Users' Information Security Perception Impact on Consumers' Continuous Purchase Intention in O2O Food and Beverage Takeaway Platforms

Yue Huang[*]Chanchai Bunchapattanasakda[**]

Boonyaporn Boonmek[***]Porntiwa Bunchapattanasakda[****]

Graduate School, Stamford International University, Thailand*

Email: 7079728@qq.com

Dean, Graduate School, Stamford International University, Thailand**

Executive Vice Chairperson and Director, YLG Bullion & Futures Public Company Limited, Thailand***

VP, Maybank Securities (Thailand) Public Company Limited****

Abstract

This study investigated the impact of user information security perception on consumers' continuous purchase intention in O2O food and beverage takeaway platforms. The study employed quantitative research using a structured-online questionnaires to collect data from 439 Chinese users who has an online buying experience in O2O food and beverage takeaway platforms in Kunming city, China, through the convenience sampling approach. This study proposed a theoretical model of the influencing factors of user's continuous purchase intention. The results from Structural Equation Model (SEM) analysis found that users' information security perception (perceived perception and controllable perception) has a positive impact on continuous purchase intentions. Besides, this research verified user trust (both cognitive trust and affective trust) is positively influenced by perceived perception, understood perception and controllable perception. Furthermore, we determined that consumers' continuous purchase intention is influenced by two dimensions of trust including both cognitive trust and affective trust. Finally, trust as a mediating variable was confirmed to play a partial mediating role in the relationship between information security perception and continuous purchase intention. The findings can further drive consumers' online purchasing behavior and provide a reference for operating companies to create an internet catering platform with mobile and interactive features.

Keywords: China, continuous purchase intention, information security perception, O2O food and beverage takeaway platform, trust

1. Introduction

The rapid development of Online to Offline (O2O) catering has led to more businesses entering and more consumers using the takeaway platforms. Behind the expansion of the takeaway platform, the security environment of the platform has become more complex due to the rich functionality and wide range of applications. According to the survey, internet security issues have been encountered for half of internet users, with the proportion of issues related to personal information leakage reaching as high as 24% in between, and problems such as online fraud, account theft and Trojan horse programs are also emerging (Cybersecurity Ventures Sponsored by Herjavec Group, 2017). At least one-third of the software in the mobile APP download ranking has

the problem of over-authorizing user information, and it is also common to collect information beyond the scope, collecting almost 20 or more items of users' private data. Some APPs also show unusual behaviors such as trying to probe other applications, read stored files and corrupt system programs (Cyberspace Administration of China, 2019), which not only affects the security of internet users' information and property but also hinders their willingness to continue using information systems. This information was accessed by political data companies, which used it to deliver targeted advertising to users for the purpose of engaging in politics. This incident triggered a global uninstallation of Facebook. (Memorabilia, 2018). China's Code of Practice on Personal Information Security of Information Security Technology came into effect in May 2018, regulating the protection of information by enterprises and clarifying their responsibilities. It not only fills the gap in information security protection in China, but also shows that both the government and the public are now paying more and more attention to personal information security (China Youth Daily, 2018). The Internet Security Joint Laboratory established by Tencent in July 2019 aims to crack down on cybercrime, reduce information security problems and provide users with secure data protection services (Xinhuanet, 2019). Similar to other systems, the information security risk issues for users during the establishment of O2O food and beverage takeaway platforms should be a major concern. In the process of using information systems, people's perception of the security of the information system also becomes an important factor influencing users' decisions. When using a takeaway platform, users have concerns about the security of the platform and may refuse to continue using it, or they may compare security of the platforms based on their previous experience of using information systems and continue or refuse using it. Thus, the impact of user perception on purchase intentions has long been a focus of research in marketing, but there has been few academic research on the perceptions of user information security. The main objectives of this study are: (1) to investigate the perceptions of information system users regarding the security of personal information and the level of knowledge of information security threats. (2) to establish a model based on the characteristics of current O2O food delivery platforms, and to investigate the influence of the variables of information security perception on users' trust and continuous purchase intention, to explore the potential influence relationship between the variables of trust and willingness of continuous purchase, and to use quantitative methods to analyze in depth the extent of the influence of each factor and the influence mechanism. (3) to provide suggestions for O2O food and beverage takeaway platform operators to enhance users' willingness to continue to purchase and strengthen their core competitiveness.

2. Literature Review

O2O food and beverage takeaway platforms are mainly offline brick-and-mortar shops that provide consumers with convenient, discounted goods and services through their presence on online platforms, while consumers complete their transactions through unified logistics and delivery. Since 2013, the development and popularity of O2O takeaway platforms have shown a strong development trend to the public (Maimaiti, Zhao, Jia, Ru & Zhu, 2018). The development of O2O in the food service industry has not only brought stable customer traffic to businesses and a convenient lifestyle to consumers, but also more entrepreneurial opportunities in the current

"Internet+" environment (CNNIC, 2018). The platform collects, classifies and summarizes offline food service information and displays it to consumers with different needs, who can then select different merchants according to their preferences for screening, enquiry, booking and payment.

