Article

The Role of Consumers' Perceived Security, Perceived Control, Interface Design Features, and Conscientiousness in Continuous Use of Mobile Payment Services

Jiaxin Zhang, Yan Luximon * and Yao Song

School of Design, The Hong Kong Polytechnic University, Kowloon, Hong Kong, China;
jx.zhang@connect.polyu.hk (J.Z.); yao.song@connect.polyu.hk (Y.S.)
* Correspondence: yan.luximon@polyu.edu.hk; Tel.: +852-2766-5493

check for
updates

Abstract: Mobile payment has played a vital role in transforming traditional payment methods into digital payment methods and has led to changes in consumers' behaviors in economic exchanges. However, there is a lack of knowledge about how perceived security influences are a sustainable use of mobile payment services. In order to examine the impact of perceived security on users' continuous use, especially regarding mobile payment services and factors related to perceived security (i.e., perceived control, interface design features, and conscientiousness), an empirical study was conducted to collect data from 252 participants. Then, the proposed research model was examined using structural equation modelling. The results revealed that the perception of interface design features was influenced by conscientiousness. Perceived security was affected by perceived control, the perception of interface design features, and conscientiousness. Moreover, perceived security was identified to have a strong impact on continuous intention to use mobile payment. The design implications for mobile service providers and designers are presented.

Keywords: Mobile payment; continuous use; perceived security; perceived control; interface design features; conscientiousness

1. Introduction

Along with advances in communication technologies, mobile commerce (m-commerce) has been experiencing rapid development worldwide in recent years. Mobile payment, which allows users to settle transactions for goods, bills, and services using mobile devices, has played a vital role in m-commerce [1]. Mobile payment services are defined as services in which a mobile device is used to settle payments for goods, services, and bills through wireless and other communication technologies [2]. Compared with traditional payment methods, mobile payment is fast, secure, and convenient [3]. Consumers can use it to pay in online and offline situations, at anytime from anywhere, and merchants can apply it to reduce transaction costs and maintain customer relationships [3]. Overall, it is a promising technology that facilitates the development of a cashless society. While the worldwide adoption of mobile payment has been uneven [4], it is enjoying rapid growth in the Chinese market [5]. In 2018, there were about 890 million mobile payment users in China [6]. According to the results of a survey conducted by the Payment and Clearing Association of China [6], most consumers (95.6%) used mobile payment services because of their ease of use and convenience, but 64.7% stated that security was a major concern, with 77.8% asking for improvement of the security of mobile payment services. In addition, 79.2% of users expected feedback warning and more than 50% required better security management.

Surprisingly, some studies have claimed that mobile payment is more secure than traditional payment methods [3], but many consumers still regard it as less secure. The gap between actual security and users' perceived security raises an interesting question for researchers regarding the influence of perceived security on technology adoption. Studies have provided evidence regarding the impact of perceived security on technology adoption, including m-commerce adoption [7–14]. Unlike technical security, perceived security is a psychological concept. Salisbury, Pearson, and Pearson [15] defined perceived security as the perceived extent to which one can transmit sensitive information securely over the web [7,15]. This definition has been adapted to fit different research contexts [7,11]. For example, in the context of mobile payment, perceived security can be defined as the degree to which mobile payment users believe that transactions on mobile payment platforms are secure in terms of both financial and personal information aspects [7,9,13]. As perceived security plays a vital in users' behaviors related to technology, many efforts have been made to explore the influential factors of perceived security. For example, some researchers identified the cognitive determinants of perceived security through cognitive aspects, including perceived controllability, perceived confidentiality, perceived availability, and perceived non-repudiation [7,16]. Other researchers concentrated on the interface features and individual characteristics that influence perceived security in e-commerce [12,17,18]. Although these studies revealed the importance of interface design, the influences of specific interface features on perceived security remain unclear. Moreover, research on interface design features in an e-commerce context may be inapplicable to m-commerce. Thus, there are research opportunities to explore this topic in the context of m-commerce. In a study focusing on the influence of individual characteristics, Shin [12] confirmed the moderating effects of age and income on the path between perceived security and use intention. In addition, some researchers revealed the influences of personality traits on security behaviors [19]. Since users' security behaviors are strongly affected by their security perceptions, personality traits could be a predictor of perceived security. However, there is still little research on the relationship between personality traits and perceived security.

In addition to considering the effect of perceived security on mobile payment adoption, it is crucial for service providers to maintain continuous use of mobile payment because they invested great resources and effort in the service [20,21]. If users are unsatisfied with the service, they can easily switch to another platform [1]. Although many researchers have proposed determinants of initial adoption of mobile payment [9,13,22–25], these determinants may have different impacts after adoption [26]. As the adoption of mobile payment services has increased, researchers have begun to study users' post-adoption behaviors and develop different research models [1,23,26–28]. For example, Gao, Waechter, and Bai [23] extended the flow theory to confirm that privacy and security concerns affect trust, flow, and satisfaction, which in turn affect continuous intention, suggesting that users' attitude towards security could be a significant predictor of their post-adoption behavior. However, an interesting question must still be answered: How can continuous intention to use mobile payment services be facilitated by improving perceived security? To address this question, we explore the relationship between continuous use and perceived security and investigate the antecedents of perceived security.

Since previous studies identified the antecedents of perceived security from cognitive and technological perspectives, this study aims to explore perceived security from the perspectives of interface design and personality traits. The study will add to the body of research on this topic by theoretically examining determining factors of perceived security, considering the relationships among perceived control, perception of interface design features, and conscientiousness and confirming the effect of perceived security on continuous use of mobile payment services. This study aims to address the following research questions:

Research question (RQ) 1: How do users' perception of interface design affect perceived control and perceived security?

RQ2: How does conscientiousness influence perception of interface design and perceived security?

RQ3: To what extent does perceived control influence perceived security?

RQ4: To what extent does perceived security influence continuous use of mobile payment services?

This article is organized into six parts. Section 2 reviews the literature and then proposes hypotheses and a research model. Section 3 illustrates the method used to conduct this empirical study. Section 4 presents the results of the structural equation modelling (SEM) performed to test the research model. Sections 5 and 6 discuss the results and limitations of the research. The paper is concluded in Section 7.

The contributions of this research to mobile payment services are manifold. From a theoretical perspective, this study constructs a model for investigating the determining factors of perceived security related to the perception of interface design features, perceived control, and conscientiousness. Additionally, the findings provide empirical evidence highlighting the important role of perceived security in continuous intention to use mobile payment. From a practical point of view, the findings indicate that mobile payment service providers can retain users by enhancing the perceived security of services. Unique practical design insights that can be used to improve perceived security by strengthening the perceptions of customization and feedback design that are provided, and the importance of conscientiousness in users' perception of interface design features and security is emphasized. Since the perceptions of interface design features and conscientiousness are rarely examined in relation to perceived security in the context of mobile payment, the design implications of this study should help designers and service providers improve their work.

