization behaviors because of the unacceptable Cronbach's alpha value of agreeableness_1 (0.497). Since the items of agreeableness from the Mini-IPIP scale may not be suitable for assessing an individual's traits in the Chinese context, further studies could attempt to examine other items from the original IPIP pool to measure Chinese traits of agreeableness.

7 Conclusion

This quantitative diary study investigated users' perceptions of the security of mobile payments in real life. The results of this study have several implications for mobile payment services providers and interface designers. The primary contribution of this study is that it reveals the relationships among users' personality traits, customization behaviors, and perceived security in mobile payments. Customization behaviors have a significant effect on users' security perceptions when using mobile payment services. Users take the initiative in modifying settings to enhance the security of mobile payment services. This implies that many users have a need for design customization in security settings and prefer security over convenience in mobile payment usage. Furthermore, we investigated the intrinsic factors of personality traits that trigger users to engage in customization behaviors and found that two personality traits are effective predictors.

The identification of the moderating role of use context on the relationship between customization behaviors and perceived security was particularly vital in this study. The influence of customization behaviors on perceived security varies according to the use context. Specifically, effect of customization behaviors on perceived security was only significant on the task contexts of QR code pay and M-payment platform pay and on the technical contexts of passwords to pay and no authentication to pay. However, although we also expected the social context to moderate the relationship between customization behaviors and perceived security, the findings showed that social context (trust in payees) is a factor influencing perceived security. This implies that the security settings of mobile payment services should be based on the use context, because users will have different security needs according to this context. Above all else, users' trust in payees is a priority when designing security experiences for mobile payment services.

Reference

Abrazhevich, D., Markopoulos, P., & Rauterberg, M. (2009). Designing Internet- Based Payment Systems: Guidelines and Empirical Basis Designing. *Human- Computer Interaction*, *24*(4), 408–443. https://doi.org/10.1080/07370020903038144

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613–643.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 179–211.

Arrasvuori, J., Boberg, M., & Korhonen, H. (2010). Understanding Playfulness: An Overview of the Revised Playful Experience (PLEX) Framework. In *Design & Emotion 2010 Conference, Design and Emotion Society* (pp. 1–12).

Bandura A. (1986). Social foundations of thoughts and action: a social cognitive theory. Englewood Cliffs, NJ: Prentice Hall.

Barnard, L., Yi, J. S., Jacko, J. A., & Sears, A. (2007). Capturing the effects of context on human performance in mobile computing systems. *Personal and Ubiquitous Computing*, *11*(2), 81–96. https://doi.org/10.1007/s00779-006-0063- x

Baron, R. M., & Kenny, D. A. (1986). The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual Strategic and Statistical Considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173– 1182. https://doi.org/10.1007/BF02512353

Belk, R. W. (1974). An exploratory assessment of situational effects in buyer behavior. *Journal of Marketing*, *11*(2), 156–163. https://doi.org/10.2307/3150553

Blom, J. O., & Monk, A. F. (2003). Theory of Personalization of Appearance: Why Users Personalize Their PCs and Mobile Phones. *Human-Computer Interaction*, *18*(3), 193–228.

Bolger, N., Davis, A., & Rafaeli, E. (2003). Diary Methods: Capturing Life as it is Lived. *Annual Review of Psychology*, *54*(1), 579–616. https://doi.org/10.1146/annurev.psych.54.101601.145030

Carlos Roca, J., José García, J., & José de la Vega, J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management and Computer Security*, *17*(2), 96–113. https://doi.org/10.1108/09685220910963983

Casaló, L. V, Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review*, *31*(5), 583–603. https://doi.org/10.1108/14684520710832315

Payment & Clearing Association of China (2019), 2018 China Mobile Payment Development Report. Retrieved December, 2019 from http://www.pcac.org.cn/index.php/focus/list_details/ids/654/id/50/topicid/3.html

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15*(5/6), 358–368. https://doi.org/10.1108/09576050210447046