Relationships between Information Security Perception and Continuous Purchase Intention

In psychology, information security can represent a perception. is classified ~~subdivided~~ into sensation and perception. Perception is a direct sensory reflection of subjective and objective states and things, produced by people's brain (He, 2014). Information security perception is a subjective expectation that users are not sure whether their private information is collected, bought, sold, or used without authorization. Thus, users pay attention to the use of their personal information and hesitate or refusal to provide their private information. Yenisey, Ozok and Salvendy (2005) concluded that the perceived security knowledge of online shopping users would affect the generation of purchase intention. Chen (2016) indicates that perceived safety related to websites and consumers have a significant impact on the willingness to purchase tourism products online. Huang (2009) confirmed the role of information security perception in promoting users' willingness and behavior to use online purchases. Gao (2010) concluded that a high degree of perceived security would make consumers more willing to use the online system. Li and Hu (2014) combined the TAM model with information security behavior theory and tested that the higher the security factor that users are aware of, the more likely they are to accept and continue using the information system.

Huang (2009) suggested that perceived perception, understood perception and controllable perception have a positive impact on consumers' continuous purchase intention. In other words, if users can detect and deal with security threats in a timely manner, they will have a strong willingness to use the O2O catering platform; if they have a high level of awareness and understanding of possible information security risks, they will be more likely to use the platform. The higher the level of awareness and understanding of possible information security risks, the stronger the willingness to continue to use the platform; and the ability to control the security threats that occur on the platform, the stronger the vision of continued use of the platform. From the above literature reviews, this study hypothesizes the followings:

H1a: Perceived perception has a positive effect on continuous purchase intentions.

H1b: Understanding perception has a positive impact on continuous purchase intentions.

H1c: Controllable perception has a positive effect on continuous purchase intentions.

Relationships between Information Security Perception and User's Trust

Furnell and Karweni (1999) reveal that all respondents remain concerned about external attacks on the internet, which also influences their cautious attitude towards building trust in e-commerce. The authors suggest that companies can enhance user trust by securing the internal and external security of their systems. Hoffman, Novak, and Peralta (1999) reveal that 71% of website users feel that stronger laws are needed to protect the security of their private information online, and 92% of website users felt that they are willing to provide information for marketing purposes if the website collect and use the information in accordance with rules agreed with them in advance.

Lu (2006) proposed factors related to customers' perceptions of image, usage, interaction, security and environment based on the characteristics of B2C websites, and the results showed that the higher the perceived security of personal information and transaction security, the higher the initial level of trust in the website. From the perspective of privacy and security, Wei (2005) analyzed and built a model of the influence of privacy perception and security perception on credit and concluded that privacy perception and security perception have a positive influence on user trust. Zhou, Lu and Zhang (2009) found that the security risks associated with mobile transactions have a negative impact on user trust, i.e., the higher the perceived security risks, the more worried consumers are about the transaction, and the lower their trust in the transaction. Ye (2012) used the UTAUT model to model the relationship between perceived privacy protection and perceived payment security and consumers' willingness to use mobile phone payments and verified that perceived payment security plays an important role in promoting consumers' trust in mobile phone payments, while perceived privacy protection has no effect on trust, probably due to the small sample size. Luo, Rao and Ji (2017) constructed a model about the factors influencing mobile payment users' willingness to use mobile payment from the perspective of current mobile payment characteristics: popularity, payment amount and compensation, and verified through an experimental approach that users' perceived security has an impact on the establishment of trust in mobile payment.

Trust occupies a considerable position in any transaction and refers to the consumer's acceptance of the risk of whether the O2O takeaway platform can provide security measures in accordance with the agreement; when the user's perceived security is high, a bond of trust begins to be established between the platform and the user. Based on the above literature analysis, this paper uses the classification of trust into cognitive trust and affective trust to measure its relationship with information security perception, and it can be argued that information security perception has a positive impact on the establishment of trust. This means that users will trust an O2O takeaway platform if they are aware of possible information security risks and threats, have a high level of awareness and knowledge, and can control them. From the above review of literatures, this study hypothesizes that:

H2a: Perceived perception has a positive effect on cognitive trust.
H2b: Perceived perception has a positive effect on affective trust.
H2c: Understanding perception has a positive effect on cognitive trust.
H2d: Understanding perception has a positive effect on affective trust.
H2e: Controllable perception has a positive effect on cognitive trust.
H2f: Controllable perception has a positive effect on affective trust.

Relationships between User's Trust and Continuous Purchase Intention

O2O food and beverage takeaway platforms have low business involvement and short decision-making processes, but risk and uncertainty still accompany the customer's purchase process. Trust, as an inherent contract to build long-term transactions, is crucial in decisions that influence user behavior. The O2O takeaway platform in this paper belongs to the domain of mobile commerce systems. Higher uncertainty and more serious security threats can increase the importance of the user's trust factor on whether to continue using the system. Swan, Bowers and Richardson (1999) argue that trust building between salespeople and customers is the key to

