https://doi.org/10.1016/j.ijhcs.2021.102675

Interaction Design for Security Based on Social Context

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

Keywords: Human-Computer Interaction for security; task-technology fit theory (TTF); design science research (DSR); social context; perception of security and usability; mobile payments

1 Introduction

Compared with the primary task regarding the use of mobile technologies, security is a secondary priority (Karat et al., 2005). However, security is a critical issue in the adoption and development of mobile payments (de Kerviler et al., 2016; Johnson et al., 2018; Oliveira et al., 2016; Zhang et al., 2019). Even though mobile payments have been considered to be a securer way of processing payments compared to traditional payment methods (Huh et al., 2017; Johnson et al., 2018), many users still require better security designs in mobile payment transactions (Beutin and Schadbach, 2017; Huh et al., 2017; Shao et al., 2019; Zhang and Luximon, 2020). For instance, 55% of German respondents claimed that security and data protection is the primary concern for mobile payment adoption in 2017 (Beutin and Schadbach, 2017); more than 50% of interviewees thought that security and privacy problems were the number one reason for not adopting Apple Pay in the United States (Huh et al., 2017); specifically, 77.8% of users asked for improved security features, such as better feedback warnings (79.2%), authentication processes (52.3%), and account management capabilities (38.7%), in mobile payment services, according to the survey result provided by the Payment and Clearing Association of China (PCAC, 2019). Security design should support users with appropriate functions and information to access the system securely (Yee, 2003). Currently, people can manage the security of their mobile transactions using a variety of settings and with the help of system information. However, mobile payments can be applied in various situations, which require different levels of security protections (Ion et al., 2010). Even though designers and practitioners allow various security functions in terms of these services, it can be a burden managing them according to different payment situations. Users may apply the undesired security functions during such transactions, and then complain about security design which not match with the payment tasks in use contexts (Shao et al., 2019; Zhang and Luximon, 2020).

Scholars have applied use contexts to refer to any situational information related to interactions (Dey, 2001; Liang et al., 2013) and the critical role of use context in mobile payments has been recognized by many researchers (Khalilzadeh et al., 2017; Kim et al., 2010; Mallat, 2007; Mallat et al., 2009; Zhang and Luximon, 2020). It is reasonable to consider the effect of use contexts since mobile services are ubiquitous (Botha et al., 2009). In mobile technologies research, studies have suggested contextual factors that describe the use context of mobile technologies, such as task, personal, social, spatial, temporal, infrastructural, device, service, and access network (Korhonen et al., 2010; Wigelius and Väätäjä, 2009). Among them, social context, which highlights relationships and interactions between payers and payees (Lu and Yang, 2014), could play a critical role in security design of mobile payments. This is because mobile payment services are considered to be technically sound in security (Johnson et al., 2018), users' preferences for security design could lie in who they interact with and how they interact with those people. So far, there is insufficient knowledge about the fit between security design and payment tasks in different social contexts.

The task-technology fit (TTF) theory explains the influences of fit on technology use, and indicates that service providers should design functionality that matches with users' requirements of performing tasks in the situated context (Tam and Oliveira, 2015; Gebauer et al., 2010; Goodhue and Thompson, 1995). Specifically, the "fit" not only refers to the good match between situated task and users' preferences for functionality, but also indicates a positive perception and attitude toward the technology (Tam and Oliveira, 2015; Chang, 2010).

With the above rationale, there is a gap in understanding the fit between security design and social context in mobile payments. We attempt to close this gap by investigating users' preferences for security design according to social contexts and perceptions of security and usability contextually, and to, therefore, provide implications for security design, which could help assign security design based on social contexts. We seek to close the research gap by addressing the following research question: how do social contexts influence users' preferences and perceptions for security design in mobile payments?

This study focuses on two types of security design: security settings (e.g. authentication settings, payment settings, privacy settings) and feedback design (e.g. providing feedback on status information, identify information, and risk information) in mobile payments. Therefore, the research question can be divided into three sub-questions:

Sub-RQ1: What are the preferences regarding security settings in different social contexts?

Sub-RQ2: Does feedback design influence the preferences regarding security settings in different social contexts?

Sub-RQ3: How should security settings and feedback design be assigned in different social contexts according to perceptions of security and usability?

To address these research questions, we executed a full factorial design experiment to control the conditions of feedback design and social contexts when using mobile payment services and to explain the variances in behaviors in relation to security settings and perceptions of security and usability in different conditions. Following a design science research approach, we created prototypes and payment scenarios to achieve our research goal of understanding the fit between security design and social contexts. To be specific, we developed customizable interfaces to investigate security setting preferences by observing behaviors in relation to security settings and manipulated feedback design in these customizable interfaces to measure how feedback information affects security setting preferences and perceptions of security and usability according to various social contexts. Our findings provide insights into the fit between security design and social contexts and discuss the fit by considering users' preferences and the perceptions of security and usability.

2 Literature Review

2.1 Theoretical Background

Task-technology fit (TTF) theory has been widely used to explain how the fit between task characteristics (e.g. the complexity of the task; routine or non-routine tasks), technology (e.g. functions or tools provided by the system), and individual characteristics (e.g. ability, demographic features) affects performance and utilization (Goodhue and Thompson, 1995; Kim et al., 2010; Zigurs and Buckland, 1998). In recent years, researchers have applied TTF to explain users' performance in terms of mobile technology use, such as mobile banking (Yuan et al., 2016; Zhou et al., 2010), mobile commerce (Kim et al., 2015; Liang et al., 2013), and mobile locatable information systems (Junglas et al., 2008). However, the ubiquitous nature of mobile technologies also suggests the necessity of considering the influences of use context in TTF (Gebauer et al., 2010) as mobile interactions can be influenced by changing situations. Use context involves personal and environmental situations that are related to interactions (Kim et al., 2015). Mobile technologies can fit with a task in one circumstance but be unsuitable for another situation. Researchers have applied TTF to explain situational needs and fits by employing use context and its contextual factors. For example, Junglas, Abraham, and Watson (2008) used TTF to explain task performance in mobile locatable information systems. Gebauer, Shaw, and Gribbins (2010) included three factors of use context (distraction, connectivity, and mobility) to understand the fit between technology and use context in a mobile information system; Kim et al. (2015) studied the fit between use context and mobile services by studying the contextual factors of time saving and mobility. However, use context is complex as its contextual factors highly depend on relevant services and specific needs in terms of technologies (Dey, 2001; Jarvenpaa and Lang, 2005).

On the other hand, research has applied TTF to predict technology adoption and continuous adoption use in mobile technologies, with a combination of the technology acceptance model (TAM), the theory of planned behavior, and the unified theory of acceptance and usage of technology (Gebauer et al., 2010; Kim et al., 2010; Liang et al., 2013; Zhou et al., 2010). The rationale behind integrating adoption theory with TTF is that technology adoption not only depends on users' perceptions and attitudes, but also on a match between tasks and technologies (Zhou et al., 2010). The "fit" between task and technology can influence users' perceptions (i.e. perceived ease of use, perceived usefulness) toward mobile technologies (Kim et al., 2015; Kim et al., 2010; Mathieson and Keil, 1998). To be specific, the TAM emphasizes the importance of users' appraisal of the perceived ease of use and perceived usefulness (Davis, 1989). Although the relationship between perceived usefulness and usability is still under debated, the perceived ease of use is confirmed to be strongly related to perceived usability (Lah et al., 2020; Lewis et al., 2015). Additionally, research has indicated that perceived security, which refers to the subjective beliefs concerning the information security in transition, is an extended construct in the TAM (Hartono et al., 2014; Salisbury et al., 2001). Therefore, it provides justification for understanding the fit through discussing perceptions of security and usability by applying the construct derived from the TAM.

2.2 The Social Context and Its Contextual Factors

The widespread adoption of contextual mobile technologies has increased the interest in studying the use context. In general, research in the human-computer interaction (HCI) field has described the use context as "any information that can be used to characterize the situation of an entity", such as "a person, place, or object that relevant to the interaction between a user and an application, including the user and the application themselves" (Dey, 2001, p.5). Similarly, other researchers also defined the use context as factors in relation to personal and environmental conditions that influence the use of mobile technologies (Kim et al., 2015; Lee et al., 2005). In this study, we define the use context as a set of personal and environmental conditions that can affect interactions in terms of using mobile payment services. Based on this definition, the use context can be categorized into two types: the personal context and the environmental context (Lee et al., 2005). To be specific, the personal context refers to the emotional or physical states of an individual (Lee et al., 2005). Regarding the environmental context, it reflects the external conditions of a user, such as the physical and social context (Lee et al., 2005). Various factors from the personal context (i.e. mobility, time saving), physical context (i.e. distraction, connectivity, location), and social context (strong/weak ties of the people in the interaction) that influence task fit have been identified (Gebauer et al., 2010; Kim et al., 2015; Lu and Yang, 2014).

Although various use contexts exist with regard to mobile technologies, the social context has been highlighted as a vital context that influences security behaviors and perceptions of security and usability (Coursaris and Kim, 2011; Dourish, 2004; Dourish and Anderson, 2006). So far, there is insufficient knowledge about the influence of the social context on perceptions of security and usability in mobile transactions. The social context refers to the environmental factors that influence users during an interaction (Cavdar et al., 2020; Lee et al., 2005), and these specific factors depend on the research field. For example, Lu and Yang (2014) used strong/weak ties and interactions to characterize the social context in social network services, and Lee et al. (2005) utilized interaction and privacy to study the social context in mobile Internet. Mobile payment services provide users with opportunities to settle payments with various kinds of payees in interpersonal or impersonal situations. As the technologies are considered to be technically sound (Johnson et al., 2018), the risk perception could lie in the relationships and interactions between payers and payees. Therefore, the social context in mobile payment transactions should emphasize the social relationships between users and payees and the ways in which users reach payees during interactions.

To describe the social context, this study applies trust to represent the social relationships between users and payees in the interactions. Although other factors, such as power dynamics, reputation, frequency of social interactions (Kabanda, 2011; Sutcliffe et al., 2015; Shao, et al., 2019), could influence social relationships, being able to trust others is fundamental in social exchange relationships among nonkin (Sutcliffe et al., 2015). Trust between payers and payees is an interpersonal relationship that can be broken or repaired through some payees' reactions to security incidents (Choi and Nazareth, 2014). Trust and security are highly relevant in mobile payments (Khalilzadeh et al., 2017; Mallat, 2007). Therefore, this study focuses on the influence of trust on the relationships between payers and payees. A certain level of trustworthiness indicates a willingness to rely on payees, as well as a degree of vulnerability, in payment situations (Gefen and Straub, 2004). Therefore, this study defined trust as a dimension in the social context of mobile payment services and as the extent of the user's trust in the payees in mobile payment transactions.

On the other hand, mobile payments involve both offline and online payment scenarios, meaning that payment transactions are settled in both interpersonal and impersonal situations. Therefore, social presence could be a contextual factor of the social context that describes how users reach payees. Social presence refers to "the degree of salience of the other in a mediated communication and the consequent salience of their interpersonal interactions" (Short, Williams, & Christie, 1976, p.65). It has been used to measure the "inherent quality of a communication medium" (Lu et al., 2016, p.226). A high level of social presence is found in direct human contact, such as face-to-face communication and interactions, while a low level of social presence is found in indirect human contact, such as online communication and e-commerce (Gefen and Straub, 2004). In terms of mobile payment services, a high social presence can be found in a face-to-face mobile transaction or direct human-contact mobile transaction, and a low social presence can be found in an online mobile transaction or indirect human-contact mobile transaction. Therefore, this study applied social presence to describe the attributes of interactions with other people in terms of physical closeness during payment interactions.

In summary, this study applied trust and social presence to characterize the social context in mobile payment transactions. To our knowledge, little research has discussed the fit between security design and social contexts or investigated the effects of the social context on behaviors and perceptions of security and usability in mobile transactions. This study attempted to understand how to provide a security design based on social contexts.

2. 3 Existing Security Design Functions in Mobile Payment Transactions

Security design can refer to the appropriate functions and information that help users to access the system and perform the task securely (Yee, 2003). In mobile payment applications, users can manage their account security through receiving feedback information and customizing various security settings, such as authentication settings, payment settings, privacy settings, and account management settings (Li and Yeh, 2010; Shao et al., 2019; Tossell et al., 2012; Zhang et al., 2019; Zhang and Yan, 2020). Therefore, this study focuses on two types of security design: security settings and feedback design.