2. Literature Review and Hypotheses

2.1. Interface Design, Perceived Control, and Perceived Security

Perceived security and its determinants have been examined in many studies [7,16,29], but the results are not consistent since the definition of perceived security changes based on the research context [7,11]. In the context of mobile payment services, perceived security refers to the degree to which users believe that a transaction on a mobile payment platform is secure in terms of both financial and personal information aspects [7,9,13]. Since little research has explored the cognitive determinants of perceived security in m-commerce, it can be expected that the general cognitive determinants of perceived security in information systems can be applied to examine effects in this context. For example, Huang et al. [16] found that perceived security is related to perceived knowledge, perceived controllability, and perceived awareness in general information technology (IT) applications and that, among these factors, perceived controllability was found to be most effective [16]. Control is defined as one's ability to change events [30]. Likewise, perceived control is the extent to which one believes that one can control a situation [31]. Although perceived control inaccurately reflects one's actual control over an event, research has found that the former influences user behavior to a greater extent than the latter [30,31]. Indeed, there is evidence from many different fields that perceived control can influence behaviors in protecting personal information [31–33]. Although there is little evidence regarding the effect of perceived control on the perception of financial security, previous research on perceived control implied that it may have an effect. Thus, this study proposes that perceived control affects users' perceptions of the financial and personal information security of mobile payments:

H1. *Perceived control has a positive effect on the perceived security of mobile payment services.*

Since perceived control can alter users' behaviors, researchers have attempted to find ways to improve perceived control. For example, Suh and Han [34] studied the influence of perceived security control on e-commerce adoption, dividing perceived security control into five dimensions: authentication, nonrepudiation, confidentiality, privacy protection, and data integrity. They found that only nonrepudiation, privacy protection, and data integrity had a significant effect on e-commerce adoption [34]. Users could not fully understand the technical mechanisms of security control; their perceived control was determined by the information or functions provided by the interface. This means that users' perceptions of interface design features could influence perceived control [32]. In this

paper, we discuss the possible influence of perceptions of customization and feedback design on perceived control.

Customization, defined as a site's or device's ability to modify itself or to be modified by users, is one of the most important interface design features in m-commerce [35–38]. This paper focuses on user customization, highlighting the effect of functional customization on perceived control [39]. In the mobile payment field, customization is related to functional features, and it can be classified into customization of information functions, payment methods, and security settings [5]. For instance, Alipay's users can select the authentication methods used to authorize payments and change privacy settings to disclose or hide their information in transactions. Researchers have found that customization design have a positive influence on the sense of control [39–41]. Since perceived control is a predictor of perceived security, we expected that users would consider mobile payment transactions to be more secure when they believe that the interfaces offered to them are customizable:

H2. *The perception of customization design positively affects perceived control in mobile payment services.*

H3. *The perception of customization design positively affects perceived security in mobile payment services.*

Feedback is another interface design feature that has been found to impact m-commerce and information security [37,42,43]. Feedback refers to "any form of communication from a system towards the user" [42]. It enables users to obtain information about the internal state of the system and results of their actions [42,44], which can affect their decisions while performing a task. Based on this definition, it is reasonable for users to feel a sense of control in the payment process when there is a feedback intervention [45]. Feedback design also provide users with a sense of security by promoting perceived control [11]. To date, the effects of feedback on perceived control and perceived security have been rarely addressed. We hypothesized the following:

H4. *The perception of feedback design positively affects perceived control in mobile payment services.*

H5. *The perception of feedback design positively affects perceived security in mobile payment services.*

2.2. Perceived Security and Continuous Use Intention

While previous studies on m-commerce have explored initial adoption, the need to explore the factors that affect continuous use intention has attracted increasing attention [1,5,46]. Researchers have applied different models, such as the theory of planning behavior (TPB) and expectation confirmation theory (ECT), to explain users' continued use of online or mobile services [28,47]. In the specific context of m-commerce, trust, flow, and satisfaction have been proposed as three determinants of continuous intention [1,23]. Zhou [1] confirmed that system quality, information quality, and service quality have different effects on trust, flow, and satisfaction. Later, Gao, Waechter, and Bai [23] added that security and privacy concerns have significant negative effects on trust, flow and satisfaction and thus could be strong predictors of continuous use of m-commerce. Other researchers suggested that continuous use of a system is based on evaluation of its actual security [5]. However, average users might not be capable of figuring out to what extent the system is secure. They tend to perceive security through information provided by the interface. As security is a perception rather than reality for average users, some researchers addressed the influence of perceived security on post-adoption behaviors. For example, Ye, Seo, Desouza, Sangareddy, and Jha [48] proved that perceived security has an influence on users' switching behaviors regarding IT products, which is considered an important post-adoption behavior. However, it is still unclear how perceived security influences users' continuous use intention regarding mobile payment services. Thus, we propose the following:

H6. *Perceived security positively influences continuous use intention regarding mobile payment services.*

2.3. Personality Traits and Conscientiousness

Personality traits have been applied to explain variances in users' cognition and behaviors. Of the many personality theories that have been developed, this study focuses on conscientiousness from the Big Five personality traits—extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience [49–51]—to investigate the influences of this trait on individuals' behavioral intentions and actual behavior. In a previous study, Nicholson et al. found that risk-takers are more likely to have high extraversion and openness and low neuroticism, agreeableness, and conscientiousness [49]. In addition, in the context of Internet use and e-commerce, McElroy, Hendrickson, and Townsend [50] found that neurotic people prefer online shopping to avoid face-to-face interaction while open-minded people tend to search for information on the Internet to satisfy their curiosity [50].

Much research has highlighted the influence of conscientiousness on users' security and privacy concerns as well as security practices in an information system [52–54]. Conscientiousness refers to a character based on dependability, responsibility, and carefulness [55–58]. Conscientious people tend to have a high level of dutifulness and self-control [58,59]. Junglas et al. [52] found that conscientious users have a higher level of concern for privacy when using location-based services and McCormac et al. [54] demonstrated that users with high conscientiousness scores tend to have higher information security awareness scores, tending to take fewer risks. In addition, Shropshire et al. [53] claimed that conscientiousness could moderate the relationship between users' intention and actual adoption of security software. Overall, the literature suggests that users with higher levels of conscientiousness tend to make more of an effort to manage system security and take fewer risks. Since conscientiousness is believed to have a strong influence on security practices, we expected that it would also have an influence on perceived security.