successful sales and that trust is a vital facilitator for customers to develop a continuous purchases intention and achieve repeat purchase behavior. Singh and Sirdeshmukh (2000) found that trust mechanisms have a positive effect on user loyalty, which ultimately causes consumers to engage in sustained buying behavior. Pavlou (2002), from the perspective of economics, sociology, and marketing theory, confirms that appropriate feedback mechanisms can enhance user trust and, through trust, influence users' propensity to transactions. Gefen and Straub (2003) concluded that users' repeat purchase behavior on online shopping platforms is influenced by trust. Li, Browne, and Wetherbe (2006) agree that trust can maintain user stickiness and enhance users' willingness to continue using. Chiu, Hsu and Lai (2012) presented that customer loyalty and willingness to repurchase are important factors in maintaining the normal operation of an online shop and based on adding consideration of user trust to the information system continued use model. Chen, Li and Song (2015) concluded that repurchase willingness is influenced by the role of trust. This may have a direct impact on user trust, especially in the current developed online environment where any negative events occurring are widely disseminated and the importance of platform word-of-mouth to consumers is increasing. Huang and Zhu (2016) constructed a model of mobile social application Weibo users' willingness to use based on privacy risk theory and concluded that trust and satisfaction have a direct effect on continuous willingness to use. Based on information adoption and institutional trust theories, Yin (2017) investigated the mechanism of consumer trust in third parties in the context of the sharing economy, confirming that trust can reduce users' perceived risk and positively influence the intention to continue using. Fang and Zhou (2017) investigated the path of social interaction on user behavior in an e-commerce context and mentioned that trust has a significant effect on both users' willingness to purchase and willingness to share.

Based on social cognitive theory, if the users perceive risks that they cannot aware, understand or control in time, their trust in the system will be reduced and, as they are rational people, they will not continue to use the system for any activities in order to avoid losses; If the perceived risks to the system are readily identifiable, well understood and controllable, trust in the system will be enhanced and the user's choice to continue using the system will be subject to rational considerations. Based on the above review of the literature, the positive relationship between user trust and willingness to continue to act in information systems has now been confirmed by scholars, with most of them agreeing. That is, a stronger trust will lead to a higher willingness to continue using the system, while a weaker trust will lead to a lower willingness to continue using the system. As a result, this paper hypothesizes that:

H3a: Cognitive trust has a positive effect on continuous purchase intention.
H3b: Affective trust has a positive effect on continuous purchase intention.

Trust as Mediating Role

Based on trust theory and behavioral intent theory, Lu (2006) established a model about users' initial trust based on the characteristics of B2C websites, and the results showed that the perception of personal information security as a key influencing factor can have a positive impact on continuous purchase intention through initial trust as a mediator. According to a combination of expectation confirmation theory, TAM theory and commitment-trust theory, Vatanasombut et al. (2008) argues that online banking user trust, as a powerful predictor in an e-commerce

environment, can indirectly positively influence customers' perceptions of online banking security through the mediating bridge of trust. Gu et al. (2016) empirically tested that user characteristic factors without satisfaction as a mediator can indirectly have an impact on continued propagation intention through online trust. Luo et al. (2017), attempted to address the issue of user trust and security in mobile payments, with the aim of examining how perceived security and perceived trust in the model can have an impact on mobile payment users' willingness to use, and how trust as a mediating variable can indirectly have an impact on willingness to use, and the study mainly chose an experimental approach to measure the above variables. Based on the above theoretical generalization, this paper replaces the original model of satisfaction with trust as a mediator, given that trust not only has a direct effect on users' intention to continue purchasing, but also acts as a mediating bridge that allows other variables to indirectly influence intention to continue purchasing through trust. As a result, this paper hypotheses that

H4: Trust has a mediating effect between information security perception and continuous purchase intention.

H4a: Cognitive trust has a mediating effect between perceived perception and continuous purchase intention.

H4b: Cognitive trust has a mediating effect between understanding perception and continuous purchase intention.

H4c: Cognitive trust has a mediating effect between controllable perception and continuous purchase intention.

H4d: Affective trust has a mediating effect between perceived perception and continuous purchase intention.

H4e: Affective trust has a mediating effect between understanding perception and continuous purchase intention.

H4f: Affective trust has a mediating effect between controllable perception and continuous purchase intention.
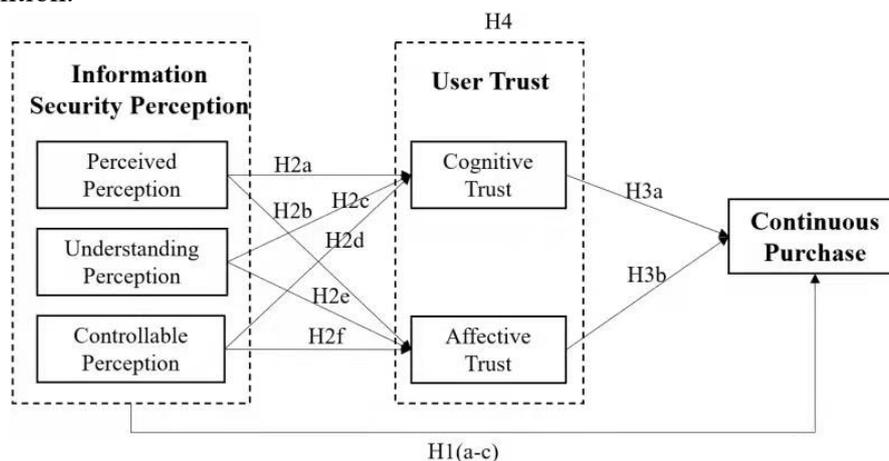

Figure 1: Conceptual Framework

3. Research Methodology

3.1 Research Design

This research is a quantitative design using questionnaire to collect data from Chinese users

who has an online buying experience in O2O food and beverage takeaway platform such as Ele. me and Meituan etc. within the past 1 year in Kunming, City. The sample size was calculated using Cochran's formula at a confidence level and error term of 95% and 5%, respectively (Cochran, 1977). The sample size was 385 after calculating.