Security settings refer to the settings (e.g. authentication settings, payment settings, and privacy settings) related to security functions that are provided by the interface. Users require various security settings in mobile payment services. For example, the design of authentication settings has been widely discussed in formation security (Gunson et al., 2011; Still et al., 2017; Zimmermann and Gerber, 2017). Still et al. (2017) developed six principles for designing usable authentication methods. Gunson et al. (2011) examined the effects of single-factor and two-factor authentication methods on the perception of security and usability. The results indicated that two-factor authentication is perceived as being more secure, but it is less usable and convenient. Besides, privacy settings, which help to manage and protect personal information (Lankton et al., 2017), are vital to information security and are regarded as one aspect of security settings in this study (Karat et al., 2005; Lewis et al., 2008). Some studies on contextual preferences for privacy settings were found. For example, research has mentioned that privacy settings should be based on the characteristics of the audience in the social network (Watson et al., 2015); other research has found that users' willingness with regard to information disclosure for online behavioral advertising is affected by various online activities (Wang et al., 2016).

Providing feedback design is one way to help users understand the system's security status (Johnston et al., 2003). Feedback design can refer to "any form of communication from a system toward the user" (Muñoz-Arteaga et al., 2009). Communication is not only important for security design in information systems, but it is also a critical element in interface design for improving security perceptions in e-commerce (Kamoun and Halaweh, 2012). In the mobile payment services provided by Alipay and WeChat Pay, the feedback design conveys to users the payment status using three kinds of information: status information, identity information, and risk information. The status information informs users about system and payment statuses, such as the progress of the payments and the network situation of the application; identity information provides information about the identity of the payees, such as names, images, or account numbers; and risk information warns users of any security risks that appear in the payment transactions, such as those concerning privacy leakages and disreputable payee accounts.

In general, previous research on security design has mainly focused on improving usability problems in security and developing usable interface design features for desktop computer security rather than for mobile technologies (Göktürk and Şişaneci, 2014; Johnston et al., 2003; Nurse et al., 2011). Although some research has suggested that the goals of usability and security are conflicting (Dhillon et al., 2016; Gunson et al., 2011), other researchers have claimed that the gap between usability and security can be bridged by creating design functions based on an understanding of users' mental models (Mohamed et al., 2017). It allows justification for investigating users' perceptions of security and usability in security design. On the other hand, the ubiquitous nature of mobile technologies requires knowledge about the fit between security design and use context, which has not been investigated sufficiently in previous research. It can be deduced that users have various preferences for security settings and feedback design according to the social context. For example, users have a high demand for security settings when they settle payments with an unknown payee, and users prefer having feedback information when the payees are absent in order to keep track of the payment status. The limited research investigating the fit between security design in use context and discussing this fit by understanding the perception of security and usability suggests the necessity of conducting more work in this area.

2.4 The Development of Research Process and Hypotheses

Given the theoretical background on TTF and the TAM and the related work on the social context and security design, we can deduce that security design should be considered in relation to the use context and that the social context is vital to the fit of security design in terms of mobile transactions. Besides, many studies implied the important role of the social context in perceptions of security and usability (Coursaris and Kim, 2011; Dourish et al., 2004; Dourish and Anderson, 2006). So far, few efforts have been made to investigate the fit between security design and the social context, and to discuss the influence of security design and the social context on behaviors and perceptions of security and usability.

Therefore, with the aim of providing design implications for security design according to social contexts, this study attempted to use TTF and the TAM as a theoretical basis to examine the fit between security design and the social context, and to investigate behaviors and perceptions of security and usability in different social contexts. To be specific, this research focuses on the security design of security settings and feedback design and characterizes social contexts using social presence and trust.

However, the technologies and functions examined in previous TTF and TAM research were usually designed by researchers or service providers (Chang, 2010; Kim et al., 2010; Wu and Chen, 2017). Although this could help to evaluate the fit of existing technologies, it limits the possibility of exploring the best "fit" and the most desired functions requested by the users. Unlike behavioral science studies, which use research models to investigate the determinants for describing, explaining, and predicting the "fit", the purpose of our work was to find out the fit between security design and social contexts and develop solutions for the fit problem. This goal would be fulfilled by constructing artefacts, which allowed participants to express their preferences for security design in social contexts through exhibiting behaviors and perceptions. Therefore, it requires a switch of the paradigm from behavioral science to design science in this study (Hevner et al., 2004; van Aken, 2004). In line with a design science research (DSR) approach, which emphasizes creating artefacts to solve the identified problem and develops knowledge that can be used to provide solutions (Choi and Nazareth, 2014; Dincelli and Chengalur-smith, 2020; Geerts, 2011; Van Aken, 2004), we would be able to design prototypes and payment scenarios to investigate the fit between security design and social contexts. In addition, DSR also considers the impact of social aspects on the creation, design, and evaluation of artefacts (De Leoz and Petter, 2018). It further justifies using a DSR process to help develop creations and achieve socially related knowledge.

We proposed five hypotheses to evaluate the effectiveness of the artefacts on identifying the fit problem and address our research question. Specifically, the ubiquitous nature of mobile technologies makes it difficult to assign the matched security settings according to the social contexts in a controlled manner. Therefore, rather than measuring the fit based on the given security settings, we investigated the fit between security settings and social contexts by allowing users to create the "task-technology fit" of security settings in social contexts by themselves. In other words, this study developed customizable interfaces, and participants tailored their security settings based on their social contexts. Then, we were able to understand the fit between security settings and social contexts by observing the variance in terms of behaviors in relation to the security settings. Therefore, we proposed a hypothesis:

H1. Behaviors in relation to security settings vary according to social contexts.

With regard to the fit between feedback design and the social context, we manipulated feedback design with two prototypes and examined the effects of feedback design on behaviors in relation to security settings and perceptions of security and usability. We suspected that feedback design can influence users' preferences in terms of security settings according to social contexts, as previous research stated that feedback information can encourage users to undertake security measures (Furnell et al., 2018; van Bavel et al., 2019). Thus, we hypothesized:

H2. Feedback design can affect behaviors in relation to security settings in different social contexts.

Since the feedback design was manipulated by the researchers in this study, we further evaluated the fit between feedback design and social contexts by discussing the perception of security and usability and continuous use intention. The literature review indicated that the match between security design and use contexts can positively affect perceptions, attitudes, and continuous use intention with regard to mobile payment services (Kim et al., 2015, 2010; Mathieson and Keil, 1998). Therefore, we applied five constructs from the TAM (Davis, 1989) and the extended TAM (Hartono et al., 2014; Salisbury et al., 2001) concerning information security to explain the fit by discussing variances in the perceptions of security and usability and post-adoption use intention. These constructs are perceived security (PS), perceived usefulness (PU), perceived ease of use (PEOU), satisfaction (SA), and continuous use intention (CU).

PS is a vital extended determinant in the TAM for predicting technology adoption (Hartono et al., 2014; Salisbury et al., 2001). It can reflect users' psychological need for security in mobile transactions, which can be affected by both security design and the social context (Dourish et al., 2004; Dourish and Anderson, 2006; Zhang et al., 2019; Zhang and Luximon, 2020). In this study, we applied PS to measure participants' attitudes toward the transaction security of the prototypes in different social contexts and defined it as the extent to which an individual believes that the interface enables secure transactions in mobile payment services (Zhang and Luximon, 2020). Here, we proposed:

H3. PS is affected by feedback design and social contexts.

Previously, usability was measured in terms of objective performance using effectiveness and efficiency, and evaluated with regard to subjective attitudes using satisfaction (Kortum and Oswald, 2018). In this research, we focused on perceived usability and used PEOU, PU, and SA to evaluate users' attitudes toward the usability of security design in different social contexts. PU and PEOU are not only fundamental predictors in the TAM, but can also be influenced by TTF (Mathieson and Keil, 1998; Wu and Chen, 2017). PEOU is also confirmed to have a strong relationship with subjective attitudes toward usability (Lah et al., 2020; Lewis et al., 2015). In this study, PU is defined as the extent to which users believe that the security design in mobile payments can help them to complete the payment effectively (Davis, 1989); in this research, PEOU refers to the extent to which a person perceives that the interface with the security design is easy to use (Davis, 1989). Besides, SA is not only a critical dimension in evaluating usability, but also a vital determinant of CU (Gao et al., 2015; Lu et al., 2017; Mohamed et al., 2017). SA reflects the extent to which the interface design can meet users' expectations (Liao et al., 2007). Thus, this study suggested:

H4. PEOU, PU, and SA are affected by feedback design and social contexts.

Lastly, in this research, CU reflects the extent to which users are willing to continuously use the interface (Gao et al., 2015). It is one of the vital behaviors in the post-adoption use of the technologies (Wu and Chen, 2017). This construct was used to explain the continuous use intention of security design in different social contexts. We proposed:

H5. CU is affected by feedback design and social contexts.

3 Method

This study employed the design science research (DSR) approach to guide the design of research methodology. The DSR approach indicates how to build and evaluate the artefacts for problem solutions. It involves a series of actions of problem identification, research rigor, design of the artefacts, demonstration of the use, evaluation of the design, and communication (Choi and Nazareth, 2014; Geerts, 2011; Peffers et al., 2007; Hevner et al., 2004). As mentioned previously, this work aimed to understand the fit problem between security design and the social context and provide solutions and design guidelines. Instead of measuring the fit based on the given security settings, we investigated the fit by allowing users to create the "task-technology fit" of security settings in social contexts by themselves. Therefore, the design goal of the artefacts in this study was to design prototypes and scenarios which could offer opportunities for participants to exhibited their preferences and perceptions for security design according to social contexts. There were two parts in the creation of the artefacts: first, we created a customizable interface without feedback information (CI) and a customizable interface with feedback intervention (CIFI). Various security settings and feedback design were embedded in these two interfaces (see Section 3.3.1); second, we transferred the targeted components (social presence and trust) of social contexts into four payment scenarios (De Leoz and Petter, 2018) (see Section 3.3.2).

We evaluated the effectiveness of the artefacts in meeting the design goal and identifying the fit problems based on the data collection in an experiment (Dincelli et al., 2020; Venable, Pries-Heje, and Baskerville, 2014). To be specific, participants could exhibit their preferred security settings by tailoring security settings and reported perceptions with the CI and the CIFI in four payment scenarios during the experiment. By measuring behaviors in relation to security settings, perceptions of security and usability, and continuous use intention (see Section 3.4), we were able to evaluate the effectiveness of artefacts in understanding the fit between security settings, feedback design, and social contexts and helping generate design guidelines and implications based on the findings.

3.1 Recruitment

This study recruited university students through posters. Participants accessed the link on the poster and reported their age, gender, usage experience, and expertise to register for participation. Since age, usage experience, and expertise could affect behaviors and perceptions (Chong et al., 2012; Liébana-Cabanillas et al., 2014; van Bavel et al., 2019; Zhang et al., 2019), we had three criteria for recruitment to reduce the potential bias: 1) we targeted users who aged at least 18; 2) to exclude novice users and control for the effect of cultural differences, we required that participants should have experienced using mobile payment applications in mainland China for longer than one year; and 3) we insisted that participants should not be experts in the information security and interface design fields. We selected the qualified users based on their reported information and chosen participants were offered a small reward as an incentive.

3.2 Experimental Design

To investigate the fit between security design and social contexts and provide guidelines for security design in mobile interactions, we employed a factorial design experiment to examine participants' behaviors in relation to security settings, perceptions of security and usability (PS, PEOU, PU, and SA), and continuous use intention (CU) when applying two different prototypes in four social contexts. This study developed a customizable interface without feedback information (CI) and a customizable interface with feedback intervention (CIFI). Different kinds of security settings, including authentication settings, payment settings, privacy settings, and account management settings, were embedded in both the CI and CIFI. Participants exhibited behaviors in relation to security settings by tailoring the settings in the interfaces while using the two prototypes in different payment scenarios. In the CIFI, participants were not only allowed to customize the security settings, but also received feedback information about their security statuses. Four payment scenarios were developed using two contextual factors of the social context: social presence and trust. Therefore, the experiment used a 2 (feedback design) × 2 (social presence) × 2 (trust) factorial design. The independent variables were feedback design (CI and CIFI), social presence (low and high levels), and trust (low and high levels). Also, the independent factors were within-subject variables. Behaviors in relation to security settings, perceived security (PS), perceived ease of use (PEOU), perceived usefulness (PU), satisfaction (SAT), and continuous use intention (CU) were measured in each treatment condition. Participants' age, usage experience, and expertise were controlled for in the experiment. Table 1 shows the treatment conditions in this study.