Because interface features could help to maintain mobile payment systems, conscientiousness may result in higher demand for interface features. For example, in a mobile payment context, customization plays an important role in security practices and feedback information influences user security and privacy concerns [5,43], as both are based on interaction between systems and users. Users with higher levels of conscientiousness might have more positive attitudes toward customization and feedback design and may be more likely to take advantage of these features. Thus, we proposed that users' perception of customization and feedback design may be affected by conscientiousness:

H7. *Conscientiousness has a positive effect on the perception of feedback design in mobile payment services.*

H8. *Conscientiousness has a positive effect on the perception of customization design in mobile payment services.*

H9. *Conscientiousness has a positive effect on the perceived security of mobile payment services.*

We also proposed a new research model to explore the factors that influence perceived security and the effect of perceived security on continuous intention of mobile payment (see Figure 1). Using this model, we constructed the relationships between the perception of interface design features, conscientiousness, perceived control, and perceived security, and we measured the impact of perceived security on continuous use intention regarding mobile payment.
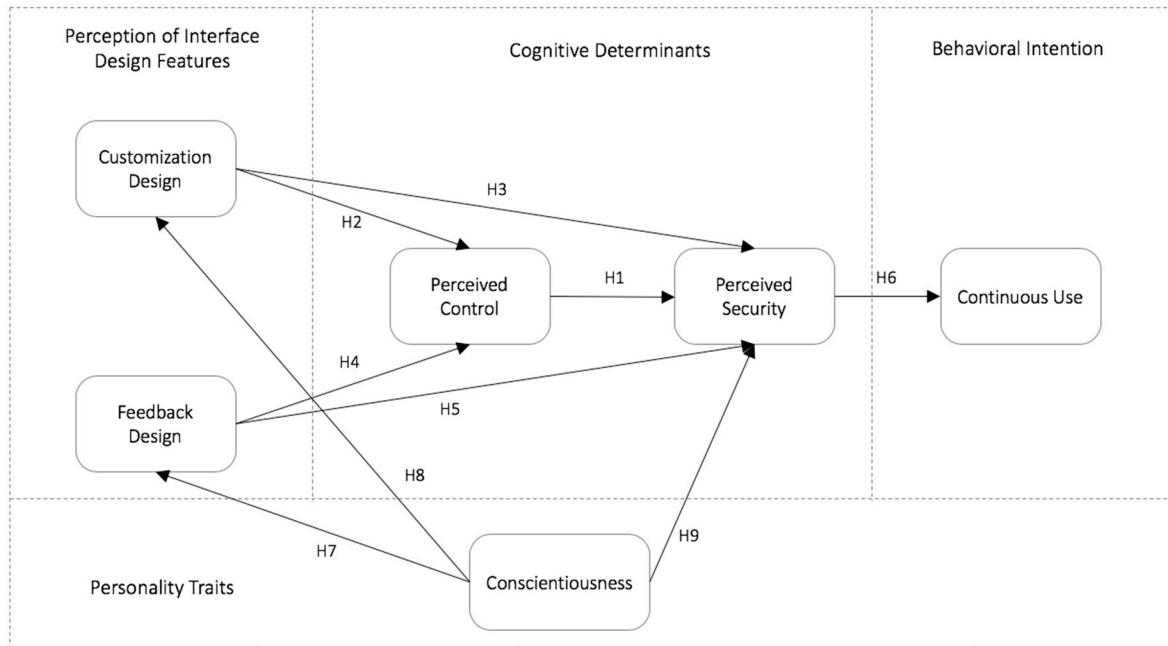
Figure 1. Research model.

3. Methodology

3.1. Instrument Development

An empirical study involving an online survey was conducted to collect data to test the research model. The survey began with two questions about participants' demographic information (age, gender) and three questions about their experience with and usage of mobile payment services (frequency of use, years of use, rank of commonly used platforms). Then, participants' conscientiousness (C) and attitudes (perception of customization design, perception of feedback design, perceived control, perceived security, and continuous use) were measured using a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). In addition, since it was possible that participants use several mobile payment platforms, they were required to respond to the items regarding perception of customization design (CD), perception of feedback design (FD), perceived control (PC), perceived security (PS), and continuous use (CU), which concerned the most commonly used platform.

The measurement items (C, CD, FD, PC, PS, and CU) and scale were adapted from previous studies. All constructs were measured with two or three items (see Table 1). The six items relating to the perception of customization and feedback design were based on the interface functions of mobile payment services and definitions identified by previous studies [5,38,42]. Items regarding the perception of customization design asked participants about their payment, privacy, and security settings, while the items regarding the perception of feedback design reflected the internal state of the system and cues for correct actions. Perceived control was measured with three items adapted from Safa et al. [60] and Hajli and Lin [31] to reflect participants' perceived control and ability to control security. Additionally, the three items concerning perceived security, which covered financial and personal information security in mobile payment transactions, were adapted from Khalilzadeh, Ozturk, and Bilgihan [9]. Two items regarding continuous use were adapted from Kim, Tao, Shin, and Kim [61] to reflect users' intention to continuously adopt services. Two items regarding conscientiousness were selected from the Mini-IPIP scales, "a 20-item short form of the 50-item International Personality Item Pool", to examine personality traits [57]. Since the online survey was conducted in China, English items were translated into Chinese and examined by translation experts. Then, we invited 10 mobile payment users to test with the questionnaire. Based on their feedback, we modified the content and deleted items. The construct and final items used in this survey are listed in Table 1.

Table 1. Constructs and measurement items.

Construct	Definition	Measure Item	Reference
Perception of customization design (CD)	Customization design refers to a system's capability that allows users to tailor it according to their needs. It usually involves customizing the information function, payment methods, and security settings in mobile payment system [5,38].	CD1: I feel that I can customize the payment methods according to my own preference. CD2: I feel that I can customize the privacy settings according to my own preference. CD3: I feel that I can customize the security settings according to my own preference.	[5]
Perception of feedback design (FD)	Feedback design describes different forms of communication from the system to a user. The information feedback should allow related information to security and the internal state of the system [42]. Regarding the Security HCI proposed by Johnston, Eloff, and Labuschagne [62], feedback design should include suggestions of secure action for problems and connections to additional information or external assistance.	FD1: I feel that the feedback information helps me to settle a payment transaction securely. FD2: I feel that the feedback information provides me with information about the account changes in my mobile payment platforms. FD3: I feel that the feedback information allows me the consequences of each performance in my mobile payment platform.	[42,62]
Perceived control (PC)	Perceived control is referred to the extent that people believe the event or situation is under their control [31]. It was studied as one of the cognitive determinants of perceived security in IT appliances [16].	PC1: I think I have the skill to keep my privacy in mobile payment platforms securely. PC2: I think that I am in control over the data securely in mobile payment platforms. PC3: I think that I am capable of preventing security risk in mobile payment platforms.	[31,60]
Perceived security (PS)	Adapting from literature [7,15], perceived security is defined as the degree to which the mobile payment user believes that transaction on mobile payment platforms is secure in both financial and personal information aspects.	PS1: I perceive secure using my credit/debit card information through mobile payment platforms. PS2:I would feel safe providing sensitive information about myself over the mobile payment platforms. PS3:I perceive that mobile payment platforms are secure systems to conduct a transaction.	[9]
Continuous use (CU)	Continuous use reflects users' intention to continuously use mobile payment services. It is one of the important post-adoption behaviors in IS use [28].	CU1: I frequently use my mobile payment platform. CU2: I will continue to use my mobile payment platform.	[28,61]
Conscientiousness (C)	Conscientiousness describes the extent to which a person is reliable, responsible, and expresses careful consideration [55–58]. People with a high score of conscientiousness tend to have higher level of self-control and they tend to make a plan and stick to it [58,59].	C1: I often forget to put things back in their proper place. C2: I make a mess of things.	[55–57]