Colobran, M. (2016). Modeling human perceived security: A conceptual framework and its application to health. *Computers in Human Behavior*, *62*, 1–8. https://doi.org/10.1016/j.chb.2016.03.050

Cooper, A. J., Smillie, L. D., & Corr, P. J. (2010). A confirmatory factor analysis of the Mini-IPIP five-factor model personality scale. *Personality and Individual Differences*, *48*(5), 688–691. https://doi.org/10.1016/j.paid.2010.01.004

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors. *The DATA BASE for Advances in Information Systems*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Dahlberg, T., Guo, J., & Ondrus, J. (2015). A critical review of mobile payment research. *Electronic Commerce Research and Applications*, *14*(5), 265–284. https://doi.org/10.1016/j.elerap.2015.07.006

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information and Computer Security*, *24*(1), 116–134. https://doi.org/10.1108/ICS-04-2015- 0018

Deci, E. L., & Ryan, R. M. (2012). Self-determination theory. In P. A. M. Van Lange, A. W. Kruglanski, & E. T. Higgins (Eds.), *Handbook of theories of social psychology* (pp. 416–436). Sage Publications Ltd. https://doi.org/10.4135/9781446249215.n21

Dey, A. K. (2001). Understanding and Using Context. *Personal and Ubiquitous Computing*, *5*, 4–7. https://doi.org/10.1371/journal.pone.0154625

Dey, A. K., Abowd, G. D., & Salber, D. (2001). A Conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications. *Human-Computer Interaction*, *16*(2–4), 97–166.

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

Dourish, P., Grinter, R. E., De La Flor, J. D., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, *8*(6), 391–401. https://doi.org/10.1007/s00779-004-0308-5

Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior*, *58*, 214–220. https://doi.org/10.1016/j.chb.2015.12.050

Engl, S., & Nacke, L. E. (2013). Contextual influences on mobile player experience - A game user experience model. *Entertainment Computing*, *4*(1), 83–91. https://doi.org/10.1016/j.entcom.2012.06.001

Fan, J., Shao, M., Li, Y., & Huang, X. (2018). Understanding users' attitude toward mobile payment use: A comparative study between China and the USA. *Industrial Management and Data Systems*, *118*(3), 524–540. https://doi.org/10.1108/IMDS-06-2017-0268

Farrell, A. M. (2010). Insufficient discriminant validity: A comment on Bove, Pervan, Beatty, and Shiu (2009). *Journal of Business Research*, *63*(3), 324–327. https://doi.org/10.1016/j.jbusres.2009.05.003

Farrell, A. M., & Rudd, J. M. (2011). Factor analysis and discriminant validity: A brief review of some practical issues. In *In Proceedings of the Australia-New Zealand Marketing Academy Conference (ANZMAC)*.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Gao, L., & Waechter, K. A. (2017). Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation. *Information Systems Frontiers*, *19*(3), 525–548. https://doi.org/10.1007/s10796-015-9611-0

Gao, L., Waechter, K. A., & Bai, X. (2015). Understanding consumers' continuance intention towards mobile purchase: A theoretical framework and empirical study - A case of China. *Computers in Human Behavior*, *53*, 249–262. https://doi.org/10.1016/j.chb.2015.07.014

Global Web (2017). CCTV 315 broadcast "allotransplanting" 360 experts decryption cracked principle. Retrieved December, 2018 from http://svein.cn/en/article/17.html

Goeke, L., & Pousttchi, K. (2010). A scenario-based analysis of mobile payment acceptance. In *2010 Ninth International Conference on Mobile Business and 2010 Ninth Global Mobility Roundtable (ICMB-GMR)* (pp. 371–378). IEEE. https://doi.org/10.1109/ICMB-GMR.2010.81

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*, 7–28.

Goldberg, Lewis R. (2018) International Personality Item Pool: A Scientific Collaboratory for the Development of Advanced Measures of Personality Traits and Other Individual Differences (http://ipip.ori.org/). Internet Web Site.

Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the Big-Five personality domains. *Journal of Research in Personality*, *37*(6), 504– 528. https://doi.org/10.1016/S0092-6566(03)00046-1

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers and Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Gross, J. B., & Rosson, M. B. (2007). Looking for Trouble: Understanding End-User Security Management. In *the 2007 Symposium on Computer Human interaction For the Management of information Technology* (p. Article No.10). New York, USA: ACM. https://doi.org/10.1145/1234772.1234786

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–151. https://doi.org/10.2753/MTP1069-6679190202

Hair Jr, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate Data Analysis*. USA: Pearson. https://doi.org/10.1007/978-3-319-01517-0_3

Halevi, T., Lewis, J., & Memon, N. (2013). A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits. In *the 22nd International Conference on World Wide Web* (pp. 737–744). New York, USA: ACM. https://doi.org/10.1145/2487788.2488034

Hanus, B., & Wu, Y. A. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*(1), 2–16. https://doi.org/10.1080/10580530.2015.1117842

Hartono, E., Holsapple, C. W., Kim, K. Y., Na, K. S., & Simpson, J. T. (2014). Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. *Decision Support Systems*, *62*, 11–21. https://doi.org/10.1016/j.dss.2014.02.006

Hayashi, E., & Hong, J. (2011). A diary study of password usage in daily life. In *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11* (p. 2627). https://doi.org/10.1145/1978942.1979326

Hays, R. D., Liu, H., & Kapteyn, A. (2015). Use of Internet panels to conduct surveys. *Behavior Research Methods*, *47*(3), 685–690. https://doi.org/10.3758/s13428-015-0617-9

He, W. (2018). Alipay makes changes after privacy criticism. Retrieved December, 2018 from http://www.chinadaily.com.cn/a/201801/05/WS5a4eb557a31008cf16da5288.html

Huang, D.-L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour and Information Technology*, *29*(3), 221–232. https://doi.org/10.1080/01449290701679361

iiMedia Rsearch (2017). 2017H1 China Third Party Mobile Payment Market Research Report. Retrieved December, 2018 from http://www.iimedia.cn/53957.html

Jia, R., & Jia, H. H. (2009). Factorial validity of problematic Internet use scales. *Computers in Human Behavior*, 25(6), 1335–1342. https://doi.org/10.1016/j.chb.2009.06.004

Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. *Computers in Human Behavior*, *79*, 111–122. https://doi.org/10.1016/j.chb.2017.10.035

Johnston, & Warkentin. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*(3), 549. https://doi.org/10.2307/25750691

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*(4), 387–402. https://doi.org/10.1057/ejis.2008.29

Kearney, W. D., & Kruger, H. A. (2016). Theorising on risk homeostasis in the context of information security behaviour. *Information and Computer Security*, *24*(5), 496–513. https://doi.org/10.1108/ICS-04-2016-0029

Khalilzadeh, J., Ozturk, A. B., & Bilgihan, A. (2017). Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. *Computers in Human Behavior*, *70*(2017), 460–474. https://doi.org/10.1016/j.chb.2017.01.001

Kim, C., Tao, W., Shin, N., & Kim, K. S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, *9*(1), 84–95. https://doi.org/10.1016/j.elerap.2009.04.014

Kim, K., Schmierbach, M. G., Bellur, S., Chung, M.-Y., Fraustino, J. D., Dardis, F., & Ahern, L. (2015). Is it a sense of autonomy, control, or attachment? Exploring the effects of in-game customization on game enjoyment. *Computers in Human Behavior*, *48*, 695–705. https://doi.org/10.1016/j.chb.2015.02.011

Kjeldskov, J., & Skov, M. B. (2014). Was it worth the hassle?: ten years of mobile HCI research discussions on lab and field evaluations. In *the 16th international conference on Human-computer interaction with mobile devices & services* (pp. 43–52). New York, USA: ACM. https://doi.org/10.1145/2628363.2628398