Table 1. Treatment conditions

		Social context	
		Social presence	Trust
Feedback design	Non-feedback information	Low level	Low level
	Feedback information	High level	Low level

3.3 Artefacts Creation

3.3.1 Prototypes: Two customizable interfaces with different feedback design

This study developed two prototypes of mobile payment applications which were installed in two mobile devices: a Samsung phone (Galaxy C7 Pro) and a Huawei phone (Nova 3). Participants performed payment tasks using either of mobile devices. The first prototype (CI) was developed with customizable settings only (see Figure 1). Participants could display behaviors in relation to security settings with this prototype. The other prototype (CIFI) was designed with both customizable settings (see Figure 1) and the feedback information (see Figure 4). In CIFI, participants were not only able to exhibit behaviors in relation to security settings, but also be informed payment status with feedback information. CI includes five main pages (see Figure 2): (1) a login page, which allows participants to input the participation number; (2) a settings page for tailoring the security settings of “payment authentication,” “wallet password,” “additional authentication for large payments,” and “daily payment limit”; (3) a home page, which displays the account balance and functions of the application; (4) a scanning page for simulating the payment process; and (5) a payment content page for inputting the payment information and modifying three payment settings: “anonymous transfer,” “payment methods,” and “transfer date”. If participants modified “payment authentication,” “wallet password,” or “additional authentication for large payments” in the settings page, the extra authentication page appeared after the settings page or after the payment content page.

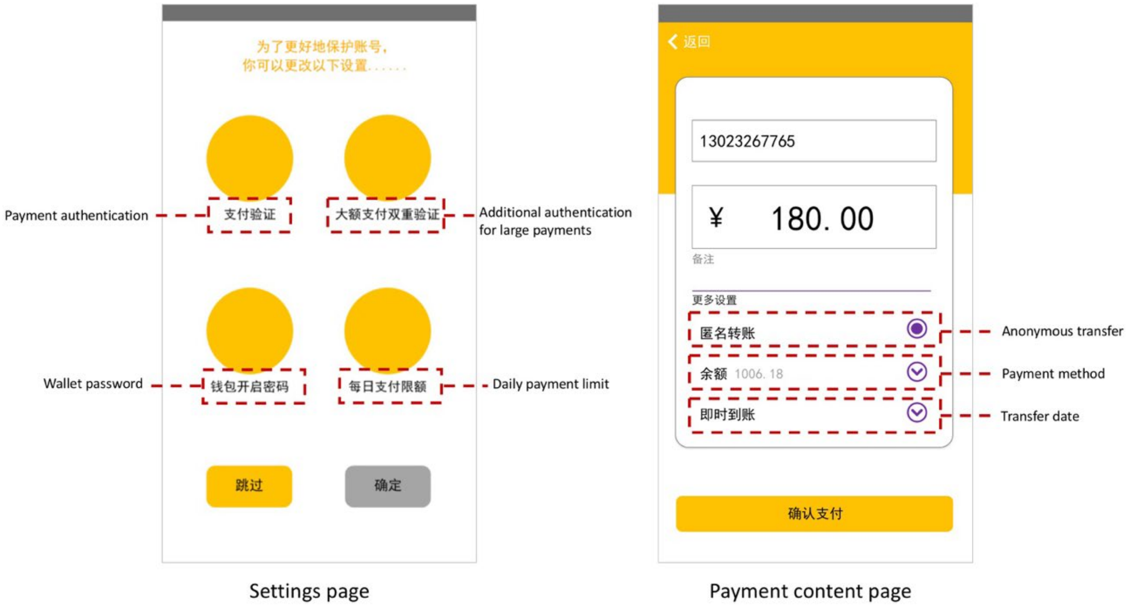


Figure 1. Customizable security settings in both CI and CIFI

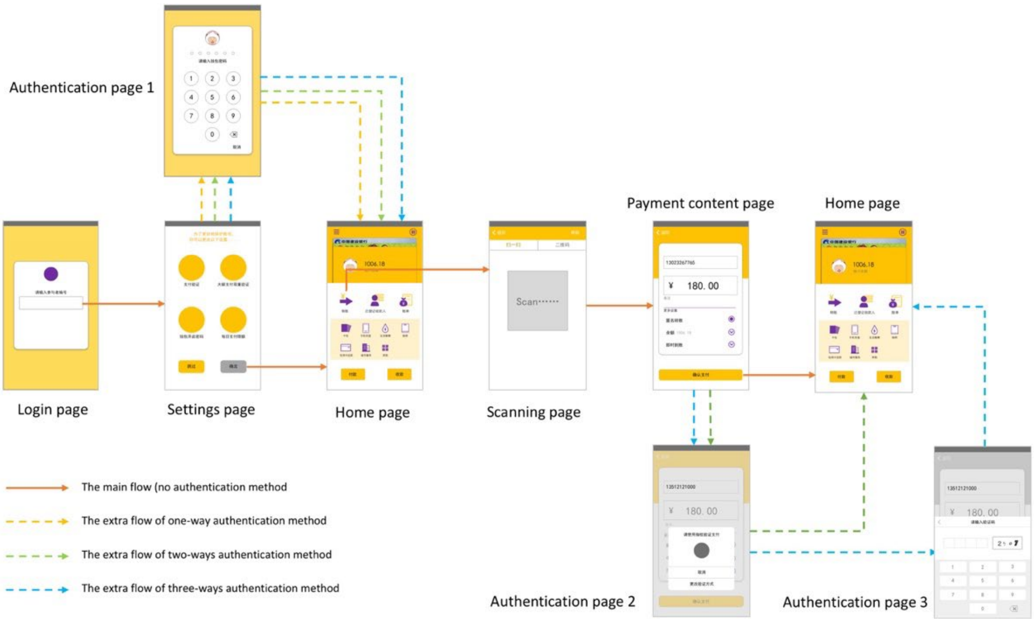

Authentication page 1
Login page
Settings page
Home page
Scanning page
Scan……
Payment content page
Home page
Authentication page 2
Authentication page 3
The main flow (no authentication method
The extra flow of one-way authentication method
The extra flow of two-ways authentication method
The extra flow of three-ways authentication method

Figure 2. The flow of CI

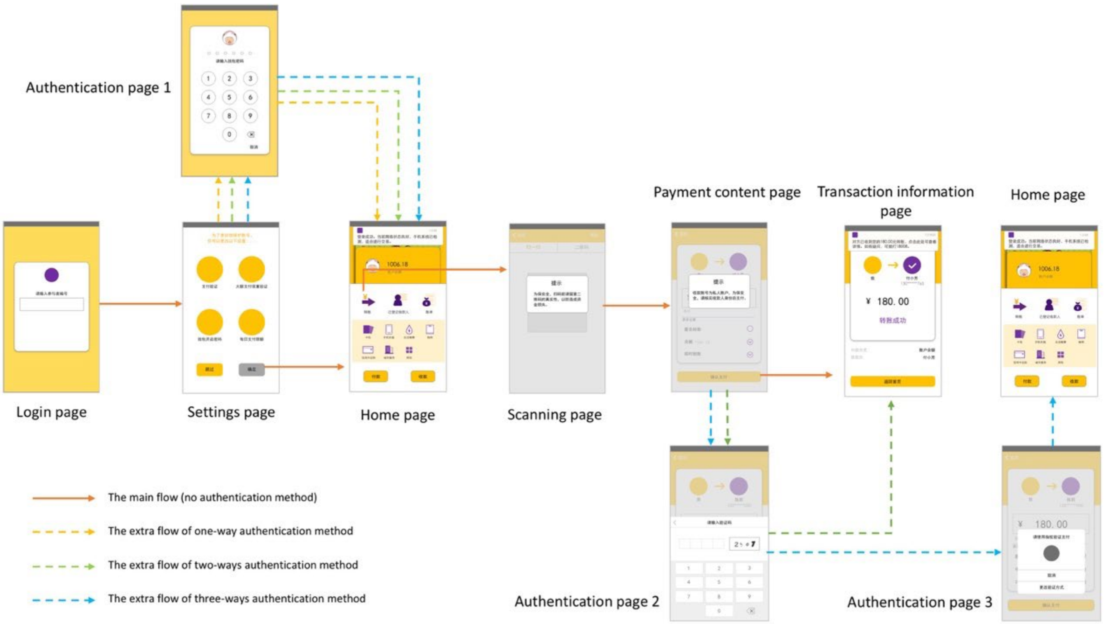
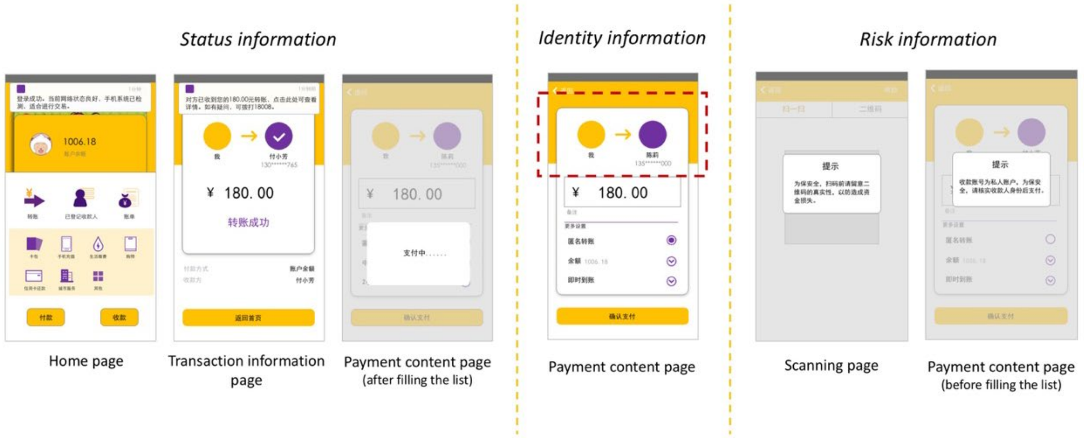

Authentication page 1
Payment content page
Transaction information page
Home page
Login page
Settings page
Home page
Scanning page
¥ 180. 00
The main flow (no authentication method)
The extra flow of one-way authentication method
The extra flow of two-ways authentication method
The extra flow of three-ways authentication method
Authentication page 2
Authentication page 3

Figure 3. The flow of CIFI

CIFI comprises six main pages. In addition to the five pages and functions that embedded in CI, CIFI also has a transaction information page that appears after the payment content page (see Figure 3). The transaction information page aims to show users the payment status. Three types of feedback information ("status information," "identity information," and "risk information") are displayed during the transaction using CIFI (see Figure 4). The "status information" is displayed on the home page, payment content page, and transaction information page to inform participants the payment status and network status; the "identity information", which appears on the payment content page and transaction information page, aims to show the payer's and payee's identity; the "risk information", which appears on the scanning page and payment content page, is used to suggest the potential risks that involved in the payment process.

Both CI and CIFI have a "pause button" on the home page and a "return button" on the left side of each page. Participants could click the "pause button" to stop the task and "return button" to back to the previous page.


登录成功。当前网络状态良好，手机系统已检测，适合进行交易。

对方已收到您的180.00元转账，点击此处可查看详情。如有疑问，可拨打18008。

提示

为保安全，扫码前请留意二维码的真实性，以防造成资金损失。

提示

收款账号为私人账户，为保安全，请核实收款人身份后支付。

Figure 4. Three types of feedback information in CIFI

3.3.2 Tasks: Four payment scenarios

Four payment tasks were created to manipulate the influences of social presence and trust (see Table 2). Both social presence and trust have two levels: a high and a low level. A high level of social presence refers to direct human contact in the payment interaction (e.g. transactions in stores with merchants or when paying a person face-to-face). In the high social presence context, the payer transfers money to a payee/merchant in person through a mobile payment application. A context with a low level of social presence represents indirect human contact in the payment interaction (e.g. mobile purchases in applications, performing transactions with people who are not there in person, or paying via vending machines). In this situation, the payer settles the payment in a situation where the payee/merchant is absent during the mobile payment. The two levels of trust indicate whether the payees are trusted or not. In a high level of trust context, the payer believes that the payee/merchant is trustworthy (e.g. friends, families, or well-known merchants). In comparison, the payer perceives the payee/merchant is untrustworthy in a low level of trust context (e.g. unknown and disreputable payees).