3.2 Data Collection

A web-based online survey was used to collect the data and the convenience sampling method was adopted. A large-scale questionnaire survey was conducted for those Chinese users with O2O food and beverage takeaway platform buying experience in Kunming. A total of 472 questionnaires were collected, and 439 valid questionnaires were deemed usable after invalid questionnaires were eliminated.

3.3 Measurement Item

All the measurement items used in this study were adapted from prior validated scales. These items were measured using a 5-point Likert scale ranging from 1, strongly disagree, to 5, strongly agree. All the survey items were pilot tested using samples collected from 30 participants. The results indicated that the measurement model fulfilled the criteria for reliability, convergent validity, and discriminant validity.

4. Data Analysis and Findings

4.1 Descriptive Analysis

A sample of male to female ratio is close to 1:1, gender balance in our respondents. Respondents were mainly at the age of 19-30 (72.53%) and with a bachelor's degree (61.86%). More than 60 percent of the respondents (63.51%) have been using the Internet O2O food and beverage takeaway platform for more than 3 years. The respondents who choose Ele. me and Meituan platform are the most, accounting for 54.61%, 40.37%, respectively. The data indicate that the above two O2O food takeaway platforms have a high proportion of users and are the leaders in the food delivery industry.

4.2 Reliability and Validity

Cronbach's alpha was used to measure reliability of the measures. As per Hair et al. (2013) the value of Cronbach's alpha coefficient of 0.7 was taken as the threshold level in order to ensure the stability and consistency of the instruments. According to Table 3, the Cronbach's alpha value of all constructs was above 0.7. Thus, the reliability of the construct is established.

Construct validity was measured by utilizing convergent validity and discriminant validity. Convergent validity was assessed with Composite Reliability (CR), Factor Loadings and Average Variance Extracted (AVE). If the value of CR reached 0.7 or above, and the value of factor loadings and AVE both reached 0.5 or above, the measurement model has good convergence validity (Hair et al., 2013). As per Table 1, all indicators met the standard, indicating that the measurement model in this study had good convergent validity. In order to determine discriminant validity, the square root of AVE of each construct was compared to the squared correlations of other constructs. From Table 2, it is evident that square root of AVE value of each construct is greater than the squared correlations of this construct to any other construct. Hence, the discriminant validity is established

(Hair et al., 2013).

Table 1: Results of Validity and Reliability Analysis

Factors	Indicators	Factor Loadings	AVE	CR	Cronbach's Alpha
Perceived Perception (PP)	PP1	0.811	0.752	0.774	0.834
	PP2	0.804			
	PP3	0.756			
Understanding Perception (UP)	UP1	0.735	0.796	0.799	0.858
	UP2	0.749			
	UP3	0.768			
	UP4	0.829			
Controllable Perception (CP)	CP1	0.801	0.824	0.824	0.817
	CP2	0.821			
	CP3	0.813			
Cognitive Trust (CT)	CT1	0.745	0.763	0.793	0.921
	CT2	0.781			
	CT3	0.746			
	CT4	0.779			
	CT5	0.716			
Affective Trust (AT)	AT1	0.820	0.853	0.851	0.905
	AT2	0.857			
	AT3	0.884			
	AT4	0.839			
	AT5	0.863			
Continuous Purchase Intention (CPI)	CPI1	0.792	0.806	0.867	0.943
	CPI2	0.806			
	CPI3	0.813			
	CPI4	0.825			
	CPI5	0.813			

Table 2: Discriminant Validity of Scale Test

Variable	PP	UP	CP	CT	AT	CPI
PP	**0.874**					
UP	0.826	**0.893**				
CP	0.859	0.802	**0.879**			
CT	0.801	0.806	0.811	**0.886**		
AT	0.785	0.715	0.726	0.741	**0.891**	
CPI	0.687	0.612	0.536	0.608	0.543	**0.877**

4.3 Measurement and Structural Model Analysis

If the implied covariance structure of the model is similar to that of the sample data, as implied by the acceptable value of the goodness of fit index (GFI), the model is considered appropriate (Cheung & Rensvold, 2002). The authors firstly verified and evaluated the measurement model and then analyzed and fitted the structural model. According to the data in Table 3, the $\chi 2/df$ of the structural equation model is 2.003 (P=0.000), which is less than 3. RMSEA is 0.044, which is smaller than the minimum standard of 0.05. CFI is 0.911, AGFI is 0.916, NFI is

0.937, and GFI is 0.942, all of which are greater than the minimum standard of 0.9 (Kline, 2011). Therefore, the indices of the model all met the evaluation standard, indicating that the theoretical model presented in the study aligned with the actual survey data.