Korhonen, H., Arrasvuori, J., & Väänänen-Vainio-Mattila, K. (2010). Analysing user experience of personal mobile products through contextual factors. In *the 9th International Conference on Mobile and Ubiquitous Multimedia* (p. Article No.11). New York, USA: ACM. https://doi.org/10.1145/1899475.1899486

Kortum, P., & Oswald, F. L. (2018). The Impact of Personality on the Subjective Assessment of Usability. *International Journal of Human–Computer Interaction*, *34*(2), 177–186. https://doi.org/10.1080/10447318.2017.1336317

Korzaan, M. L., & Boswell, K. T. (2008). The Influence of Personality Traits and Information Privacy Concerns on Behavioral Intentions. *Journal of Computer Information Systems*, *48*(4), 15–24. https://doi.org/https://doi.org/10.1080/08874417.2008.11646031

Lee, Y. E., & Benbasat, I. (2004). A Framework for the Study of Customer Interface Design for Mobile Commerce. *International Journal of Electronic Commerce*, *8*(3), 79–102. https://doi.org/10.1080/10864415.2004.11044299

Li, Y.-M., & Yeh, Y.-S. (2010). Increasing trust in mobile commerce through design aesthetics. *Computers in Human Behavior*, *26*(4), 673–684. https://doi.org/10.1016/j.chb.2010.01.004

Liang, T. P., & Yeh, Y. H. (2011). Effect of use contexts on the continuous use of mobile services: The case of mobile games. *Personal and Ubiquitous Computing*, *15*(2), 187–196. https://doi.org/10.1007/s00779-010-0300-1

Mahatanankoon, P., Wen, H. J., & Lim, B. (2005). Consumer-based m-commerce: Exploring consumer perception of mobile applications. *Computer Standards and Interfaces*. https://doi.org/10.1016/j.csi.2004.10.003

Mallat, N. (2007). Exploring consumer adoption of mobile payments – A qualitative study. *The Journal of Strategic Information Systems*, *16*(4), 413–432. https://doi.org/10.1016/j.jsis.2007.08.001

Mallat, N., Rossi, M., Tuunainen, V. K., & Anssi, O. (2009). The impact of use context on mobile services acceptance: The case of mobile ticketing. *Information & Management*, *46*(3), 190–195. https://doi.org/10.1016/j.im.2008.11.008

Marathe, S., & Sundar, S. S. (2011). What drives customization? Control or Identity? In *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11* (pp. 781–790). https://doi.org/10.1145/1978942.1979056

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139–150. https://doi.org/10.1016/j.chb.2018.11.002

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems*, *34*(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Mendoza-González, R., Martin, M. V., Muñoz-Arteaga, J., Rodríguez, F. Á., & Ochoa Ortíz Zezzatti, C. A. (2009). Web service-security specification based on usability criteria and pattern approach. *Journal of Computers*, *4*(8), 705–712. https://doi.org/10.4304/jcp.4.8.705-712

Muñoz-Arteaga, J., González, R. M., Martin, M. V., Vanderdonckt, J., & Álvarez- Rodríguez, F. (2009). A methodology for designing information security feedback based on User Interface Patterns. *Advances in Engineering Software*, *40*(12), 1231–1241. https://doi.org/10.1016/j.advengsoft.2009.01.024

Multiple Payment Methods of WeChat Pay. (n.d.) Retrieved December, 2018 from https://pay.weixin.qq.com/wechatpay_guide/intro_method.shtml

Nguyen, T. T., Maxwell Harper, F., Terveen, L., & Konstan, J. A. (2018). User Personality and User Satisfaction with Recommender Systems. *Information Systems Frontiers*, *20*(6), 1173–1189. https://doi.org/10.1007/s10796-017-9782- y

Nicholson, N., Soane, E., Fenton-O'Creevy, M., & Willman, P. (2005). Personality and domain-specific risk taking. *Journal of Risk Research*, *8*(2), 157–176. https://doi.org/10.1080/1366987032000123856

Nilashi, M., Ibrahim, O., Reza Mirabi, V., Ebrahimi, L., & Zare, M. (2015). The role of Security, Design and Content factors on customer trust in mobile commerce. *Journal of Retailing and Consumer Services*, *26*, 57–69. https://doi.org/10.1016/j.jretconser.2015.05.002

Nunnally, J. C. (1978). *Psychometric Theory*. New York, NY: McGraw-Hill.