This experiment designed the payment scenarios, name of the payee, payee's payment account, and payment amount in each payment task. The four payment scenarios were simulated using two levels of social presence and two levels of trust. Scenario 1 (S1) is a payment context with a high level of social presence and a high level of trust, where the transaction is settled with a friend next to the payer; Scenario 2 (S2) is a payment context with a low social presence level and a high trust level, where the payer transfers money to a remote friend using the mobile payment application; Scenario 3 (S3) is a payment context with a high level of social presence and a low level of trust, where the payer transfers taxi charges to a driver (a stranger) face to face; Scenario 4 (S4) is a payment context with a low level of social presence and a low level of trust, where the charge is paid to an unknown company's account using a remote transfer through the mobile payment application. To reduce the probable influence of the payment amount, this experiment designed a similar charge in each payment scenarios, ranging from 136 to 180 yuan. To control the effect of payment interaction methods, we required participants to scan a specific QR code for settling the payment in each task. In S1 and S3, the payees were acted by a researcher. The QR code was sent to the participant in S2, while the QR code was pasted in a simulated machine in S4. Each participant was also provided with an information sheet (see Table 3), which displayed the password, account balance, debit card balance, and credit limit. We also applied a manipulation test to observe if two levels of trust are successfully controlled in four payment scenarios.

Table 2. The design of payment scenarios

Scenarios	**Description**
S1: High level of social presence High level of trust	• Description: Imagine that you just had have a lunch with your friend, Xiaofang, and she paid for the bill. Now you are going to scan her QR code and pay back money to her. Now, she is next to you. • Name of payee: Fu Xiaofang • Payment account: 13023267765 • Payment amount: 156 yuan
S2: Low level of social presence High level of trust	• Description: You would like to pay back money to a friend (called Wen), who had helped you to buy a museum ticket. Because Wen is now far away from you, you sent a message to Wen and asked for her QR code. Now, you are going to scan the QR to transfer money to her. • Name of payee: Zhang Wen • Payment account: 13634323289 • Payment amount: 180 yuan

S3: High level of social presence Low level of trust	• Description: You are in an unfamiliar city for a business trip, and you take a taxi to the hotel. After arrival, the driver allows you to scan his QR code to pay the fee. • Name of payee: Huang Ruibin • Payment account: 18987679007 • Payment amount: 136 yuan
S4: Low level of social presence Low level of trust	• Description: Your phone battery is going to die and you see a charging station. Although you had never heard of the name of company (Power of Panzhihua Xiaoyou), you decide to scan the QR code pasted in the charging station and recharge your phone. • Name of payee: Power of Panzhihua Xiaoyou • Payment account: Power of Panzhihua Xiaoyou • Payment amount: 150 yuan

Table 3. The information sheet

Information Sheet	
Participant number	No. _____
Account balance	1,000–1,500 yuan
Debit card balance	1,500 yuan
Credit card limit	1,500 yuan

Wallet password	321456
Payment password	789123

3.4 Measurements

This experimental study evaluated both objective and subjective measurements. We measured behaviors in relation to security settings by recording participants' performance in each task, and evaluated perceptions of security and usability and continuous use intention using questionnaires.

3.4.1 Manipulation of trust level

A pre-test questionnaire was used to examine if we successfully manipulated the trust level by assigning different types of payees in the payment scenarios. A nine-point Likert scale question, "To what extent do you trust the payee?" was designed. Participants were required to report their trustworthiness to the payee in each payment scenarios by selecting from 1 (not at all trustworthy) to 9 (extremely trustworthy)

3.4.2 Behaviors in relation to security settings

We measured participants' behaviors in relation to security settings by observing the number of security settings that they used in each task. Participants were allowed to display four types of behaviors in relation to security settings in both CI and CIFI. These four types of behaviors in relation to security settings are: behaviors in relation to password protection settings (three settings), enhanced control settings (two settings), privacy protection settings (one setting), and account management settings (one setting).

- Behaviors in relation to password protection settings: Behaviors relating to authentication schemes were defined as behaviors in relation to password protection settings (Das and Khan, 2016). Participants could customize the security settings of "payment authentication," "wallet password," or "additional authentication for large payments" on the settings page. With these modification of settings, they could apply no authentication method, a one-factor authentication scheme, a two-factor authentication scheme, or a three-factor authentication scheme during the transaction.
- Behaviors in relation to enhanced control settings: it refer to the security practices relating to acquire a higher level of the payment process control. Participants could display behaviors in relation to enhanced control settings by

modifying the “daily payment limit” and “transfer date” on the settings page and payment content page.

- Behaviors in relation to privacy protection settings: behaviors associating with protecting the personal information in the payment transaction were categorized into behaviors in relation to privacy protection settings . Both CI and CIFI allow participants to determine if they would like to disclose their personal information (such as name and phone number) to the payee by using the “anonymous transfer” function on the payment content page.
- Behaviors in relation to account management settings: it refers to the practices of managing the account by altering the payment methods, including using a debit card, credit card, or balance to pay in the transaction. Participants could exhibit behaviors in relation to account management settings on the payment content page.

3.4.3 Perception and attitudes

We applied a nine-point Likert scale range from 1 (extremely disagree) to 9 (extremely agree) to evaluate perceptions and continuous use intention toward each task. PS was measured with four items adapted from Zhang et al. (2020) and Khalilzadeh et al. (2017); PEOU and PU were respectively measured with three items adapted from Yoon and Steege (2013), Liao et al. (2007), and Davis (1989); three items regarding SA were adapted from Chang and Chen (2008), Liao et al. (2007); CU were examined with three items adapted from Zhou (2011), Kim et al., (2010) (see Appendix. Table A).

3.5 Procedure

Participants were given an introduction about the experiment, and then they signed a consent form. As the experiment was the simulation task, participants needed to follow two preconditions during the experiment: (1) the payment context and transaction were true in each simulation task, and (2) CI and CIFI were reliable mobile payment applications.

The experiment comprised three parts. Firstly, participants should take the manipulation test which aimed to ensure the successful manipulation of two trust levels in four payment scenarios. The researcher read the payment scenario, and the participants were then required to indicate their trustworthiness toward the payee in that payment scenario. Four payment scenarios were read in a random order. After finishing the manipulation test, the researcher introduced the functions and the payment process of CI and CIFI to participants. Participants then went through the functions and the payment process in both CI and CIFI, and therefore they were familiar with the two prototypes in the payment tasks. An information sheet (see Table 3) which provided the details of the account balance, debit card balance, and credit limit, wallet password, payment passwords was given to each participant.

Since the experiment comprised 2 (CI and CIFI) × 2 (social presence with low level and high level) × 2 (trust with low level and high level) settings, each participant was required to complete a total of eight payment transactions. First, the researcher randomly assigned the participant with a prototype. Then, the researcher selected one of the four payment scenarios and read the description of the scenario to participants. The participants conducted the payment task based on the scenario and reported their perceptions and continuous use intention toward the task. Four payment scenarios were selected and read in a random order.

During each payment task, the participants entered participation number to login, tailored the security settings if their needed, selected the "transfer" button, scanned the QR code, input the payment information, modified the payment settings, and settled the payment. Then, the participants were back to the home page and clicked the "pause" button (see Figure 5). Each participant had a 30-second break between each task.

When completed eight tasks, the participants reported their age, gender, and usage experience of mobile payment using a questionnaire.

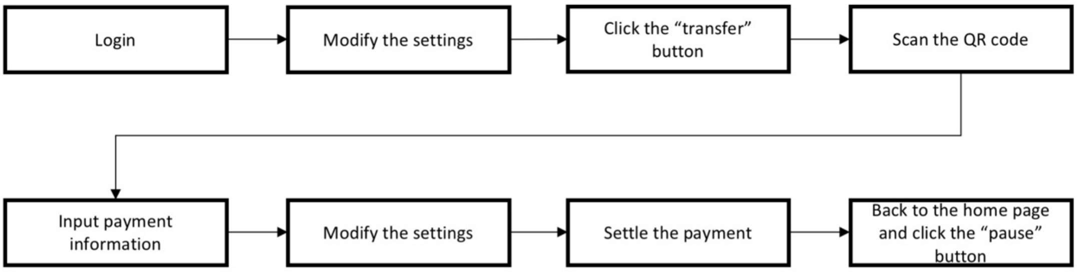

Login
Modify the settings
Click the "transfer" button
Scan the QR code
Input payment information
Modify the settings
Settle the payment
Back to the home page and click the "pause" button

Figure 5. The payment steps

3.6 Manipulation Test: Validity Manipulation Checks

A repeated measures t-test was used to examine if the manipulation of trust level was successful. There was a significant mean difference between the payment scenarios designed with two trust levels (t(112) = 20.195, p < 0.001). The trust level in S1 and S2 (mean=7.982) was significantly higher than that in S3 and S4 (mean=4.196). The result suggested that the experiment had successfully manipulated the trust level.

4. Data Analysis

The results of the values of skewness and kurtosis indicated that the distributions of behaviors in relation to security settings, PS, PEOU, PU, SA, and CU were normal (Field, 2009; George, 2011; Gravetter and Wallnau, 2014; Trochim and Donnelly, 2006). Therefore, we performed a repeated measures ANOVA to evaluate the effects of feedback design, social presence, and trust. The interaction effects between the variables were further examined using the repeated measures t-test as the post-hoc test. Additionally, a descriptive analysis was performed to examine the distributions of the specific behaviors in relation to security settings in different payment scenarios.

5. Results

5.1 Participants

There were 60 participants, comprised of 24 males and 36 females participating in the experiment. The age of participants was between 18 and 30 years. Most of the participants (82%) used mobile payments daily; others of them used mobile payments weekly (18%); almost all of participants (98.3%) had used mobile payments for more than three years. The results of usage experience indicated that all participants had been familiar with mobile payment services. Therefore, the influence of usage experience was reduced. In addition, none of them claimed to be experts in interface design and information security.

5.2 Behaviors in Relation to Security Settings

Table 4. The mean of number of behaviors in relation to security settings in eight experimental conditions

Feedback design	Social presence	Trust	Behaviors in relation to security settings in overall	
			Mean	SD
CI	Low	Low	3.17	1.55
		High	2.10	1.41
	High	Low	2.82	1.37
		High	1.77	1.24
CIFI	Low	Low	3.03	1.54

	High	2.20	1.31
High	Low	2.73	1.33
	High	2.03	1.26

The repeated measures ANOVA revealed that there were significant main effects of social presence (F(1,59) = 13.703, $p < 0.001$) and trust (F(1,59) = 44.760, $p < 0.001$) on security behaviors. The result indicated that more security behaviors were undertaken in the payment contexts with a low level of social presence (mean=2.63) than those with a high level of social presence (mean=2.34). Also, participants displayed more security behaviors in the low trust contexts (mean=2.94) than the high trust contexts (mean=2.03). However, there was no significant difference between CI and CIFI on security behaviors, demonstrating that feedback information could not encourage participants to exhibit more security behaviors. Table 4 shows the mean values of behaviors in relation to security settings in different experimental conditions. Thus, the results supported H1 and rejected H2.

Table 5. Descriptive analysis of specific behaviors in relation to security settings according to two levels of social presence and trust

Social presence	Trust	Password Protection		Account Management		Enhanced Control		Privacy Protection		Overall Behaviors	
		Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD
Low	Low	1.93	0.95	0.05	0.22	0.49	0.69	0.63	0.49	3.10	1.54
	High	1.72	0.94	0.03	0.16	0.24	0.49	0.17	0.37	2.15	1.36
High	Low	1.81	0.93	0.01	0.09	0.31	0.48	0.65	0.48	2.78	1.34
	High	1.60	0.97	0.02	0.13	0.17	0.40	0.12	0.32	1.90	1.25

Overall	1.76	0.96	0.03	0.16	0.30	0.54	0.39	0.49	2.48	1.45

A descriptive analysis was further examined the distribution of mean number of specific behaviors in relation to security settings in different payment scenarios. The mean number of specific behaviors in relation to security settings is illustrated in Table 5. There were three settings for behaviors in relation to password protection settings, and these behaviors were displayed mostly on average (mean=1.76). We designed two settings for exhibiting behaviors in relation to enhanced control settings, and participants exhibited a mean number of 0.3 on average. There was only one setting for behaviors in relation to account management settings and behaviors in relation to privacy protection settings, respectively. Participants undertook few behaviors in relation to account management settings (mean=0.03), while they displayed behaviors in relation to privacy protection settings (mean=0.39) more often than behaviors in relation to account management settings. To be specific, it could be observed that behaviors in relation to enhanced control settings (low vs. high: 0.40 vs. 0.21) and behaviors in relation to privacy protection settings (low vs. high: 0.64 vs. 0.15) were exhibited frequently in the low trust context than in the high trust context.

