E-Payment Continuance Usage: The Roles of Perceived Trust and Perceived Security

Thanh D. Nguyen(✉) and Quynh N. T. Tran

Banking University of Ho Chi Minh City, Ho Chi Minh City, Vietnam
thanhnd@buh.edu.vn

Abstract. E-payment is an important concept of the core e-commerce elements; it has become one of the essential success factors for financial and business services. This work elaborates the roles of perceived trust and perceived security on continuance usage of e-payment through collecting data from students who have used e-payment for e-commerce in Vietnam. The maximum likelihood of structural equation modelling is analyzed on a total sample of convenient of 210 customers. Research findings demonstrate that perceived trust and perceived security have significant roles in the model of e-payment adoption. The model amounts to 26% of continuance usage of e-payment.

Keywords: Continuance usage · e-payment · Perceived security · Perceived trust

1 Introduction

E-payment has gained recognition and is deployed worldwide [16]. The habit of cash payment is the biggest impediment for the e-payment development. Besides, in e-commerce, customers and consumers are still reluctant to use non-cash payments. E-payment brings convenience, efficiency, and risk reduction because there is no longer have to bear the cost of handling the amount of cash held and reach more customers. E-payment allows customers to make e-transactions anywhere and anytime. Besides, customers can directly deal with manufacturers, bypassing intermediaries so they can buy goods in a convenient solution [18]. E-commerce in Vietnam is booming at over 25% per year [35]. Notwithstanding, according to market research by Q&Me [36], the number of e-payment transactions is quite low, accounting for 20% of payments, although up to 70% of the population uses the Internet, according to We Are Social [30], the habit of paying cash is the biggest obstacle to the development of e-payments in Vietnam. Customers are still reluctant to use e-payment when participating in e-commerce. There are many theoretical models of IT adoption such as TAM [6], TAM2 [37], TAM3 [38], and UTAUT [28], UTAUT [39] – these are typical theories for measuring the behavioral intention of information systems and actual use by users. There are several IT adoption theories, which are based on the users' use intention and actual usage of information systems. Although there are many works related to e-payment continuance usage (e.g., Bhattacherjee [4], Limayem et al. [16], Ventakesh et al. [29]), m-learning [34], e-commerce [40], not many related works in Vietnam.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
O. Gervasi et al. (Eds.): ICCSA 2022 Workshops, LNCS 13381, pp. 253–264, 2022.
https://doi.org/10.1007/978-3-031-10548-7_19

This work objective examines the roles of perceived trust and perceived security on e-payment continuance usage, which tests impact factors on continuance usage of e-payment for customers. The data was collected from students who used e-payments in Vietnam. The analysis of the maximum likelihood (ML) of structural equation modelling (SEM) for testing the model. Interestingly, research findings are accommodating information to corporations in expanding the e-payment system for e-commerce and adding scientific to the theory of continuance usage. Therefore, the rest of the paper is structured as follows: in the next section, related works and research models show the definition of e-payment and the model reviews of literature and theoretical framework, including hypotheses. The following section presents research methods. Then, analysis results and result discussion. Finally, the conclusion is in Sect. 5.

2 Related Works and Research Model

2.1 E-payment

The trade presto expansion through technological and e-commerce progress are the elements that led to the rapid development of e-payment and resulted in the constantly evolving payment services [25]. According to Abrazhevich [1, p. 3], *e-payment is defined as online transactions are conducted via the Internet*. Whereby there are a variety e-payment of types, e.g., e-wallet, e-cash, debit/credit cards, digital accumulating balances, digital checking payments, and online stored value [13, 24]. The e-payment systems stakeholders include customers, merchants, consumer banks, merchant banks, payment instrument issuers, and payment service providers [14].

2.2 Advantages and Disadvantages of E-Payment

- **Advantages**
  For Economy. E-payment has numerous positive positive aspects to the economy [9]. It guarantees the price and guarantees quality. E-payment reduces the quantum of cash in rotation and brings profitable benefits. E-payment gradationally eliminates the use of cash, limiting illegal conditioning, thereby adding translucency and law enforcement capacity. *For Organization.* E-payment costs are another benefit for utmost providers, businesses and merchandisers–this cost is accessible [33]. *For Customer.* E-payment systems are veritably accessible–the most significant benefit of electronic payments is to reuse their deals. It allows customers to make their electronic payments anytime and anywhere [33]. Either, it can increase the benefit of cashless payment without using retail payment. Inversely important, the e-payment systems can commit to the quality of e-commerce services to serve the requirements of customers [9]. Consequently, every sale is translated, making coverage more accessible and effective.
- **Disadvantages**
  Fee. Some e-payment system merchandisers bear customers or merchandisers to pay a service figure [22]. In addition, one of the disadvantages of electronic payments is the rejection of freights, as there's no transactional information about electronic payments, so customers may have a grueling time agitating these costs [26]. Hence, customers