3.2. Data Collection

Participants were required to be above 18 years old and have experience with mobile payment services. To approach the target users, questionnaires were distributed through Wenjuanxing, an online survey panel with a generalized population of users. To avoid confusion between experiences with multiple mobile payment methods, participants were required to respond to the questions regarding CD, FD, PC, PS, and CU based on their experience with the most commonly used platform. A small reward was transferred to participants' mobile payment accounts via Wenjuanxing for their participation. In order to improve data quality, we designed an attention filter to identify careless respondents [63]. This question asked participants to click on only designated items. If they did not do so, their responses were considered invalid and they did not receive the reward.

Data collection began in February 2019 and took four weeks to complete. In total, 477 responses were collected. After deleting disqualified and careless responses examined by the attention filter, 252 valid responses were used for data analysis.

3.3. Participants

Of the 252 valid participants, 42.9% were male and 57.1% were female. Around half (43.3%) were 18–29 years of age, 37.3% were 30–39 years of age, 13.4% were 40–49 years of age, and 9% were 50 years of age or above. The age distribution of the participating mobile payment users is similar to that reported by the Payment and Clearing Association of China in 2018. The majority of respondents used mobile payment methods daily (72.8%), and most of them (69%) used mobile payment services in the past three years. Most of the participants (99%) most commonly used Alipay or WeChat Pay (see Figure 2).
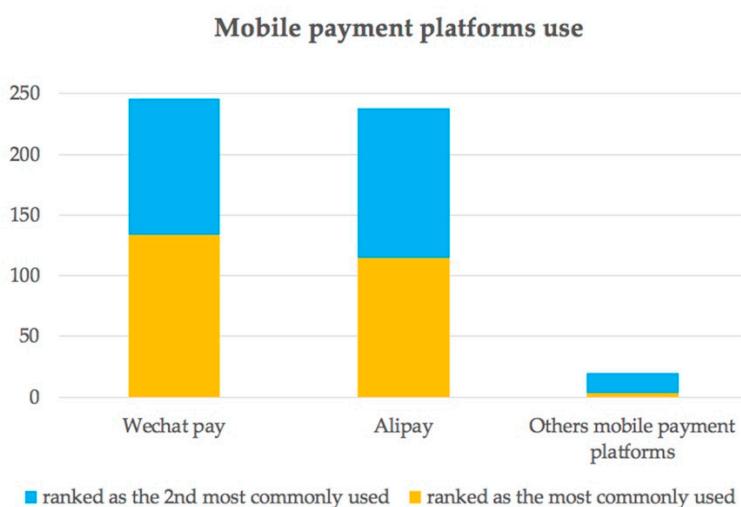

Figure 2. The first and the second most commonly used mobile payment platforms ranked by participants.

4. Results

4.1. Reliability and Validity

The composite reliability (CR) of all constructs was examined to determine whether it is above the suggested value of 0.7 [64]. The convergent validity of all constructs was evaluated based on the average variance extracted (AVE) and factor loadings, the recommended values of which are above 0.5 [65]. Table 2 summarizes the reliability and validity results. All the values of composite reliability exceed the recommended threshold of 0.70, suggesting good reliability and internal consistency for all constructs. The minimum standardized factor loading is 0.6 and most of the standardized factor

loading values are greater than 0.7. The AVE values for all six constructs are above the reference threshold of 0.5, indicating adequate convergent validity for all constructs.

Table 2. Reliability and unidimensionality.

Construct	Cronbach's Alpha	Variable	Standardized Factor Loading	CR (t-value)	SMC	AVE	Composite Reliability
CD	0.795	cd1	0.637		0.406	0.578	0.802
		cd2	0.814	9.934	0.663		
		cd3	0.816	9.839	0.666		
FD	0.803	fd1	0.803		0.645	0.586	0.809
		fd2	0.700	10.713	0.490		
		fd3	0.789	11.569	0.623		
PC	0.853	pc1	0.801		0.642	0.661	0.854
		pc2	0.800	12.969	0.640		
		pc3	0.838	13.476	0.702		
PS	0.805	ps1	0.820		0.672	0.593	0.813
		ps2	0.766	11.524	0.587		
		ps3	0.720	10.959	0.518		
CU	0.744	cu1	0.670		0.449	0.615	0.758
		cu2	0.884	5.217	0.781		
C	0.657	con1	0.617		0.381	0.578	0.727
		con2	0.881	4.664	0.776		

Note: *SMC refers to Square multiple Correlation.

Discriminant validity was determined by examining whether the square root of the AVE of each construct surpasses the related coefficients of the constructs [65]. Table 3 shows that all the square roots are larger than the coefficients, indicating good discriminant validity.

Table 3. Correlation matrix of the measurements.

Measurement	AVE	CD	FD	PC	PS	C	CU
CD	0.578	(0.760)					
FD	0.586	0.596 ***	(0.765)				
PC	0.661	0.614 ***	0.489 ***	(0.812)			
PS	0.593	0.299 ***	0.432 ***	0.501 ***	(0.771)		
C	0.578	0.338 ***	0.334 ***	0.230 **	0.352 ***	(0.755)	
CU	0.615	0.206 *	0.280 **	0.201 *	0.432 ***	0.336 **	(0.782)

Note: * $p < 0.1$; ** $p < 0.05$; *** $p < 0.01$; square root of AVEs are on diagonal.

4.2. Model Fit

Model fit was evaluated by confirmatory factor analysis and model fit indexes, namely Chi-square, df, Chi-square/df, Goodness-of-Fit Index (GFI), Adjusted Goodness-of-Fit Index (AGFI), the Root Mean Square Residual (SRMR), the Root Mean Square Error of Approximation (RMSEA), Normed-Fit Index (NFI), Incremental-Fit Index (IFI), Tucker-Lewis Index (TLI), and Comparative-Fit Index (CFI). The results show that the collected data fits the proposed model (chi-square = 159.081, df = 93, chi-square/df = 1.711, GFI = 0.927, AGFI = 0.893, SRMR=0.033, RMSEA = 0.053, NFI = 0.908, IFI = 0.960, TLI = 0.947, and CFI = 0.959). All of the values are within the recommended thresholds (see Table 4). Thus, the research model fits well with the collected data.

Table 4. Model fitness indexes.