To understand participants' preference for authentication schemes, we further analyzed behaviors in relation password protection settings by comparing of the number of different authentication schemes used in different payment contexts with two prototypes (CI and CIFI). Figure 6 shows the results. Participants could decide to use different authentication schemes by tailoring the "payment authentication," "wallet password," or "additional authentication for large payments" functions in the settings page. We defined four levels for different authentication schemes: very low level (no authentication used), low level (one-factor authentication scheme), medium level (two-factor authentication scheme), and high level (three-factor authentication scheme). In general, the two-factor authentication scheme was mostly used. There were between 22 and 26 payment tasks in each scenario using a two-factor authentication scheme. The three-factor authentication scheme was mostly used in S4, with a number of tasks between 18 and 20. In comparison with other payment scenarios, more tasks with a no authentication scheme and a one-factor authentication scheme were conducted in S1 and S2. To be specific, the number of the tasks that conducting without authentication was the least in four scenarios. There were 10 tasks paid without using authentication in S1, and only between 5 and 8 tasks paid using no authentication scheme in S2, S3, and S4.

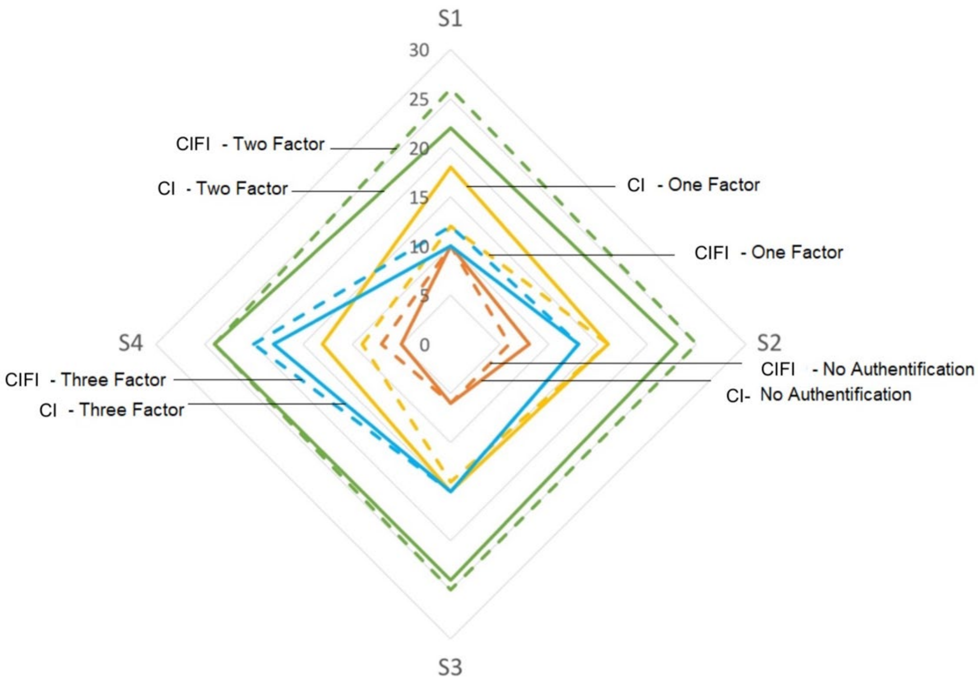


Figure 6. Comparison of behaviors in relation to password protection settings in four payment contexts with CI and CIFI

5.3 Perceptions and Attitudes

A nine-point Likert scale was used to measure the participants' PS, PEUO, PU, SA, and CU intention. The means for the perceptions and continuous use intention towards CI and CIFI in four payment scenarios are showed in Table 6. In general, the mean values of perceptions and attitudes indicated that participants had at least a medium level (5.52 out of 9) of PS, and considerably higher levels of PEOU, PU, and SA (at least 8.09 out of 9, 7.74 out of 9, and 6.78 out of 9, respectively). This demonstrated that participants obtained an acceptable level of PS and relatively high levels of PEOU, PU, and SA when using the self-tailored security settings in different social contexts. The mean values of CU also suggested that participants showed a willingness to continuously adopt their preferred security settings in different social contexts. Mostly, participants reported higher scores of PS, PEOU, PU, SA, and CU when they were able to receive feedback information with the CIFI in the four social contexts. The following analysis will further investigate the variances in PS, PEOU, PU, SA, and CU with regard to the two prototypes in the four social contexts.

Table 6. Means of participants' perceptions and continuous use intention in eight experimental conditions

Social Presence	Trust	Feedback Design	Perceived security (PS)		Perceived ease of use (PEOU)		Perceived usefulness (PU)		Satisfaction (SA)		Continuous use (CU)	
			Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD
Low	Low	CI	5.52	2.27	8.11	1.13	7.59	1.25	6.78	1.92	6.19	2.28
		CIFI	6.36	2.11	8.13	1.41	8.04	1.27	7.54	1.61	7.17	1.87
	High	CI	6.98	1.78	8.10	1.01	7.74	1.19	6.97	1.69	6.74	1.80
		CIFI	7.81	1.17	8.34	0.97	8.03	1.12	7.69	1.39	7.54	1.56
High	Low	CI	6.40	2.06	8.13	1.01	7.84	0.99	7.02	1.58	6.67	1.99
		CIFI	7.00	1.85	8.09	1.29	7.88	1.35	7.57	1.48	7.45	1.65
	High	CI	7.67	1.48	8.20	1.02	7.95	1.00	7.32	1.36	7.23	1.48
		CIFI	8.16	1.05	8.33	0.92	7.98	1.41	7.68	1.43	7.46	1.58

The Cronbach's alphas of all constructs exceed 0.7, suggesting good reliability. A repeated measures ANOVA revealed that there were main effects of feedback design (F(1,59) = 26.277, $p < 0.001$), social presence (F(1,59) = 34.774, $p < 0.001$), and trust on PS (F(1,59) = 49.617, $p < 0.001$). Participants perceived a higher level of security with CIFI, and they also felt more secure in high social presence context or high trust context. Therefore, H3 was supported.

A significant main effect of trust on PEOU (F(1,59)=4.565, p=0.037) and a significant interaction effect between feedback design and trust on PEOU (F(1,59) = 4.185, p = 0.045) were found (see Figure 7). The mean difference of PEOU between CI and CIFI in two levels of the trust context was examined by the post-hoc test. There was no significant difference of PEOU between CI (mean=8.117) and CIFI (mean=8.110) in the low trust context (t(119) = 0.052, p = 0.958). However, there was a significant difference of PEOU between CI and CIFI in the high trust context (t(119) = -2.398, p = 0.018). The findings suggest that participants believed that CIFI (mean=8.339) was easier to use than CI (mean=8.150) in the high trust context.

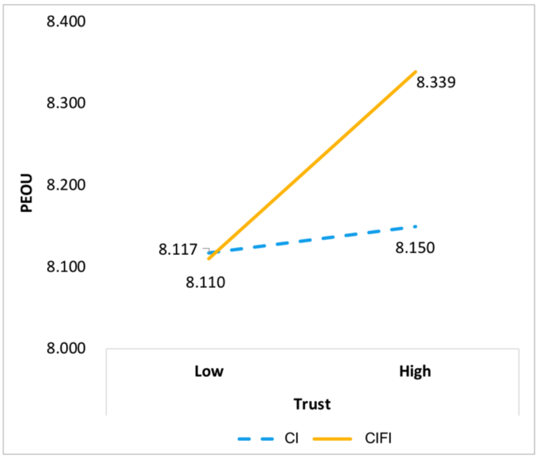


Figure 7. The interaction effect between feedback design and trust on PEOU

However, there was no significant main effect of feedback design, social presence, and trust on PU, while a significant interaction effect between feedback design and social presence on PU (F(1,59)=6.281, p=0.015) was found (see Figure 8). The post-hoc test revealed there was a significant difference of PU between CI and CIFI in the low social presence level (t(119) = -3.935, $p < 0.001$), while there was no significant difference of PU between CI (mean = 7.898) and CIFI (mean = 7.931) in the high social presence level. CIFI (mean = 8.036) was perceived more useful than CI (mean = 7.667) in the low trust context. It was notable that the mean of PU of CIFI had a slight decrease from 8.036 to 7.931 when the level of social presence increased. By contrast, the mean of PU of CI had an increase from 7.667 to 7.898 when the social presence had grown from low level to high level.

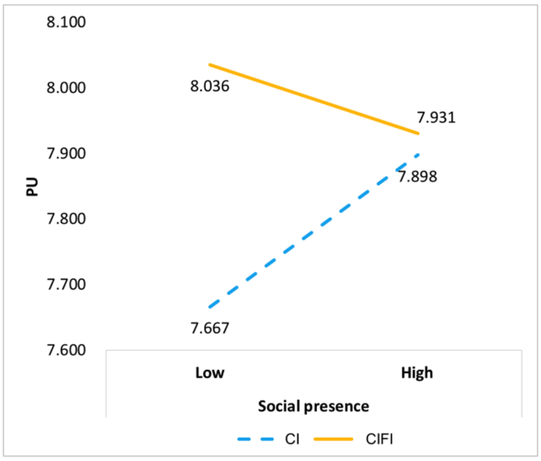


Figure 8. The interaction effect between feedback design and social presence on PU

There was a significant simple main effect of feedback design (F(1,59) = 18.648, *p* <0.001) and social presence (F(1, 59) = 4.480, *p* = 0.039) on SA. CIFI was more satisfactory than CI. Also, the participants were more satisfied to pay in the high social presence context than the low social presence context. A marginally significant interaction was found between feedback design and social presence on SA (F(1,57) = 3.958, *p* = 0.051). Participants became more satisfied with CI (low vs. high: 6.875 vs. 7.170) when the social presence level increased, while the score for SA in CIFI just changed a little between the low level and the high level of social presence context (low vs. high: 7.619 vs. 7.635; see Figure 9). In general, the participants were more satisfied with CIFI in the two levels of social presence contexts, while CI could be also acceptable to use in the high social presence context. Overall, H4 was supported by the results.

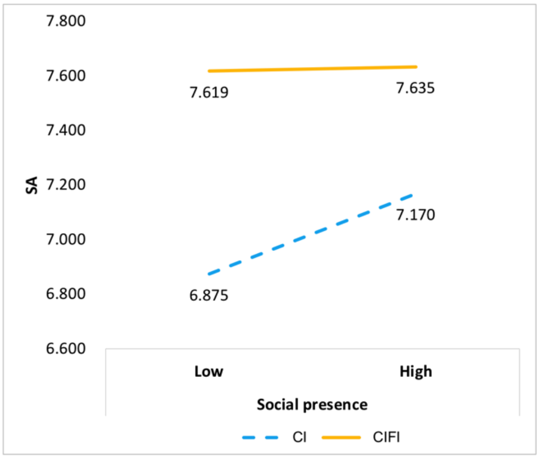


Figure 9. The interaction effect between feedback design and social presence on SA

We observed significant simple main effects of feedback design (F(1,59) = 19.016, *p* < 0.001), social presence (F(1, 59) = 10.014, *p* < 0.001), and trust (F(1, 59) = 4.906, *p* = 0.031) on CU, supporting H5. CIFI could enhance users' continuous use intention. Social presence and trust could positively affect CU. Additionally, there was a significant interaction effect between feedback design and social presence (F(1,59) = 8.476, *p* = 0.005) on CU (see Figure 10). For increasing continuous use intention, social presence has a stronger positive impact on CI than CIFI. The mean score of continuous intention of CI increased from 6.470 to 6.953 when the social presence level was rising to higher. However, there was only a small increase of continuous intention (from 7.358 to 7.453) of CIFI when the social presence was moving higher.