Table 3: Fit Indices of Measurement and Structural Models

Fit indices	χ^2 /df	GFI	AGFI	NFI	CFI	RMSEA
Recommended Values	<3	>0.9	>0.8	>0.9	>0.9	<0.05
Measurement Model	2.001	0.913	0.918	0.937	0.944	0.044
Structural Model	2.003	0.911	0.916	0.937	0.942	0.044

4.4 Results of Hypotheses Testing

Table 4 showed the standardized path coefficient and path significance for each of the hypotheses. It indicates that all the hypotheses proposed in this paper were all supported except H1b. With regard to H1a, H1c, it can be observed that a significant and positive correlation between information security perception including perceived perception ($\beta= 0.627$, $p<0.001$) and controllable perception ($\beta= 0.198$, $p<0.001$) and user continuous purchase intention towards the O2O food delivery platform, which means that H1a and H1c were supported. However, users' understanding perception has no significant relationship with users' continuous purchase intention ($\beta= 0.198$, $p>0.05$), Therefore, hypothesis H1b was rejected. In support of H2, we find that information security perception, including perceived perception, understood perception and controllable perception, is significant positively correlated with the users' cognitive trust (PP: $\beta= 0.135$, $p<0.05$; UP: $\beta= 0.413$, $p<0.001$; CP: $\beta= 0.467$, $p<0.001$) and affective trust (PP: $\beta= 0.259$, $p<0.05$; UP: $\beta= 0.406$, $p<0.001$; CP: $\beta= 0.485$, $p<0.001$) towards O2O food delivery platform, so H2a, H2b, H2c, H2d, H2e, H2f, H4g were all supported. When H3a and H3b were examined, it was found that user trust including cognitive trust ($\beta=0.549$, $p<0.001$) and affective trust ($\beta=0.528$, $p<0.001$), was positively correlated with continuous purchase intention. Thus, H3a and H3b were supported.

Table 4: Test Results of Research Hypothesis

Hypothesis	Path	Path Coefficient (β)	S.E.	C.R.	Results
H1a	PP→CPI	0.627	0.130	4.720***	Supported
H1b	UP→CPI	0.430	0.103	3.358	Rejected
H1c	CP→CPI	0.198	0.059	4.362***	Supported
H2a	PP→CT	0.135	0.071	5.205***	Supported
H2b	PP→AT	0.259	0.042	4.003***	Supported
H2c	UP→CT	0.413	0.092	5.246***	Supported
H2d	UP→AT	0.406	0.034	5.886***	Supported
H2e	CP→CT	0.467	0.057	4.956***	Supported
H2f	CP→AT	0.485	0.026	4.525***	Supported
H3a	CT→CPI	0.549	0.124	4.261***	Supported
H3b	AT→CPI	0.528	0.116	4.937***	Supported
Note: *P< 0.05; **P<0.01; ***P<0.001					

4.5 Mediation Testing

Table 5 shows how user trust (cognitive trust and affective trust) acts as a mediating factor

วารสารวิชาการสถาบันวิทยาการจัดการแห่งแปซิฟิค

The Journal of Pacific Institute of Management science

ปีที่ 9 ฉบับที่ 3 กันยายน – ธันวาคม 2566

Vol.9 No.3 (2023) September - December

****

in the relationship between independent variables like information security perception as well as dependent variable continuous purchase intentions. The results of mediation were assessed using the bootstrapping process, which is considered to be the most effective method for testing mediation and other interfering consequences (Biesanz, Falk, & Savalei, 2010). Under the 95% bias-corrected bootstrapping confidence interval, 5000 samples were used to determine whether there was a mediating effect. The mediating effect was formed if there was no zero between the upper and lower limits of the bias-corrected confidence interval (Hayes, 2009). As can be seen from Table 5, cognitive trust plays a significant total mediating role in the impact of information security perception on users' continuous purchase intention, with 95% confidence interval of (0.216, 0.423), excluding zero. Regarding the mediating effect of perceived, found that perception understood perception and controllable perception were all significant, and the indirect effect was 0.156, 0.202 and 0.287, respectively. Hence, H4a, H4b and H4c are all supported. Concerning H4d, H4e and H4f, the total mediating effect of affective trust on the influence of information security perception on users' continuous purchase intention is also significant, with 95% confidence interval (0.203, 0.344), excluding zero. To be more specific, the mediating effects of perceived perception, understood perception and controllable perception were significant, which were 0.037, 0.116and 0.152, respectively. Therefore, H4d, H4e and H4f are fully supported.

Table 5: Test Results of Mediating Effect

Hypotheses	Paths	Effect	Bootstrapping 95% Confidence Interval		Whether Mediating Effect or Not?
			Lower	Upper	
Total Mediation Effect		0.645	0.216	0.423	YES
H4a	PP→CT→CPI	0.156	0.042	0.227	YES
H4b	UP→CT→CPI	0.202	0.021	0.154	YES
H4c	CP→CT→CPI	0.287	0.019	0.193	YES
Total Mediation Effect		0.315	0.203	0.344	YES
H4d	PP→AT→CPI	0.037	0.032	0.188	YES
H4e	UP→AT→CPI	0.126	0.047	0.175	YES
H4f	CP→AT→CPI	0.152	0.086	0.195	YES

5. Discussion and Conclusions

This study innovates the research perspective and investigates the antecedent variables of continuous purchase intention based on information security perception theory and trust theory. This is different from previous research on the mechanisms of user behavior on catering platforms based on perceived risk, perceived value, satisfaction and other perspectives, and there is less research on the perception of information security on O2O food takeaway platforms in previous literature. This research also further enriches the theory of information security. Previous studies have mostly taken information security as an entire influencing factor, and there is few research on information security sub-dimensions. In this study, information security is divided into three dimensions, namely perceived perception, understood perception and controllable perception, based on the characteristics of Internet catering platforms, thus portraying the factor of information security in more detail. Using user trust as an intermediate variable, we attempt to investigate the path of the perception of information security indirectly interacting with O2O food and beverage takeaway users' continuous purchase intention through trust. The findings of this study are as follows.