Category	Measure	Acceptable Values [64,66]	Value
Absolute fit indices	Chi-square		159.081
	df		93
	Chi-square/df	1–5	1.711
	GFI	0.90 or above	0.927
	AGFI	0.80 or above	0.893
	SRMR	0.08 or below	0.033
	RMSEA	0.05–0.08	0.053
Incremental fit indices	NFI	0.90 or above	0.908
	IFI	0.90 or above	0.960
	TLI	0.90 or above	0.947
	CFI	0.90 or above	0.959

4.3. Hypothesis Testing and Path Analysis

The path analysis results for the relationships among conscientiousness, perception of interface design features, perceived control, perceived security, and continuous use are illustrated in Table 5. The perception of interface design features can significantly influence perceived control and perceived security. Customization and feedback design are positively associated with perceived control ($\beta = 0.501$, $p < 0.001$; $\beta = 0.19$, $p < 0.05$). Thus, H2 and H4 were supported. While customization design did not have a direct impact on perceived security ($\beta = -0.206$, $p > 0.05$), feedback design had an impact on perceived security ($\beta = 0.265$, $p < 0.01$). Therefore, H3 was rejected and H5 was supported. The results also revealed significant effects for perceived control, perceived security, and continuous use; perceived control affected perceived security ($\beta = 0.440$, $p < 0.001$) and perceived security influences continuous use intention ($\beta = 0.442$, $p < 0.01$), supporting H1 and H6. There were three significant hypothesis paths from conscientiousness to the perception of interface design features and perceived security: conscientiousness was found to have a positive effect on the perception of feedback design ($\beta = 0.336$, $p < 0.001$) and customization design ($\beta = 0.340$, $p < 0.001$) as well as on perceived security ($\beta = 0.249$, $p < 0.01$). Thus, H7, H8, and H9 were confirmed. Figure 3 shows the results of the proposed research model.

Table 5. Hypotheses testing.

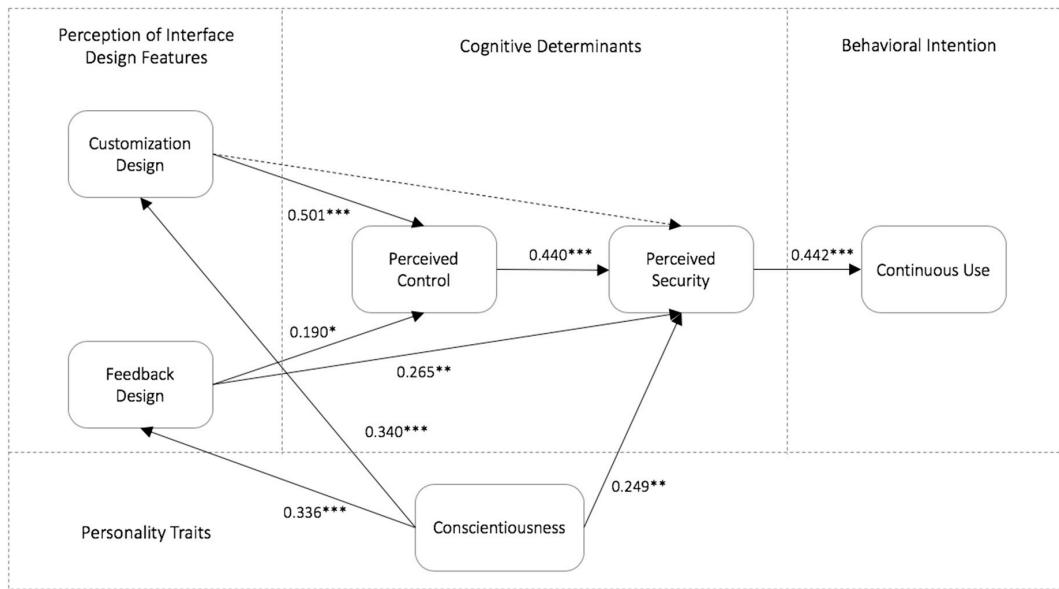| Hypothesis	Path	Standardized Coefficient	Standard Error	CR (t-Value)	*p*	Result
H1	Perceived Control > Perceived Security	0.440	0.077	4.577	0.001	Supported
H2	Customization Design > Perceived Control	0.501	0.149	5.034	0.001	Supported
H3	Customization Design > Perceived Security	−0.206	0.134	−1.843	0.065	Rejected
H4	Feedback Design > Perceived Control	0.190	0.117	2.127	0.033	Supported
H5	Feedback Design > Perceived Security	0.265	0.102	2.710	0.007	Supported
H6	Perceived Security > Continuous Use	0.442	0.067	3.129	0.002	Supported
H7	Conscientiousness > Feedback Design	0.336	0.082	4.023	0.001	Supported
H8	Conscientiousness > Customization Design	0.340	0.073	3.962	0.001	Supported
H9	Conscientiousness > Perceived Security	0.249	0.081	3.129	0.002	Supported

Figure 3. Results of the research model (Note: *$p < 0.05$, **$p < 0.01$, ***$p < 0.005$).

5. Discussion and Implications

The goals of this study were to develop a theoretical model to describe the structural relationships among the perception of interface design features, perceived control, perceived security, and conscientiousness and to explain the influence of perceived security on continuous use of mobile payment services. For this purpose, empirical data was collected to test the proposed model. Most of the hypotheses proposed in this study were supported. The evidence shows that perceived security is influenced by the perception of interface design features, perceived control, and conscientiousness and that there are interrelationships among these three dimensions. The results also reveal that perceived security is a strong predictor of continuous use of mobile payment.

Unlike previous studies, which proposed an indirect relationship between perceived security and continuous use [23], this research found that perceived security had a strong direct impact on continuous use. The strong standardized coefficient between perceived security and continuous intention ($\beta = 0.442$, $p < 0.01$) implied that perceived security plays an important role in users' decision regarding long-term use of mobile payment platforms. Thus, mobile payment service providers should consider financial and personal information security in order to retain users. However, current providers tend to enhance convenience while ignoring security. For example, currently, Alipay automatically logs in users' accounts without authentication. This could lead to complaints by users who are concerned about security. Since perceived security is crucial to the success of mobile payment services, we suggest that service providers should make a different tradeoff between security and convenience.

The results of this study support prior research on the effect of perceived control on perceived security in general information technology use [11,60]. The findings of this study reveal that perceived control is a vital factor affecting perceived security in mobile payment services. Feelings of control cause users to believe that they have the ability to manipulate the transaction process and achieve their expected outcome [41], thus enhancing the perceived security of the transaction.