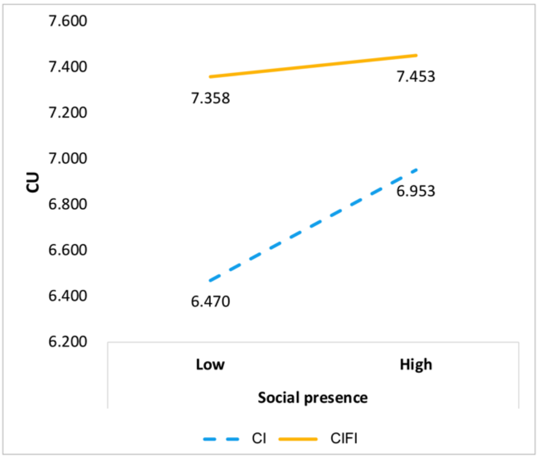


Figure 10. The interaction effect between feedback design and social presence on CU

6. Discussion

6.1 The Effect of Feedback Design on Behaviors in Relation to Security Settings and Perceptions

This study developed CIFI to observe the influence of the feedback design on users' behaviors and perceptions. There was no significant difference between CI and CIFI on behaviors in relation to security settings, suggesting that the feedback information had no impact on participants' preferences for security settings. Participants displayed similar security strategies in both CI and CIFI. Scholars had suggested that the feedback information could inform users to undertake more security behaviors (Furnell et al., 2018; van Bavel et al., 2019). This result suggested a conflicting view on the effect of the feedback information on behaviors in relation to security settings. There are two possible reasons for this result. One is that participants did not read the risk information and go directly to the next step, as they had developed an interface habits for a faster processing of their primary task when using mobile payment applications (Garaialde et al., 2020). Therefore, the feedback information did not take effect on increasing behaviors in relation to security settings. Another possible reason is that although the risk information could improve users' motivation to protection the system, the status information and the identity information could inform users the payment status which could increase perceived security (Zhang et al., 2019). As a result, participants did not exhibit significant different behavior patterns between two prototypes. Although there was no statistical difference of behaviors in relation to security settings in overall between CI and CIFI, we noted that participants tended to apply different authentication schemes between CI and CIFI in the four payment contexts. The descriptive analysis indicated that when using CIFI, participants adopt more two- and three-factor authentication schemes and fewer one-factor authentication scheme for the tasks than using CI. Further studies are needed to investigate the effects of the feedback information on specific types of behaviors in relation to security settings.

The results confirmed the effects of feedback design on participants' perception. Participants had a higher level of PS with CIFI, which provided the feedback information. As we had discussed previously that feedback information could not motivate participants to exhibit more behaviors in relation to security settings, it can enhance participants' feelings of security in mobile payment transactions. The positive effect of the feedback information on perceived security were also demonstrated by the previous empirical research (Zhang et al., 2019) (Kamoun and Halaweh, 2012). This study further validated the influence of the feedback information with an experimental method.

We could expect that participants might perceived a greater PEOU and PU when using CI, because adding a feedback information might interrupt the operations and decrease the usability of the system (Dhillon et al., 2016). However, the results of this study showed that there was no simple main effect of feedback design on PEOU and PU. The feedback design could either decrease or increase usability of the system in the specific context, which would be discussed in the section 7.3. As the mean values of PEOU (mean=8.18) and PU (mean=7.88) were high, it was indicated that participants perceived both CI and CIFI are easy to use and useful. Also, the mean value of SA and CU of CIFI were significantly higher than CI, suggesting that participants were more satisfied with CIFI and more willing to adopt CIFI in all payment contexts. Compared with CI, CIFI provides feedback information. Therefore, it was indicated that a visible status of security is needed (Furnell, 2007; Nurse et al., 2011), while we should further discuss how to provide a security status which causes less interruption. In general, adding feedback information could increase perceived security, satisfaction, and continuous intention toward the system, and in the meanwhile, its effects on the usability of the system are influenced by the social context.

6.2 The Social Context and Behaviors in Relation to Security Settings

We found that the participants displayed various behaviors in relation to security settings according to the social context. Participants exhibited more behaviors in relation to security settings in the contexts with a low social presence level (F(1,59) = 13.703, $p < 0.001$) or a low trust level (F(1,59) = 44.760, $p < 0.001$), suggesting that these context involves more security risks. Previous research has revealed the negative relationship between trust and risks (Olivero and Lunt, 2004; Yang et al., 2015). This study indicated that the low trust contexts encouraged participants to undertake more security practices. Although there are few studies about social presence and risks, the result of this study suggested that users could perceive more risks in the low social presence contexts, which prompt them to undertake more behaviors in relation to security settings.

The descriptive analysis indicated that participants the most frequently exhibited behaviors in relation to password protection settings in all payment tasks. To be specific, participants used two-way authentication scheme the most frequently among four authentication methods. This result suggested that participants would like to apply two-factor authentication scheme in all conditions. Although the simple authentication method (i.e., no authentication used and one-factor authentication scheme) is faster and convenient, users prefer to apply the two-way authentication scheme for enhancing security (Gunson et al., 2011). Therefore, designers and practitioners could consider allowing the two-factor authentication scheme as the default settings in mobile payments. While the prototypes only enabled participants to modify one privacy setting, participants exhibited a mean number of 0.64 behaviors in privacy protection settings in the low trust context. Additionally, we found that participants displayed more behaviors in relation to enhanced control settings in the low trust context. The specific behaviors in relation to security settings in the low trust context suggested that the security settings for privacy protection and system control were in demand in this situation.

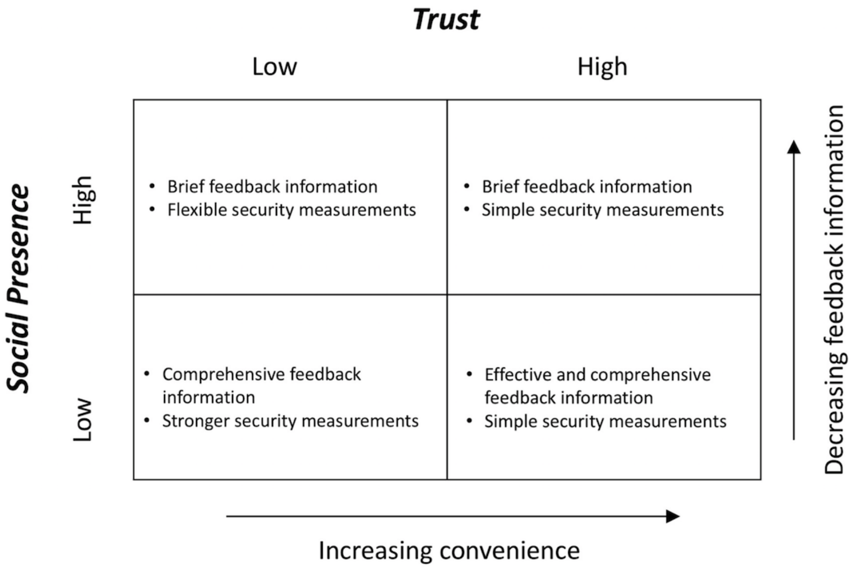
6.3 The Social Context and Perceptions

It was found that PS, PEOU, SA, and CU were varied from the social contexts. Additionally, PEOU, PU, SA and CU were affected by the interaction effects of feedback design and social context. The participants reported that they perceived a higher level of security in the high social presence context and the high trust context (Nilashi et al., 2015; Shin and Shin, 2011) , even though they undertook fewer behaviors in relation to security settings in these contexts . This is probably because participants perceived fewer risks in the high social presence context and the high trust context (Yang et al., 2015), leading to the increase of PS (Khalilzadeh et al., 2017; Olivero and Lunt, 2004).

There was a simple positive main effect of trust on PEOU, and there was no main effect of social presence and trust on PU. Nevertheless, we observed significant differences of participants' PEOU and PU between CI and CIFI in particular social contexts. For example, in the high trust context, the PEOU of CIFI (mean = 8.339) was significantly greater than that of CI (mean = 8.150). This is likely because the feedback information could better assist participants to balance security and convenience in the high trust context. Since participants would display fewer behaviors in relation to security settings in the high trust context (mean=2.02) than in the low trust context (mean= 2.93, F(1,59) = 44.760, $p < 0.001$), they might need help to adjust their security strategies (van Bavel et al., 2019). When the payment status and risk status were visible, users were able to change to a more effective security strategies (such as a simple authentication scheme and fewer security settings) in the high trust context based on the suggestions provided by the feedback information. Therefore, users perceived CIFI was easier to use in the high trust context. In contrast with PEOU, the mean of PU of CIFI decreased slightly from 8.04 to 7.93 as the social presence level rose, while the mean of PU of CI significantly increased from 7.67 to 7.90 as the social presence level increased. Additionally, there was no significant difference of PU between CI and CIFI in the high social presence context. The feedback information has positive effect on perceived social presence (Lu et al., 2016). Therefore, participants' demand for the feedback information was a compensation for the loss of presence in the low social presence context. However, this compensation was less needed in the high social presence. As a result, users considered CI was less useful than CIFI in the low social presence context and it was as useful as CIFI in the high social presence context.

Although social presence has a positive effect on SA and both social presence and trust have positive effects on CU, the influences are different between CI and CIFI. When using CIFI, SA and CU varied slightly in different social contexts. However, when using CI, participants' SA and CU had a distinct difference between two levels of social presence. As discussed above, the feedback information can increase perceived social presence in e-commerce (Lu et al., 2016). Additionally, social presence has a positively effect on continuous use intention (Hassanein and Head, 2007). Participants reported lower scores of SA and CU on CI in the low social presence context, because there was lack of a sense of social presence. Without feedback information, CI could not satisfy users' needs in the low social presence context. However, CI's SA and CU rose in the payment context where payees were present. It was indicated that participants' demand for feedback information decreased in the high social presence context. This explains why participants felt more satisfied and willing to continuously use CI in the high social presence context. These findings implied that the feedback information might be less needed in the high social presence context. Practitioners and designers could think of embedding less feedback information in the high social presence context.

6.4 Design Implications



Social Presence	Trust: Low	Trust: High
High	• Brief feedback information • Flexible security measurements	• Brief feedback information • Simple security measurements
Low	• Comprehensive feedback information • Stronger security measurements	• Effective and comprehensive feedback information • Simple security measurements

Figure 11. Framework for providing security settings and feedback information in different social contexts

This study investigated the fit between security settings, feedback information, and social contexts by explaining the influences of feedback design, social presence, and trust on participants' behaviors and perceptions. The findings revealed participants' preferences for security measures and feedback information through discussing behaviors, perceptions of security and usability, and continuous use intention. Summarizing the results and findings, we propose the following implications for embedding security measures and feedback information into the four social contexts (see Figure 11). However, this study was conducted with university students aged between 18 and 30 and had experienced using mobile payments in mainland China, and the implications typically address the fit between security settings, feedback information, and social contexts in terms of mobile payments for this user type. The generalization of the findings and the implications for other population groups (e.g. non-students, older adults, or users with different cultural background) should be further validated.

6.4.1 The social context with a high social presence level and a high trust level

Based on the findings, we suggest designers and practitioners to embed simple security settings and brief feedback information in this social context. In this context, we observed that participants undertook fewer behaviors in relation to security settings, and also PU of CIFI decreased in the high social presence context. Although security is vital in mobile payment transactions (Zhang et al., 2019; Zhang and Luximon, 2020), we could focus on users' preferred security functions and provide fewer security measurements to increase usability in the high social presence and high trust context (Weir et al., 2009). For example, when an individual is paying to a friend next to him/her, he/she can apply a one-factor authentication scheme and receive a brief feedback information that informs him/her that the payment is settled.

6.4.2 The social context with a low social presence level and a high trust level

The findings imply that it would be better to assign effective and comprehensive feedback information and simple security measurements in this context. Participants reported that the interface with a comprehensive feedback information was easier to use in the low social presence context. Additionally, participants exhibited fewer behaviors in relation to security settings in the high trust context. Therefore, the design of the interface could highlight users' needs for feedback information rather than security measurements in this social context. For instance, users can use a simple authentication scheme (i.e., one-factor authentication scheme) and get feedback information to ascertain the payment status and the identity of the payee when they are transferring to a trusted payee who is not physically present in this context.