Ohly, S., Sonnentag, S., Niessen, C., & Zapf, D. (2010). Diary Studies in Organizational Research- An Introduction and Some Practical Recommendations. *Journal of Personnel Psychology*, *9*, 79–93. https://doi.org/10.1027/1866-5888/a000009

Payment Products of Alipay. (n.d.). Retrieved December, 2018 from https://intl.alipay.com/open/product.htm

Radke, K., Boyd, C., Nieto, J. G., & Buys, L. (2013). "Who decides?" Security and Privacy in the Wild. In *the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration* (pp. 27–36). New York, USA: ACM. https://doi.org/10.1145/2541016.2541043

Rahman, M. S. (2017). The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language "Testing and Assessment " Research: A Literature Review. *Journal of Education and Learning*, *6*(1), 102– 112. https://doi.org/10.5539/jel.v6n1p102

Rayport, J. F., & Jaworski, B. J. (2002). *Cases in e-commerce*. Boston: McGraw- Hill/Irwin.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, *28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Riegelsberger, J., & Sasse, A. (2001). Trustbuilders and trustbusters - The role of trust cues in interfaces to e-commerce applications. In B. Schmid, K. Stanoevska- Slabeva, & V. Tschammer (Eds.), *Towards the E-Society. IFIP International Federation for Information Processing* (Vol. 74, pp. 17–30). Boston, MA: Springer. https://doi.org/https://doi.org/10.1007/0-306-47009-8_2

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91, 1, 93–114.

Rogers, R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo, J., Petty, R. (Eds.), Social Psychophysiology: a source book. New York: Guilford Press.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Saldaña, J. (2015). *The Coding Manual for Qualitative Researchers*. (J. Seaman, Ed.) (Second). SAGE. https://doi.org/10.1017/CBO9781107415324.004

Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems*, *101*(4), 165–177. https://doi.org/10.1108/02635570110390071

Schwiderski-Grosche, S., & Knospe, H. (2002). Secure mobile commerce. *Electronics & Communication Engineering Journal*, *14*(5), 228–238. https://doi.org/10.1049/ecej:20020506

Shao, Z., Zhang, L., Li, X., & Guo, Y. (2019). Antecedents of trust and continuance intention in mobile payment platforms: The moderating effect of gender. *Electronic Commerce Research and Applications*, *33*, 1–10. https://doi.org/10.1016/j.elerap.2018.100823

Shin, D. H. (2009). Towards an understanding of the consumer acceptance of mobile wallet. *Computers in Human Behavior*, *25*(6), 1343–1354. https://doi.org/10.1016/j.chb.2009.06.001

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. In *Proceedings of the Twelfth Americas Conference on Information Systems* (pp. 3443–3449). Acapulco, Mexico: Association for Information Systems.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers and Security*, *49*, 177–191. https://doi.org/10.1016/j.cose.2015.01.002

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: A tradeoff between security and convenience. *Behaviour and Information Technology*, *29*(3), 233–244. https://doi.org/10.1080/01449290903121386

Tarasewich, P. (2003). Desiging mobile commerce application. *Communications of the ACM*, *46*(12), 57–60.