This study also reveals practical ways to improve perceived control and perceived security through interface design features. The perception of customization design was proposed to have an effect on both perceived control and perceived security, and the results show that the influence of the perception of customization design on perceived security is fully mediated by perceived control ($\beta = 0.501$, $p < 0.005$). In addition, the strong impact of the perception of customization design on perceived control indicated that it plays a significant role in enhancing perceived security. Thus, one

can improve perceived security by improving users' perceived control. For example, when users can modify their payment methods and security privacy settings on a mobile payment platform, they are likely to feel that the transaction process is under their control and thus that there is a higher level of perceived security. Existing studies in other fields have also found a relationship between customization design and perceived control [39,40]. The perception of feedback design significantly influenced both perceived control and perceived security in this study. Interaction and communication between users and a system are vital parts of m-commerce [67]. Although a few studies have mentioned the influence of feedback design on perceived control, evidence suggests that information cues could enhance users' information control [32]. With the feedback provided by the system, users can gain a clear understanding of the status of payments and be capable of manipulating the transaction process. This study also found that the perception of feedback design has a strong impact on perceived security. Feedback design are recommended by the HCI-S (Human-Computer Interaction for Security) criteria, which is a human-computer interaction guideline applied in the computer security aspect. This criterion helps users determine the status of a system [62]. In mobile payment services, feedback design could include security warnings, notifications, and interaction cues. For instance, Alipay provides security warnings to users when they transfer money to a private account. Also, most mobile payment platforms provide users an electronic receipt with the transaction status. Overall, this study confirmed that feedback design affects perceived security.

The effect of the perception of customization design on perceived security is fully mediated by perceived control, while the effect of perception of feedback on perceived security is only partially explained by perceived control. The impact of perception of customization design on perceived control is much stronger than that of feedback design, perhaps because customization design allows users to take an initiative and manipulate a situation while feedback is usually passively received. Users perceive a stronger feeling of control if they feel self-motivated to engage in specific behaviors. The perception of feedback design can directly affect perceived security, while the perception of customization design can influence perceived security through perceived control. The distinct effects of the perception of customization and feedback design on perceived control and security imply that mobile payment services can use different interface design strategies. First, because the interaction between users and mobile devices could be constrained by the visual display, different interface design features could be applied based on the size of the display of mobile devices [67]. Currently, people can use mobile payment services with mobile devices of various sizes, such as tablet PCs, smartphones, and smart watches. In order to enhance perceived security, for example, feedback design would be more appropriate for smaller screens because users may become frustrated by customization features on a small screen. For medium and larger screens, such as those associated with smartphones and tablet PCs, both customization and feedback design could be combined to have a powerful effect on perceived security. Since customization design have a much stronger impact on perceived control than feedback design, we suggest prioritizing customization over feedback when users feel a loss of perceived control.

Lastly, the results reveal that conscientiousness has a significant impact on the perception of both customization and feedback design and confirm the positive relationships between conscientiousness and perceived security in the context of mobile payments. Users with high conscientiousness scores tend to have more positive attitudes toward interface design features, suggesting that they rely more on these features to enhance the perceived security of mobile payment services. For example, they might prefer to modify mobile payment settings according to their needs and situation, and they might like to carefully check feedback information while making a payment. Mobile services are more personalized, since users can modify mobile functions based on their needs. Service providers and designers could take account the personality traits of conscientious people when designing mobile payment services. In other words, people with various levels of conscientiousness could be offered interfaces with different functionalities. For instance, people with a high level of conscientiousness could be recommended an advanced customization and feedback interface to meet their needs, while people with a low level of conscientiousness could be offered a basic customization and feedback

interface to improve convenience. Previous research revealed that conscientiousness has a positive influence on security behaviors [53,54] and this research confirmed that conscientious people are associated with a high level of perceived security. This might be because conscientious people tend to engage in more security behaviors when offered opportunities for customization and feedback, which make them feel that the mobile payment platform is more secure.

6. Limitations and Future Studies

This study presents a theoretical model to explore the factors that influence perceived security, the perception of interface design features, perceived control, and personality traits. This study also explains the effect of perceived security on continuous use intention regarding mobile payment services. Nonetheless, this study has several limitations. First, it focused only on mobile payment users in China, in which mobile payment services are prevalent. However, the findings are applicable to other markets with a similar context (i.e., those in which well-developed mobile payment platforms are commonly used). Since security is a widespread concern among mobile payment users [7–14,68], the results of this study might also help promote mobile payment services in developing mobile payment markets by providing design directions to service providers. Despite this, we suggest that further validation be performed before the results are applied to other mobile payment markets. Second, this study did not explore the possible impact of perceived control on user behaviors. As we found that the perception of customization design is a strong motivator of perceived control, future research could further explore the effect of perceived control on mobile payment use. Third, our model did not consider the functional differences between mobile payment platforms and the influences of external factors (such as the reputation of the platform, popularity of the service, service quality) on perceived security. This is because we found that most of our participants (99%) used common mobile payment platforms (see Figure 2), which have similar interface functions, reputation, popularity and quality. However, if the mobile payment platforms used by participants in other studies have distinct interface features (as is the case for platforms such as Apple Pay and Alipay), it is necessary to examine the effects of the perception of interface design features on perceived security in different mobile payment platforms. Moreover, future studies could extend this research by collecting and comparing users' attitudes toward mobile payment platforms with distinct interface functions and design features. Finally, we did not account for differences in usage experience (e.g., the number of years of use, frequency of use). This can be studied in detail in the future.

7. Conclusions

Sustainable use of mobile payment services is very important for promoting m-commerce. Expanding upon the limited theoretical evidence provided by previous studies, this study proposed that perceived security is a predictor of continuous use of technology. We conducted an empirical study to explore the determining factors of perceived security from the perspectives of customization design and feedback design, perceived control and conscientiousness, and revealed the strong relationship between perceived security and continuous use. This study provides a basis for further research on the influence of perceived security on users' behavioral intentions regarding long-term use. Future studies could extend this research model by exploring the effect of perceived security on other post-adoption behaviors, such as switching behaviors, advanced use, and recommended intention. The constructed theoretical model also provides a holistic picture of the factors that influence perceived security. The interpretation of this model offers design implications for service providers and designers.