First, information security perception has a positive impact on continuous purchase intentions. This paper verifies that among the three dimensions of information security perception, only perceived perception and controllable perception have a significant positive impact on continuous purchase intentions, that is, when users use the O2O catering takeaway platform to make enquiries, order food and give feedback, if they have a strong ability to detect and control the information security risks and threats that may exist on the platform, then the willingness of users to continue to use the platform will greatly increase. However, understanding perception has no significant influence on continuous purchase intention. The reason might be the questionnaire of the respondents have frequent online reservation experience, for information security problems may have already quite advanced knowledge and understanding, at the same time, the development of O2O enterprises platforms provide more and more high safety coefficient, resulting in low sensitivity of users' perception of understanding in continuous purchase behavior.

Secondly, this study verifies the influence of each dimension of information security perception on each dimension of user trust, and concludes that both cognitive trust and affective trust are positively influenced by perceived perception, understood perception and controllable perception, that is, when users use the O2O food and beverage takeaway platform to fill in and query information, reserve and receive food and beverage, make evaluation and feedback, etc., if they perceive that the possible information security risks of the operating company's platform can be detected in a timely and effective manner, and they could have a basic and comprehensive understanding and controlling, then users' trust in using the platform will be strengthened. We measure user trust in terms of both cognitive and affective trust. Cognitive trust is based on judgments of the operator's competence and reliability and evidence from other parties that the operator can be trusted and is a perception of trust based on the user's full knowledge of and proficiency in using the O2O food delivery platform. Trust requires the operator to be able to prevent the user's interests from being compromised, and if the user perceives a loss of interest when using the platform, the user will deepen their trust in the platform if they perceive that the operator has good information security measures in place to protect the integrity of their interests. Affective trust comes from the user's emotions towards the O2O food delivery platform. Users may be introduced to the platform by friends, advertising, social relationship and other positive public opinion guidance, as well as their own familiarity, pleasure and other emotional perceptions when using the platform, they will have the emotion to continue using the platform, believing that the platform could protect personal information security, not to harm the interests of consumers. This creates a strong behavioral willingness to use the platform to make ongoing purchases. Affective trust may not be justified by objective reasons, but only by one's own preference. Unlike cognitive trust, which can be built in a short period of time, affective trust can only be generated through long periods of communication and interaction between the two parties, whether it be direct interaction between the platform and the consumer, or indirect knowledge through publicity etc.

Third, we verified that consumers' continuous purchase intention is influenced by two dimensions of trust including both cognitive trust and affective trust, i.e., the cognitive trust and affective trust generated by users in the process of using O2O food delivery platforms move in the same direction as the continuous purchase intention, and the higher the degree of trust, the more

they believe in the operational development of the platform, and the more likely users will continue to use the platform. the greater the likelihood of continued use on that platform. Users objectively and rationally recognize the benefits of O2O food delivery platforms in terms of safeguarding their privacy, saving time and making their lives easier is a perceived trust in the platform. The more trust users have in the platform, the more they can be said to trust that the platform will deliver on its promises and bring them benefits, and this tendency makes it more likely that users will continue to use the platform. Consumers subjectively accept O2O takeaway platforms from a perceptual point of view, just as the platforms advertise that they will put consumers' interests first and will not do anything to jeopardize them, which is affective trust in the platform. The more a user believes in the platform's claims about information security, the more likely they are to continue using the platform. Trust, whether based on rational perceptions or sentimental emotions, increases consumers' willingness to continue purchasing on the platform.

Finally, the paper validates the mediating role of trust using the Bootstrap method. In the research model of the O2O takeaway platform, trust as a mediating variable plays a partial mediating role. Users' continuous purchase intention can be positively influenced directly by the perception of information security, and indirectly by the establishment of trust through the strengthening of intermediaries. If consumers can easily detect, understand and control the information security risks that may arise when using an O2O takeaway platform, then information security perceptions will both promote the idea of continuous use and enhance the trust that consumers have built when using the platform, and continuous purchase intentions will increase as trust is passed on. Therefore, if consumers are not aware of the threats and losses to their privacy and information security when using O2O takeaway platforms, and are unable to discover them in a timely manner, are completely unfamiliar with them and cannot be controlled, on the one hand, this will affect the idea of continuing to use the platform, and on the other hand, the platform will be perceived as untrustworthy, and consumers will think less of continuing to use it in order to avoid losses.