Tossell, C. C., Kortum, P., Shepard, C., Rahmati, A., & Zhong, L. (2012). An empirical analysis of smartphone personalisation: Measurement and user variability. *Behaviour and Information Technology*, *31*(10), 995–1010. https://doi.org/10.1080/0144929X.2012.687773

Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers and Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

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*, 203–212. https://doi.org/10.4236/jis.2013.44023

Vaithilingam, S., Nair, M., & Guru, B. K. (2013). Do Trust and Security Matter for the Development of M-banking? Evidence from a Developing Country. *Journal of Asia-Pacific Business*, *14*(1), 4–24. https://doi.org/10.1080/10599231.2013.728402

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, *21*(1), 105–125. https://doi.org/10.1016/j.chb.2003.11.008

Wang, Y., Hahn, C., & Sutrave, K. (2016). Mobile payment security, threats, and challenges. In *the 2016 2nd Conference on Mobile and Secure Services, MOBISECSERV 2016* (pp. 1–5). IEEE. https://doi.org/10.1109/MOBISECSERV.2016.7440226

Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, *28*(1–2), 47–62. https://doi.org/10.1016/j.cose.2008.09.008

Wieland, A., Durach, C. F., Kembro, J., & Treiblmaier, H. (2017). Statistical and judgmental criteria for scale purification. *Supply Chain Management*, *22*(4), 321–328. https://doi.org/10.1108/SCM-07-2016-0230

Wigelius, H., & Väätäjä, H. (2009). Dimensions of Context Affecting User Experience in Mobile Work. In T. Gross (Ed.), *Human-Computer Interaction – INTERACT 2009. INTERACT 2009. Lecture Notes in Computer Science* (pp. 604–617). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642- 03658-3_65

Wolf, F., Kuber, R., & Aviv, A. J. (2018). An empirical study examining the perceptions and behaviours of security-conscious users of mobile authentication. *Behaviour & Information Technology*, *37*(4), 320–334. https://doi.org/10.1080/0144929X.2018.1436591

Worthington, R. L., & Whittaker, T. A. (2006). Scale Development Research: A Content Analysis and Recommendations for Best Practices. *The Counseling Psychologist*, *34*(6), 806–838. https://doi.org/10.1177/0011000006288127

Xin, H., Techatassanasoontorn, A. A., & Tan, F. B. (2015). Antecedents of Consumer Trust in Mobile Payment. *Journal of Computer Information Systems*, *55*(4), 1– 10. https://doi.org/10.1007/s10854-017-7534-x

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42–52. https://doi.org/10.1016/j.dss.2010.11.017

Zhang, X. J., Li, Z., & Deng, H. (2017). Information security behaviors of smartphone users in China: An empirical analysis. *Information Security Behaviors*, 35(6), 1177–1190. https://doi.org/10.1108/EL-09-2016-0183

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management and Computer Security*, *17*(4), 330–340. https://doi.org/10.1108/09685220910993980

Zheng, L., Goldberg, L. R., Zheng, Y., Zhao, Y., Tang, Y., & Liu, L. (2008). Reliability and concurrent validation of the IPIP Big-Five factor markers in China: Consistencies in factor structure between Internet-obtained heterosexual and homosexual samples. *Personality and Individual Differences*, *45*(7), 649– 654. https://doi.org/10.1016/j.paid.2008.07.009

Zhou, T. (2013). An empirical examination of continuance intention of mobile payment services. *Decision Support Systems*, *54*(2), 1085–1091. https://doi.org/10.1016/j.dss.2012.10.034

Zhou, T., & Lu, Y. (2011). The effects of personality traits on user acceptance of mobile commerce. *International Journal of Human-Computer Interaction*, *27*(6), 545–561. https://doi.org/10.1080/10447318.2011.555298

Zimmermann, V., & Gerber, N. (2017). “If It Wasn’t Secure, They Would Not Use It in the Movies” – Security Perceptions and User Acceptance of Authentication Technologies. In T. Tryfonas (Ed.), *Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science* (pp. 265– 283). Cham: Springer. https://doi.org/10.1007/978-3-319-58460-7_18

List of figures

List of tables