6.4.3 The social context with a high social presence level and a low trust level

This study implies that less feedback information and more security measurements are needed in this context. The results revealed that participants tended to prioritize security over convenience in the low trust context. Therefore, practitioners and designers could embed more security measurements, particularly the privacy settings and system control settings in this social context. However, to improve usability, we could provide flexible security functions which allow users to tailor the security measurements (Gong and Tarasewich, 2004). For example, the interface can enable users to undertake an anonymous method to pay (i.e., using a nickname and hiding the payers' name) and allow users to customize the payment settings (i.e., modifying the authentication schemes, the daily limit and the transfer date) when users believe that the payee is untrusted. The necessary feedback information can be provided to warn users about the potential risks and inform them of the payment status.

6.4.4 The social context with a low social presence level and a low trust level

Practitioners and designers can design stronger security measurements and comprehensive feedback information in this social context. Participants exhibited more behaviors in relation to security settings and they were more satisfied with the interface which embedded with feedback information in this context than others. Participants were concerned about security and privacy risks in this context. Therefore, we can focus on providing a secure transaction process in this context. For example, the interface can provide a multiple authentication scheme, privacy settings and system control settings when users are paying to an untrusted online payee. Additionally, a comprehensive feedback information, such as providing a visible payment process and payment status, the identity information of the payee, and the risk information are necessary in this context.

7 Conclusion

This study investigated the fit between security settings, feedback information, and social contexts by observing users' preferences and perceptions for security design in different social contexts. Following the DSR approach, this study developed prototypes and payment scenarios as artefacts that were used in the experiment to understand the fit problems and generate design implications. The results demonstrated that behaviors in relation to security settings are significantly affected by social presence and trust. However, feedback information does not influence participants' preferences regarding security settings in different social contexts. Feedback design, social presence, and trust can increase PS, SA, and CU in all payment scenarios, while there are only interaction effects on PEOU and PU. Overall, the findings revealed that preferences concerning security settings vary between different social contexts. Participants tended to undertake more behaviors in relation to security settings in the low social presence and low trust context. With regard to feedback information, the findings suggested that the addition of feedback information can be matched with the low social presence context by considering the perceptions of security and usability. The design implications propose insights into balance security and usability based on the social contexts.

However, this study focuses on the two contextual factors of social context. Since other possible contextual factors are still unexplored, future studies could further investigate the relationships between use contexts and security design. Additionally, this study embedded three types of feedback information together into the prototype CIFI. It is noted that different types of feedback information (Walter et al., 2015) would have various effects on perceptions and behaviors. A future study on discussing the effects of specific types of feedback information could be conducted. Additionally, the results and findings were mainly generated from the views of university students and the age range of the participants were between 18 and 30. However, young adults and students can merely represent a part of mobile payment users. Therefore, the findings might have a limitation in generalizability. The extension of these findings to different population groups should be further discussed and validated in future work, as the demographic characteristics and cultural differences might influence the results.

Acknowledgements

This work was supported by the Hong Kong Polytechnic University under the UGC Funding Scheme [Grant Number RUPB].

Appendix

Table A. Measurements of Perceptions and Attitudes

Constructs	Description
Perceived Security (PS) (adapted from Khalilzadeh et al., 2017)	PS1 In this situation, I perceive that my transaction information would not go wrong.
	PS2 In this situation, I perceive that my sensitive information is protected.
	PS3 In this situation, I perceive that the transaction is financially secure.
	PS4 In this situation, I perceive that mobile payment platforms are secure systems to conduct a transaction.

Perceived Ease of Use (PEOU) (adapted from Yoon and Steege, 2013; Liao et al., 2007; Davis, 1989)	PEOU1 In this situation, it is easy for me to operate this interface. PEOU2 In this situation, this interface is easy to use. PEOU3 In this situation, this interface is easy to operate.
Perceived Usefulness (PU) (adapted from Yoon and Steege, 2013; Liao et al., 2007; Davis, 1989)	PU1 In this situation, this interface enables me to settle my payment quickly. PU2 In this situation, this interface enables me to settle my payment effectively. PU3 In this situation, this interface enables me to settle my payment easier.
Satisfaction (SA) (adapted from Chang and Chen, 2008; Liao et al., 2007)	SA1 In this situation, I feel satisfied with this interface. SA2 In this situation, I like using this interface for payment. SA3 In this situation, using this interface makes me feel pleased.
Continuous Use Intention (CU) (adapted from Zhou, 2011; Kim et al., 2010)	CU1 I would like to continue to use this mobile payment system to pay. CU2 I would like to frequently use this mobile payment system to pay. CU3 I would like to use this mobile payment system to pay in the future.

Reference

Beutin, N., Schadbach, D., 2017. Mobile Payment Report 2017: What customers really want. https://doi.org/10.1016/j.envpol.2011.08.003

Botha, R.A., Furnell, S.M., Clarke, N.L., 2009. From desktop to mobile: Examining the security experience. Comput. Secur. 28, 130–137. https://doi.org/10.1016/j.cose.2008.11.001

Cavdar, S.K., Taskaya-Temizel, T., Musolesi, M., Tino, P., 2020. A multi-perspective analysis of social context and personal factors in office settings for the design of an effective mobile notification system. Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol. 4. https://doi.org/10.1145/3381000

Chang, H.H., Chen, S.W., 2008. The impact of customer interface quality, satisfaction and switching costs on e-loyalty: Internet experience as a moderator. Comput. Human Behav. 24, 2927–2944. https://doi.org/10.1016/j.chb.2008.04.014

China, P.& C.A. of, 2018. 2019 China Mobile Payment Development Report [WWW Document]. URL http://www.pcac.org.cn/index.php/focus/list_details/ids/654/id/50/topicid/3.html

Choi, J., Nazareth, D.L., 2014. Repairing trust in an e-commerce and security context: An agent-based modeling approach. Inf. Manag. Comput. Secur. 22, 490–512. https://doi.org/10.1108/IMCS-09-2013-0069

Chong, A.Y.L., Chan, F.T.S., Ooi, K.B., 2012. Predicting consumer decisions to adopt mobile commerce: Cross country empirical examination between China and Malaysia. Decis. Support Syst. https://doi.org/10.1016/j.dss.2011.12.001

Coursaris, C.K., Kim, D.J., 2011. A Meta-Analytical Review of Empirical Mobile Usability Studies. J. Usability Stud. 6, 117–171.

Das, A., Khan, H.U., 2016. Security behaviors of smartphone users. Inf. Comput. Secur. 24, 116–134. https://doi.org/10.1108/ICS-04-2015-0018

Davis, F.D., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. Manag. Inf. Syst. 13, 319–339. https://doi.org/10.2307/249008

de Kerviler, G., Demoulin, N.T.M., Zidda, P., 2016. Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers? J. Retail. Consum. Serv. 31, 334–344. https://doi.org/10.1016/j.jretconser.2016.04.011

De Leoz, G., Petter, S., 2018. Considering the social impacts of artefacts in information systems design science research. Eur. J. Inf. Syst. 27, 154–170. https://doi.org/10.1080/0960085X.2018.1445462

Dey, A.K., 2001. Understanding and Using Context. Pers. Ubiquitous Comput. 5, 4–7. https://doi.org/10.1371/journal.pone.0154625

Dhillon, G., Oliveira, T., Susarapu, S., Caldeira, M., 2016. Deciding between information security and usability: Developing value based objectives. Comput. Human Behav. 61, 656–666. https://doi.org/10.1016/j.chb.2016.03.068

Dincelli, E., Chengalur-smith, I., 2020. Choose your own training adventure : designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. Eur. J. Inf. Syst. 00, 1–19. https://doi.org/10.1080/0960085X.2020.1797546

Dincelli, E., Yayla, A., Kusyk, L., 2020. Cyber Attack ! A Story-driven Educational Hacking Game, in: In Proceedings of the 16th USENIX Symposium on Usable Privacy and Security (SOUPS). Boston, MA.

Dourish, P., 2004. What we talk about when we talk about context. Pers. Ubiquitous Comput. 8, 19–30. https://doi.org/10.1007/s00779-003-0253-8

Dourish, P., Anderson, K., 2006. Collective information practice: Exploring privacy and security as social and cultural phenomena. Human-Computer Interact. 21, 319–342. https://doi.org/10.1207/s15327051hci2103_2

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. Pers. Ubiquitous Comput. 8, 391–401. https://doi.org/10.1007/s00779-004-0308-5

Field, A. 2009. Discovering statistics using SPSS. (Sage, Ed.). London.

Furnell, S., 2007. Making security usable: Are things improving? Comput. Secur. 26, 434–443. https://doi.org/10.1016/j.cose.2007.06.003

Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W., Li, N., 2018. Enhancing security behaviour by supporting the user. Comput. Secur. 75, 1–9. https://doi.org/10.1016/j.cose.2018.01.016

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. Comput. Human Behav. 53, 249–262. https://doi.org/10.1016/j.chb.2015.07.014

Garaialde, D., Bowers, C.P., Pinder, C., Shah, P., Parashar, S., Clark, L., Cowan, B.R., 2020. Quantifying the impact of making and breaking interface habits. Int. J. Hum. Comput. Stud. 142. https://doi.org/10.1016/j.ijhcs.2020.102461

Gebauer, J., Shaw, M.J., Gribbins, M.L., 2010. Task-technology fit for mobile information systems. J. Inf. Technol. 25, 259–272. https://doi.org/10.1057/jit.2010.10

Geerts, G.L., 2011. A design science research methodology and its application to accounting information systems research. Int. J. Account. Inf. Syst. 12, 142–151. https://doi.org/10.1016/j.accinf.2011.02.004

Gefen, D., Straub, D.W., 2004. Consumer trust in B2C e-Commerce and the importance of social presence: Experiments in e-Products and e-Services. Omega 32, 407–424. https://doi.org/10.1016/j.omega.2004.01.006

George, D., 2011. SPSS for windows step by step: A simple study guide and reference, 17.0 updat. ed. Pearson Education India.

Göktürk, M., Şişaneci, I., 2014. A perception oriented approach for usable and secure interface development, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 23–31. https://doi.org/10.1007/978-3-319-07638-6_3

Gong, J., Tarasewich, P., 2004. Guidelines for handheld mobile device interface design. Proc. DSI 2004 Annu. Meet. 3751–3756.

Goodhue, D.L., Thompson, R.L., 1995. Task-Technology Fit and Individual Performance. MIS Q. 19, 213–236.

Gravetter, F., Wallnau, L., 2014. Essentials of statistics for the behavioral sciences, 8th ed. ed. Wadsworth, Belmont.

Gunson, N., Marshall, D., Morton, H., Jack, M., 2011. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Comput. Secur. 30, 208–220. https://doi.org/10.1016/j.cose.2010.12.001

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. Decis. Support Syst. 62, 11–21. https://doi.org/10.1016/j.dss.2014.02.006

Hassanein, K., Head, M., 2007. Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. Int. J. Hum. Comput. Stud. 65, 689–708. https://doi.org/10.1016/j.ijhcs.2006.11.018

Hevner, A.R., March, S.T., Park, J., Ram, S., 2004. Design Science in Information Systems Research. MIS Q. 28, 75–105.

Hsin Chang, H., 2010. Task-technology fit and user acceptance of online auction. Int. J. Hum. Comput. Stud. 68, 69–89. https://doi.org/10.1016/j.ijhcs.2009.09.010

Huh, J.H., Verma, S., Sri V Rayala, S., Bobba, R., Beznosov, K., Kim, H., 2017. I Don't Use Apple Pay Because It's Less Secure ...: Perception of Security and Usability in Mobile Tap-and-Pay, in: Proceedings 2017 Workshop on Usable Security. Internet Society, Reston, VA. https://doi.org/10.14722/usec.2017.23021

Ion, I., Langheinrich, M., Kumaraguru, P., Čapkun, S., 2010. Influence of user perception, security needs, and social factors on device pairing method choices, in: ACM International Conference Proceeding Series. https://doi.org/10.1145/1837110.1837118

Jarvenpaa, S.L., Lang, K.R., 2005. Managing the Paradoxes of Mobile Technology. Inf. Syst. Manag. 22, 7–23. https://doi.org/10.1201/1078.10580530/45520.22.4.20050901/90026.2

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. Comput. Human Behav. 79, 111–122. https://doi.org/10.1016/j.chb.2017.10.035

Johnston, J., Eloff, J.H.P., Labuschagne, L., 2003. Security and human computer interfaces. Comput. Secur. 22, 675–684. https://doi.org/10.1016/S0167-4048(03)00006-3

Junglas, I., Abraham, C., Watson, R.T., 2008. Task-technology fit for mobile locatable information systems. Decis. Support Syst. 45, 1046–1057. https://doi.org/10.1016/j.dss.2008.02.007

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. Eur. J. Inf. Syst. 17, 387–402. https://doi.org/10.1057/ejis.2008.29

Kabanda, S. Power dynamics in e-commerce adoption in least developing countries: The case of dar-es-salaam SMEs, Tanzania. In International Conference on e-Infrastructure and e-Services for Developing Countries. Springer, Berlin, Heidelberg. pp. 218-227.