6. Implications

Findings from this study contribute to several areas. Firstly, the results confirm the concept that customers' trust is prime concern for customers in continuing using the online purchasing of foods and beverage via platforms. Secondly, the stores consider that using personal information in their IT systems can result in both advantages and disadvantages. Thus, in practice, e-commerce operators, particularly food and beverage (take away) stores must place high degree concern on development of the O2O model that can protect customers' privacy and increase security in the use of internet systems. For sustainability of their online business, the stores must be honest in using the consumers' personal information in accordance with the agreement they commit to the service users. On the other hand, consumers must raise their awareness of information security that they should not completely trust the information relevant to promotions of the company and take the initiative to understand the information security terms and conditions when registering on the platform. When using the platform's service, consumers should always pay more attention to the content and manner of data collection and the scope of use of the data by

****

the operating company, in order to prevent companies from using security provisions to force the collection of information. It is also crucial to pay attention to whether the positioning function of the software is closed in time after finishing the use, as the positioning at all times can expose the location of the user's frequent activities and cause security risks to the consumers.

For food and beverage delivery companies that want to recommend services to fit consumers' personal characteristics, tastes, consumption habits, time cycle, and spending range, they data analysis should be based on the big data collected by the O2O catering platforms in the past. As a result, each user can be pinpointed and recommended information that they are likely to enjoy and accept. Therefore, the operating companies should enhance the security technology investment for each user's data and use professional protection measurement mechanism to avoid information leakage. The application software should be updated in time to protect it from illegal invasion and illegal damage. The core strategy of network security protection is to control access to data, including the use of encrypted storage and encrypted transmission technology, timely firewall upgrades, intrusion detection and security scanning to control user information data from being illegally queried and used. It is also essential to provide alerts on possible information security risks, to inform users in a timely manner when they perform inappropriate operations that their actions may pose risk issues, and to collect, use and continuously track users' private information after obtaining their authorization. Platforms have established a comprehensive information security system and do not use private information for profit without the user's permission, so as not to damage the user's information rights. For merchants and riders on takeaway platforms, operating companies should not only strengthen their awareness of the dangers of leaking consumers' privacy information and protect it, but also establish a scientific and effective management system, sign privacy protection treaties with merchants and riders, and take appropriate punitive measures when necessary.

In terms of consumer trust, O2O takeaway platforms are trusted by users for their professional ability to protect personal privacy and security, and consumers' trust is accompanied by their intention to continue using the platform. The platform can make use of various new internet media platforms and social networking platforms to promote its information security concept in various ways, explaining how the platform collects, uses and stores personal privacy information in as easy-to-understand a way as possible to deepen potential users' knowledge and understanding of the O2O catering platform. Companies can also show users how the company protects information security and the penalties for leaking information to increase users' awareness of the platform's responsibilities and capabilities; and make good use of positive word-of-mouth to increase affective trust from users. Thus, it is crucial for O2O catering (takeaway) platforms to enhance word-of-mouth communication. The platform should firstly realize that word-of-mouth marketing is vital to the business and actively improve information security measures to enhance the user's good experience to win public trust. However, when negative word of mouth is encountered, platforms need to promptly self-correct and self-examine to improve themselves and their image in the eyes of the public.

****

7. Limitations and Recommendations for Further Research

This study has several limitations. Firstly, the samples in this study are mainly university students and working people in the well-developed city with good education, easy dissemination of information, understanding of important of information leakage, and more precautions for personal privacy. The singularity of the sample may affect the application of the results to other cities. In future studies, data collection on users in other types of cities can be added to expand the scope of the study to increase the generalizability of the results. Moreover, the division of trust presented by Yadav, Sharma and Tarhini (2016) and Siau and Shen (2003) can be used in future research as technical trust, institutional trust, merchant trust, and platform trust. Finally, this research only investigates the influence of information security perceptions on behavior, without considering the antecedent variables of information security perceptions. In future research, factors affecting information security could be considered in the construction of the model.

Reference

Biesanz, J. C., Falk C. F., & Savalei, V. (2010) **Assessing Mediational Models: Testing and interval estimation for indirect effects.** Multivariate Behavioral Research, 45(4), 661-701

Chen B.B. (2016). **Research on Tourists' Perception of Online Consumption security.** Dissertation. Chongqing: Chongqing Normal University.

Chen H.T., Li T.Q., & Song S.S. (2015). **Modeling and empirical research on repeated purchase behavior of online food delivery platform users.** Soft Science, 29(11):79-82.

Cheung, G. W., & Rensvold, R. B. (2002). **Evaluating goodness-of-fit indexes for testing measurement invariance.** Structural Equation Modeling: A Multidisciplinary Journal. 9(2), 233-255

China Internet Network Information Center (CNNIC). (2018). **41thStatistical report on the development of China Internet network.** Retrieved from http://www.cac.gov.cn/2018-01/31/c_1122347026.htm.

China Youth Daily (2018.5.22). **Information security technology personal information security standards behind the introduction.** Retrieved from http://www.xinhuanet.com/tech/2018-05-22/c_1122866629.htm,2018-05-22.

Chiu C M., Hsu, M. H. & Lai, H. (2012). **Re-examining the influence of trust on online repeat purchase intention: The moderating role of habit and its antecedents.** Decision Support Systems, 53(4):835-845.