Author Contributions: Conceptualization, J.Z.; Methodology, J.Z. and Y.L.; Data curation, J.Z. and Y.S.; Writing, J.Z. and Y.L.; Supervision, Y.L.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zhou, T. An empirical examination of continuance intention of mobile payment services. *Decis. Support Syst.* **2013**, *54*, 1085–1091. [CrossRef]
2. Yang, S.; Lu, Y.; Gupta, S.; Cao, Y. Does Context Matter? The Impact of Use Context on Mobile Internet Adoption Does Context Matter? The Impact of Use Context on Mobile Internet Adoption. *J. Hum. Comput. Interact.* **2012**, *28*, 530–541. [CrossRef]
3. Johnson, V.L.; Kiser, A.; Washington, R.; Torres, R. Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. *Comput. Hum. Behav.* **2018**, *79*, 111–122. [CrossRef]
4. Lin, X.; Wu, R.; Lim, Y.T.; Han, J.; Chen, S.C. Understanding the Sustainable Usage Intention of Mobile Payment Technology in Korea: Cross-Countries Comparison of Chinese and Korean Users. *Sustainability* **2019**, *11*, 5532. [CrossRef]
5. Shao, Z.; Zhang, L.; Li, X.; Guo, Y. Antecedents of trust and continuance intention in mobile payment platforms: The moderating effect of gender. *Electron. Commer. Res. Appl.* **2019**, *33*, 100823. [CrossRef]
6. 2019 China Mobile Payment Development Report. Payment & Clearing Association of China, 2018. Available online: http://www.pcac.org.cn/index.php/focus/list_details/ids/654/id/50/topicid/3.html. (accessed on 21 September 2019).
7. Hartono, E.; Holsapple, C.W.; Kim, K.Y.; Na, K.S.; Simpson, J.T. Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. *Decis. Support Syst.* **2014**, *62*, 11–21. [CrossRef]
8. Dahlberg, T.; Guo, J.; Ondrus, J. A critical review of mobile payment research. *Electron. Commer. Res. Appl.* **2015**, *14*, 265–284. [CrossRef]
9. Khalilzadeh, J.; Ozturk, A.B.; Bilgihan, A. Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. *Comput. Hum. Behav.* **2017**, *70*, 460–474. [CrossRef]
10. Schierz, P.G.; Schilke, O.; Wirtz, B.W. Understanding consumer acceptance of mobile payment services: An empirical analysis. *Electron. Commer. Res. Appl.* **2010**, *9*, 209–216. [CrossRef]
11. Huang, D.-L.; Rau, P.L.P.; Salvendy, G. Perception of information security. *Behav. Inf. Technol.* **2010**, *29*, 221–232. [CrossRef]
12. Shin, D.H. Towards an understanding of the consumer acceptance of mobile wallet. *Comput. Hum. Behav.* **2009**, *25*, 1343–1354. [CrossRef]
13. Fan, J.; Shao, M.; Li, Y.; Huang, X. Understanding users' attitude toward mobile payment use: A comparative study between China and the USA. *Ind. Manag. Data Syst.* **2018**, *118*, 524–540. [CrossRef]
14. Oliveira, T.; Thomas, M.; Baptista, G.; Campos, F. Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Comput. Hum. Behav.* **2016**, *61*, 404–414. [CrossRef]
15. Salisbury, W.D.; Pearson, R.A.; Pearson, A.W.; Miller, D.W. Perceived security and World Wide Web purchase intention. *Ind. Manag. Data Syst.* **2001**, *101*, 165–177. [CrossRef]
16. Huang, D.L.; Rau, P.L.P.; Salvendy, G.; Gao, F.; Zhou, J. Factors affecting perception of information security and their impacts on IT adoption and security practices. *Int. J. Hum. Comput. Stud.* **2011**, *69*, 870–883. [CrossRef]
17. Chang, H.H.; Chen, S.W. Consumer perception of interface quality security, and loyalty in electronic commerce. *Inf. Manag.* **2009**, *46*, 411–417. [CrossRef]
18. Meskaran, F.; Ismail, Z.; Shanmugam, B. Online Purchase Intention: Effects of Trust and Security Perception. *Aust. J. Basic Appl. Sci.* **2013**, *7*, 307–315.
19. Uffen, J.; Kaemmerer, N.; Breitner, M.H. Personality Traits and Cognitive Determinants-An Empirical Investigation of the Use of Smartphone Security Measures. *J. Inf. Secur.* **2013**, *4*, 203–212. [CrossRef]
20. Yuan, S.; Liu, Y.; Yao, R.; Liu, J. An investigation of users' continuance intention towards mobile banking in China. *Inf. Dev.* **2016**, *32*, 20–34. [CrossRef]
21. Zhou, T. Examining continuance usage of mobile Internet services from the perspective of resistance to change. *Inf. Dev.* **2014**, *30*, 22–31. [CrossRef]

22. Kim, C.; Mirusmonov, M.; Lee, I. An empirical examination of factors influencing the intention to use mobile payment. *Comput. Hum. Behav.* **2010**, *26*, 310–322. [CrossRef]

23. Gao, L.; Waechter, K.A.; Bai, X. Understanding consumers' continuance intention towards mobile purchase: A theoretical framework and empirical study-A case of China. *Comput. Hum. Behav.* **2015**, *53*, 249–262. [CrossRef]

24. Gao, L.; Waechter, K.A. Examining the role of initial trust in user adoption of mobile payment services: An empirical investigation. *Inf. Syst. Front.* **2017**, *19*, 525–548. [CrossRef]

25. Su, P.; Wang, L.; Yan, J. How users' Internet experience affects the adoption of mobile payment: A mediation model. *Technol. Anal. Strateg. Manag.* **2018**, *30*, 186–197. [CrossRef]

26. Yang, S.; Lu, Y.; Gupta, S.; Cao, Y.; Zhang, R. Mobile payment services adoption across time: An empirical study of the effects of behavioral beliefs, social influences, and personal traits. *Comput. Hum. Behav.* **2012**, *28*, 129–142. [CrossRef]

27. Lu, J.; Wei, J.; Yu, C.S.; Liu, C. How do post-usage factors and espoused cultural values impact mobile payment continuation? *Behav. Inf. Technol.* **2017**, *36*, 140–164. [CrossRef]

28. Zhou, T. An empirical examination of users' post-adoption behaviour of mobile services. *Behav. Inf. Technol.* **2011**, *30*, 241–250. [CrossRef]

29. Chellappa, R.K.; Pavlou, P.A. Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logist. Inf. Manag.* **2002**, *15*, 358–368. [CrossRef]

30. Burger, J.M. Negative Reactions to Increases in Perceived Personal Control. *J. Pers. Soc. Psychol.* **1989**, *56*, 246–256. [CrossRef]

31. Hajli, N.; Lin, X. Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *J. Bus. Ethics* **2016**, *133*, 111–123. [CrossRef]

32. Arcand, M.; Nantel, J.; Arles-Dufour, M.; Vincent, A. The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Inf. Rev.* **2007**, *31*, 661–681. [CrossRef]

33. Zhang, J.; Reithel, B.J.; Li, H. Impact of perceived technical protection on security behaviors. *Inf. Manag. Comput. Secur.* **2009**, *17*, 330–340. [CrossRef]

34. Suh, B.; Han, I. The impact of customer trust and perception of security control on the acceptance of electronic commerce. *Int. J. Electron. Commer.* **2003**, *7*, 135–161.

35. Ingaldi, M.; Ulewicz, R. How to Make E-Commerce More Successful by Use of Kano's Model to Assess Customer Satisfaction in Terms of Sustainable Development. *Sustainability.* **2019**, *18*, 4830. [CrossRef]

36. Tarasewich, P. *Designing Mobile Commerce Applications*; Communications of the ACM: New York, NY, USA, 2003; Volume 46, pp. 57–60.