Kamoun, F., Halaweh, M., 2012. User interface design and e-commerce security perception: An empirical study. Int. J. E-bus. Res. 8, 15–32. https://doi.org/10.4018/jebr.2012040102

Karat, C.M., Karat, J., Brodie, C., 2005. Why HCI research in privacy and security is critical now. Int. J. Hum. Comput. Stud. 63, 1–4. https://doi.org/10.1016/j.ijhcs.2005.04.016

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

Kim, C., Mirusmonov, M., Lee, I., 2010. An empirical examination of factors influencing the intention to use mobile payment. Comput. Human Behav. 26, 310–322. https://doi.org/10.1016/j.chb.2009.10.013

Kim, M.J., Chung, N., Lee, C.-K., Preis, M.W., 2015. Motivations and Use Context in Mobile Tourism Shopping: Applying Contingency and Task–Technology Fit Theories. Int. J. Tour. Res. 17, 13–24. https://doi.org/10.1002/jtr

Kim, T. (Terry), Suh, Y.K., Lee, G., Choi, B.G., 2010. Modelling Roles of Task-technology Fit and Self-efficacy in Hotel Employees' Usage Behaviours of Hotel Information Systems. Int. J. Tour. Res. 709–725.

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. ACM, New York, USA, p. Article No.11. https://doi.org/10.1145/1899475.1899486

Kortum, P., Oswald, F.L., 2018. The Impact of Personality on the Subjective Assessment of Usability. Int. J. Human–Computer Interact. 34, 177–186. https://doi.org/10.1080/10447318.2017.1336317

Lah, U., Lewis, J.R., šumak, B., 2020. Perceived Usability and the Modified Technology Acceptance Model. Int. J. Human–Computer Interact. 36, 1216–1230.

Lankton, N.K., McKnight, D.H., Tripp, J.F., 2017. Facebook privacy management strategies: A cluster analysis of user privacy behaviors. Comput. Human Behav. 76, 149–163. https://doi.org/10.1016/j.chb.2017.07.015

Lee, I., Kim, Jaesoo, Kim, Jinwoo, 2005. Use contexts for the mobile internet: A longitudinal study monitoring actual use of mobile internet services. Int. J. Hum. Comput. Interact. 18, 269–292. https://doi.org/10.1207/s15327590ijhc1803_2

Lewis, J.R., Utesch, B.S., Maher, D.E., 2015. Measuring Perceived Usability: The SUS, UMUX-LITE, and AltUsability. Int. J. Hum. Comput. Interact. 31, 496–505. https://doi.org/10.1080/10447318.2015.1064654

Lewis, K., Kaufman, J., Christakis, N., 2008. The taste for privacy: An analysis of college student privacy settings in an online social network. J. Comput. Commun. 14, 79–100. https://doi.org/10.1111/j.1083-6101.2008.01432.x

Li, Y.-M., Yeh, Y.-S., 2010. Increasing trust in mobile commerce through design aesthetics. Comput. Human Behav. 26, 673–684. https://doi.org/10.1016/j.chb.2010.01.004

Liang, T.-P., Ling, Y.-L., Yeh, Y.-H., Lin, B., 2013. Contextual factors and continuance intention of mobile services. Int. J. Mob. Commun. 11, 313–329.

Liao, C., Chen, J.L., Yen, D.C., 2007. Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: An integrated model. Comput. Human Behav. 23, 2804–2822. https://doi.org/10.1016/j.chb.2006.05.006

Liébana-Cabanillas, F., Sánchez-Fernández, J., Muñoz-Leiva, F., 2014. Antecedents of the adoption of the new mobile payment systems : The moderating effect of age. Comput. Human Behav. 35, 464–478. https://doi.org/10.1016/j.chb.2014.03.022

Lu, B., Fan, W., Zhou, M., 2016. Social presence, trust, and social commerce purchase intention: An empirical research. Comput. Human Behav. 56, 225–237. https://doi.org/10.1016/j.chb.2015.11.057

Lu, H.P., Yang, Y.W., 2014. Toward an understanding of the behavioral intention to use a social networking site: An extension of task-technology fit to social-technology fit. Comput. Human Behav. 34, 323–332. https://doi.org/10.1016/j.chb.2013.10.020

Lu, J., Wei, J., Yu, C.S., Liu, C., 2017. How do post-usage factors and espoused cultural values impact mobile payment continuation? Behav. Inf. Technol. 36, 140–164. https://doi.org/10.1080/0144929X.2016.1208773

Mallat, N., 2007. Exploring consumer adoption of mobile payments – A qualitative study. J. Strateg. Inf. Syst. 16, 413–432. https://doi.org/10.1016/j.jsis.2007.08.001

Mallat, N., Rossi, M., Tuunainen, V.K., O¨o¨rni, A., 2009. The impact of use context on mobile services acceptance: The case of mobile ticketing. Inf. Manag. 46, 190–195. https://doi.org/10.1016/j.im.2008.11.008

Mathieson, K., Keil, M., 1998. Beyond the interface: Ease of use and task/technology. Inf. Manag. 34, 221–230.

Mohamed, M.A., Chakraborty, J., Dehlinger, J., 2017. Trading off usability and security in user interface design through mental models. Behav. Inf. Technol. 36, 493–516. https://doi.org/10.1080/0144929X.2016.1262897

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. Adv. Eng. Softw. 40, 1231–1241. https://doi.org/10.1016/j.advengsoft.2009.01.024

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. J. Retail. Consum. Serv. 26, 57–69. https://doi.org/10.1016/j.jretconser.2015.05.002

Nurse, J.R.C., Creese, S., Goldsmith, M., Lamberts, K., 2011. Guidelines for usable cybersecurity: Past and present, in: Proceedings - 2011 3rd International Workshop on Cyberspace Safety and Security, CSS 2011. pp. 21–26. https://doi.org/10.1109/CSS.2011.6058566

Oliveira, T., Thomas, M., Baptista, G., Campos, F., 2016. Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. Comput. Human Behav. 61, 404–414. https://doi.org/10.1016/j.chb.2016.03.030

Olivero, N., Lunt, P., 2004. Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. J. Econ. Psychol. 25, 243–262. https://doi.org/10.1016/S0167-4870(02)00172-1

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

Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S., 2007. A Design Science Research Methodology for Information Systems Research. J. Manag. Inf. Syst. 24, 45–77. https://doi.org/10.2753/MIS0742-1222240302

Salisbury, W.D., Pearson, R.A., Pearson, A.W., Miller, D.W., 2001. Perceived security and World Wide Web purchase intention. Ind. Manag. Data Syst. 101, 165–177. https://doi.org/10.1108/02635570110390071

Shao, Z., Zhang, L., Li, X., Guo, Y., 2019. Antecedents of trust and continuance intention in mobile payment platforms: The moderating effect of gender. Electron. Commer. Res. Appl. 33, 1–10. https://doi.org/10.1016/j.elerap.2018.100823

Shin, D.H., Shin, Y.J., 2011. Consumers' trust in virtual mall shopping: The role of social presence and perceived security. Int. J. Hum. Comput. Interact. 27, 450–475. https://doi.org/10.1080/10447318.2011.552060

Short, J., Williams, E., & Christie, B., 1976. The social psychology of telecommunications. John Wiley & Sons.

Still, J.D., Cain, A., Schuster, D., 2017. Human-centered authentication guidelines. Inf. Comput. Secur. 25, 437–453. https://doi.org/10.1108/ICS-04-2016-0034

Sutcliffe, A.G., Wang, D., Dunbar, R.I.M., 2015. Modelling the role of trust in social relationships. ACM Trans. Internet Technol. 15, 16–24. https://doi.org/10.1145/2815620

Tossell, C.C., Kortum, P., Shepard, C., Rahmati, A., Zhong, L., 2012. An empirical analysis of smartphone personalisation: Measurement and user variability. Behav. Inf. Technol. 31, 995–1010. https://doi.org/10.1080/0144929X.2012.687773

Trochim, W.M., Donnelly, J.P., 2006. The research methods knowledge base, 3rd ed. ed. OH:Atomic Dog, Cincinnati.

Van Aken, J.E., 2004. Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules. J. Manag. Stud. 41, 219–246. https://doi.org/10.1111/j.1467-6486.2004.00430.x

van Bavel, R., Rodríguez-Priego, N., Vila, J., Briggs, P., 2019. Using protection motivation theory in the design of nudges to improve online security behavior. Int. J. Hum. Comput. Stud. 123, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Venable, J., Pries-Heje, J., Baskerville, R., 2016. FEDS: A Framework for Evaluation in Design Science Research. Eur. J. Inf. Syst. 25, 77–89. https://doi.org/10.1057/ejis.2014.36

Walter, N., Ortbach, K., Niehaves, B., 2015. Designing electronic feedback - Analyzing the effects of social presence on perceived feedback usefulness. Int. J. Hum. Comput. Stud. 76, 1–11. https://doi.org/10.1016/j.ijhcs.2014.12.001

Wang, Y., Xia, H., Huang, Y., 2016. Examining American and Chinese Internet Users-Contextual Privacy Preferences of Behavioral Advertising, in: Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing - CSCW '16. pp. 538–551. https://doi.org/10.1145/2818048.2819941

Watson, J., Lipford, H.R., Besmer, A., 2015. Mapping User Preference to Privacy Default Settings. ACM Trans. Comput. Interact. 22.

Weir, C.S., Douglas, G., Carruthers, M., Jack, M., 2009. User perceptions of security, convenience and usability for ebanking authentication tokens. Comput. Secur. 28, 47–62. https://doi.org/10.1016/j.cose.2008.09.008

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

Wu, B., Chen, X., 2017. Continuance intention to use MOOCs: Integrating the technology acceptance model (TAM) and task technology fit (TTF) model. Comput. Human Behav. 67, 221–232.

Yang, Q., Pang, C., Liu, L., Yen, D.C., Michael Tarn, J., 2015. Exploring consumer perceived risk and trust for online payments: An empirical study in China's younger generation. Comput. Human Behav. 50, 9–24. https://doi.org/10.1016/j.chb.2015.03.058

Yee, K.-P., 2003. Secure Interaction Design and the Principle of Least Authority. Communications.

Yoon, H.S., Barker Steege, L.M., 2013. Development of a quantitative model of the impact of customers' personality and perceptions on Internet banking use. Comput. Human Behav. 29, 1133–1141. https://doi.org/10.1016/j.chb.2012.10.005

Yuan, S., Liu, Y., Yao, R., Liu, J., 2016. An investigation of users' continuance intention towards mobile banking in China. Inf. Dev. 32, 20–34. https://doi.org/10.1177/0266666914522140

Zhang, J., Luximon, Y., 2020. A quantitative diary study of perceptions of security in mobile payment transactions. Behav. Inf. Technol. 0, 1–24. https://doi.org/10.1080/0144929X.2020.1771418

Zhang, J., Luximon, Y., Song, Y., 2019. The role of consumers' perceived security, perceived control, interface design features, and conscientiousness in continuous use of mobile payment services. Sustain. 11. https://doi.org/10.3390/su11236843

Zhou, T., Lu, Y., Wang, B., 2010. Computers in Human Behavior Integrating TTF and UTAUT to explain mobile banking user adoption. Comput. Human Behav. 26, 760–767. https://doi.org/10.1016/j.chb.2010.01.013

Zigurs, I., Buckland, B.K., 1998. A Theory of Task / Technology Fit and Group Support Systems Effectiveness. MIS Quart. 22, 313–334.

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: Tryfonas, T. (Ed.), Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science. Springer, Cham, pp. 265–283. https://doi.org/10.1007/978-3-319-58460-7_18