Cybersecurity Ventures Sponsored by Herjavec Group. (2017). **Cybercrime Damages Will Cost the World $6 Trillion Annually by 2021.** Retrieved from: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-CybercrimReport.pdf (accessed on 21 January 2019)

Cyberspace Administration of China (2019). **China's Internet network security situation in the first half of 2019.** Retrieved from http://www.cac.gov.cn/2019-08/13/c_1124871596.htm,2019-08-13.

Fang W.K. & Zhou, T. (2017). **Research on the mechanism of social Interaction on social Business User behavior.** Journal of Information science, 2017(1):167-172.

Furnell, S. M.& Karweni, T. (1999). **Security implications of Electronic Commerce: A Survey of Consumers and Businesses.** Internet Research, 9(5). 372-382

Gao F. (2010). **Mobile Information Security Perception and its Impact on mobile Payment Acceptance.** Dissertation. Beijing: Tsinghua University.

Gefen D., & Straub, K. D. W. (2003). **Trust and TAM in Online Shopping: An Integrated Model.** MIS Quarterly, 27(1):51-90.

Gu D.X, & Zhang Y. (2016). **Research on positive public opinion information dissemination model of social network based on expectation confirmation theory.** Information Science, 4.

Hair J, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2013). **Multivariate data analysis (7thed.), 541-663.** USA: Pearson Education Limited.

Hayes, A. F. (2009). **Beyond Baron and Kenny: Statistical mediation analysis in the new millennium.** Communication monographs, 76(4), 408-420

He X.F. (2014). **Research on Management Application Mode Based on Safety Perception Theory.** Dissertation. Xi,an: Xi 'an University of Architecture and Technology.

Hoffman, D. L, Novak, T. P., & Peralta, M. (1999). **Building Consumer Trust Online.** Communications of the ACM. 42(4):80-85

Huang B.X.& Zhu X.D. (2016). **Research on the influencing factors of users' intention to continue using mobile social apps.** Modern Information, 2016(12).

Huang, D.L. (2009). **Information Security Awareness Model and its Application.** Dissertation. Beijing: Tsinghua University.

Kline, R. B. (2011). **Principles and practice of structural equation modeling (3rd ed.).** New York, NY: The Guilford Press.

Li D., Browne G. J. & Wetherbe J. C. (2006). **Why Do Internet Users Stick with a Specific Web Site? A Relationship Perspective.** International Journal of Electronic Commerce, 10(4):105-141.

Li, J. & Hu, R. (2014). **Research on influencing factors of mobile library users' willingness to use -- from the perspective of information security perception.** Books and information. 2014(4):99-104.

Lu, F.H. (2006). **Research on the Influencing Factors of customers' Initial trust on B2C Websites Dissertation.** Zhejiang: Zhejiang university.

Luo H., Rao, P.L., & Ji X. (2017). **The influence of trust and security on mobile payment decision making.** Enterprise Economics,08:70-74.

Mainaiti, M., Zhao, X.Y., Jia, M.H., Ru, Y. & Zhu, S.K. (2018). **How we eat determines what we become: opportunities and challenges brought by food delivery industry in a changing world in China.** European Journal of Clinical Nutrition. 72(9):1282-1286

Memorabilia (2018). **Timeline: Facebook User data breach.** Retrieved from http://www.dsj365.cn/front/article/6019.html,2018-03-17.

Pavlou, B. P. A. (2002). **Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior.** MIS Quarterly, 26(3):243-268.

Siau K, & Shen Z. (2003). Building customer trust in mobile commerce. Communications of the ACM, 46(4):91-94.

Singh J. & Sirdeshmukh D. (2000). Agency and trust mechanisms in consumer satisfaction and loyalty judgments. Journal of the Academy of Marketing Science, 28(1):150-167.

Swan J E, Bowers M R, & Richardson L D (1999). Customer Trust in the Salesperson: An Integrative Review and Meta-Analysis of the Empirical Literature. Journal of Business Research, 44(2):93-107.

Wei M.X. (2005). Research on the Impact of perceived privacy and perceived security on E-commerce credit. Chinese Journal of Management, 2(1):61.

Xinhuanet. (2019). Hit the net black ash production! Didi and Tencent set up a joint lab on Internet security. Retrieved from http://m.xinhuanet.com/gd/2019-08/01/c_1124822840.htm

Yadav R., Sharma, S. K. & Tarhini, A. (2016). A multi-analytical approach to understand and predict the mobile commerce adoption. Journal of Enterprise Information Management, 29(2):222-237.

Ye Q.F. (2012). An Empirical study on factors influencing mobile payment adoption. Dissertation. Chengdu: University of Electronic Science and Technology of China.

Yenisey, M. M., Ozok, A. A., & Salvendy, G. (2005). Perceived security determinants in e-commerce among Turkish university students. Behaviour and Information Technology, 24(4), 259-274.

Yin H. (2017). Research on consumer trust in third-party travel platform in sharing economy。 Dissertation. Harbin: Harbin Institute of Technology.

Zhou, T., Lu, Y. B. & Zhang, J. L. (2009). Research on The Acceptance Behavior of Mobile Business Users based on perceived Value and trust. Journal of Management Science, 6(10):1407-1412.