37. Lee, Y.E.; Benbasat, I. A Framework for the Study of Customer Interface Design for Mobile Commerce. *Int. J. Electron. Commer.* **2004**, *8*, 79–102. [CrossRef]

38. Nilashi, M.; Ibrahim, O.; Mirabi, V.R.; Ebrahimi, L.; Zare, M. The role of Security, Design and Content factors on customer trust in mobile commerce. *J. Retail. Consum. Serv.* **2015**, *26*, 57–69. [CrossRef]

39. Kim, K.; Schmierbach, M.G.; Chung, M.Y.; Fraustino, J.D.; Dardis, F. Is it a sense of autonomy, control, or attachment? Exploring the effects of in-game customization on game enjoyment. *Comput. Hum. Behav.* **2015**, *48*, 695–705. [CrossRef]

40. Marathe, S.; Sundar, S.S. What drives customization? Control or Identity? In Proceedings of the 2011 annual conference on Human factors in computing systems-CHI, Vancouver, BC, Canada, 13 June 2011; pp. 781–790.

41. Huang, L.; Ba, S.; Lu, X. Building Online Trust in a Culture of Confucianism. *ACM Trans. Manag. Inf. Syst.* **2014**, *5*, 4. [CrossRef]

42. Muñoz-Arteaga, J.; González, R.M.; Martin, M.V.; Vanderdonckt, J.; Álvarez-Rodríguez, F. A methodology for designing information security feedback based on User Interface Patterns. *Adv. Eng. Softw.* **2009**, *40*, 1231–1241. [CrossRef]

43. Bauer, S.; Bernroider, E.W.N.; Chudzikowski, K. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Comput. Secur.* **2017**, *68*, 145–159. [CrossRef]

44. Walter, N.; Ortbach, K.; Niehaves, B. Designing electronic feedback-Analyzing the effects of social presence on perceived feedback usefulness. *Int. J. Hum. Comput. Stud.* **2015**, *76*, 1–11. [CrossRef]

45. Povey, R.; Conner, M.; Sparks, P.; James, R.; Shepherd, R. Application of the Theory of Planned Behaviour to two dietary behaviours: Roles of perceived control and self-efficacy. *Br. J. Health Psychol.* **2000**, *2*, 121–139. [CrossRef]

46. Chun, S.H. E-commerce liability and security breaches in mobile payment for e-business sustainability. *Sustainability* **2019**, *11*, 715. [CrossRef]

47. Liao, C.; Chen, J.L.; Yen, D.C. Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: An integrated model. *Comput. Hum. Behav.* **2007**, *23*, 2804–2822. [CrossRef]

48. Ye, C.; Seo, D.; Desouza, K.C.; Sangareddy, S.P.; Jha, S. The Role of Innovation and Wealth in the Net Neutrality Debate. *J. Am. Soc. Inf. Sci. Technol.* **2008**, *59*, 2115–2132. [CrossRef]

49. Nicholson, N.; Soane, E.; Fenton-O'Creevy, M.; Willman, P. Personality and domain-specific risk taking. *J. Risk Res.* **2005**, *8*, 157–176. [CrossRef]

50. Mcelroy, J.C.; Hendrickson, A.R.; Townsend, A.M.; Demarie, S.M. Dispositional factors in Internet use: Personality versus cognitive style. *MIS Q.* **2007**, *31*, 809–820. [CrossRef]

51. John, O.P.; Srivastava, S. *Handbook of Personality: Theory and Research*, 2nd ed.; Guilford: New York, NY, USA, 1999.

52. Junglas, I.A.; Johnson, N.A.; Spitzmüller, C. Personality traits and concern for privacy: An empirical study in the context of location-based services. *Eur. J. Inf. Syst.* **2008**, *17*, 387–402. [CrossRef]

53. Shropshire, J.; Warkentin, M.; Sharma, S. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Comput. Secur.* **2015**, *49*, 177–191. [CrossRef]

54. McCormac, A.; Zwaans, T.; Parsons, K.; Calic, D.; Butavicius, M.; Pattinson, M. Individual differences and Information Security Awareness. *Comput. Hum. Behav.* **2017**, *69*, 151–156. [CrossRef]

55. Goldberg, L.R. A broad-bandwidth, public-domain, personality inventory measuring the lower-level facets of several five-factor models. *Personal. Psychol. Eur.* **1999**, *7*, 7–28. Available online: https://ipip.ori.org/A%20broad-bandwidth%20inventory.pdf (accessed on 21 November 2019).

56. Goldberg, L.R.; Johnson, J.A.; Eber, H.W.; Hogan, R.; Ashton, M.C.; Cloninger, C.R.; Gough, H.G. The international personality item pool and the future of public-domain personality measures. *J. Res. Pers.* **2006**, *40*, 84–96. [CrossRef]

57. Donnellan, M.B.; Oswald, F.L.; Baird, B.M.; Lucas, R.E. The Mini-IPIP scales: Tiny-yet-effective measures of the Big Five factors of personality. *Psychol. Assess.* **2006**, *18*, 192–203. [CrossRef] [PubMed]

58. Zhou, T.; Lu, Y. The effects of personality traits on user acceptance of mobile commerce. *Int. J. Hum. Comput. Interact.* **2011**, *27*, 545–561. [CrossRef]

59. Halevi, T.; Lewis, J.; Memon, N. A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits. In Proceedings of the International Conference on World Wide Web, New York, NY, USA, 13–17 May 2013; pp. 737–744.

60. Safa, N.S.; Sookhak, M.; von Solms, R.; Furnell, S.; Ghani, N.A.; Herawan, T. Information security conscious care behaviour formation in organizations. *Comput. Secur.* **2015**, *53*, 65–78. [CrossRef]

61. Kim, C.; Tao, W.; Shin, N.; Kim, K.S. An empirical study of customers' perceptions of security and trust in e-payment systems. *Electron. Commer. Res. Appl.* **2010**, *9*, 84–95. [CrossRef]

62. Johnston, J.; Eloff, J.H.P.; Labuschagne, L. Security and human computer interfaces. *Comput. Secur.* **2003**, *22*, 675–684. [CrossRef]

63. Meade, A.W.; Craig, S.B. Identifying careless responses in survey data. *Psychol. Methods* **2012**, *17*, 437–455. [CrossRef]

64. Hair, J.F.; Black, W.C.; Babin, B.J.; Anderson, R.E. *Multivariate Data Analysis*; Pearson: Essex, UK, 2014.

65. Fornell, C.; Larcker, D.F. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]

66. Bagozzi, R.P.; Yi, Y. On the evaluation of structural equation models. *J. Acad. Mark. Sci.* **1988**, *16*, 74–94. [CrossRef]

67. Lee, Y.E.; Benbasat, I. Interface design for mobile commerce. *Commun. ACM* **2003**, *12*, 48–52. [CrossRef]

68. Huh, J.H.; Verma, S.; Sri, S.; Rayala, V.; Bobba, R.; Beznosov, K.; Kim, H. I Don't Use Apple Pay Because It's Less Secure Perception of Security and Usability in Mobile Tap-and-Pay. In Proceedings of the 2017 Workshop on Usable Security, San Diego, CA, USA, 26 February 2017.