should know how to cover themselves against charges for indecorous processing of electronic payment systems, videlicet. *Missed Mistake.* The goods arrive with an error paid for and ordered in the e-shop [26], so they can not be used, and customers have run out of plutocrat [22]. *Online security.* e-payment systems warrant authentication – the biggest problem of electronic payments [22]. In the meantime, there are no results to corroborate or corroborate who has entered electronic payment information systems, which are not culprits.

2.3 Related Works

- **IT Adoption**
  The Reasoned Action (TRA) theory aimed to explain the relationship from attitudes to behaviours within the action of a human. Planned Behavior (TPB) recommended a new component of perceived behavioural control. Davis et al. [6] built the Technology Acceptance Model (TAM), which is based on the foundational theories of TPB and TRA, with the two new factors of usefulness and perceived ease of use. TAM2 of Venkatesh and Davis [37] and TAM3 of Venkatesh and Bala [38] are extended models of TAM. Besides, Unified Theory of Acceptance and Use of Technology (UTAUT) is proposed by Venkatesh et al. [28]. Then, Venkatesh et al. [29] added facilitating conditions, effort expectancy, social influence, and a key of perceived trust to introduce the information systems continuance intention theory. UTAUT2 of Venkatesh et al. [39] is an extended model of UTAUT. These theories of UTAUTs and TAMs are the celebrated information systems models with the most cited in the global.
- **Perceived Risk**
  Perceived risk theory explains the behavior of users in the face of risks [3]. Negative antecedents can emphasize stoner conduct and lead to a significantly established conception in consumer behavior, videlicet perceived risk [3]. Meanwhile, perceived risk is a natural generality of the sense of unreliability regarding possible use negatively affiliated with a service or product [7]. Perceived risk has been divided into two confines perceived risk in the electronic sale and perceived risk with a service or product [20]. In which, the perceived risk in the electronic transaction is a possible threat of deals that druggies may face when using e-commerce [20].
- **Perceived Trust**
  Perceived trust is one of the two critical challenges of electronic payment systems [2]. In addition, perceived trust is the private belief in good faith that one party will fulfill its scores according to the prospects of the stakeholders [21]. Trust also comes from reputation, and reputation is belief in the trading terrain. Numerous authors have studied both perceived risk and perceived trust in e-services [7], e-commerce [21], e-banking [8], m-learning [34], and they have proven that perceived risk and trust are the most salient rudiments in electronic payment. When making a comparison between traditional payment and electronic payment systems, the confidence in electronic payments will be advanced if further consumers prefer to use electronic payment channels [32].

2.4 Research Model

From the theoretical basis of IT adoption (e.g., TRA, TAM, UTAUT), the theories of perceived security, and perceived trust, and the previous studies, it proposes the roles of perceived security and perceived trust on e-payment continuance usage for measuring the relationships between the factors of a structure model (Fig. 1). All concepts are performed as below:

- *Technical Protections (TEP).* Specific technical mechanism series are used to stabilize e-payment transactions safety on the Internet and have now been developing [13]. Furthermore, Chellappa and Pavlou [5] emphasized that the factors of technical protections, such as integrity, and stability, including privacy, have a positive impact on perceived trust and perceived security.
- *Transaction Procedures (TRP).* There are steps users must take to perform a service [13]. There are three procedures in transaction procedures: (1) providing customers with many separate steps toward the e-payment completion; (2) authenticating each participant before the making of the transaction; and (3) sending messages of acceptance to each attendance after the e-payment consummation [11].
- *Security Statements (SES).* Which are statements made by enterprises providing e-payment services on security [13]. Security statements are possible to influence the perceived trust and perceived security of customers in e-payment [21], by reassuring and informing consumers regarding the e-payment transaction security.
- *Personal Past Experience (PPE).* That is a level of familiarity with a certain amount of knowledge [31]. Personal past experience leads to faster than e-payment adoption [22]. Meanwhile, Hackbarth et al. [10] interest that users are more convenient to use technology when users have advanced underwent.

  The related works showed the positive effect of the factors of transaction procedures, technical protections, personal past experience, and security statements on the perceived trust and the perceived security as Kim et al. [13], Linck et al. [17], Oney et al. [19]. Hence, under the e-payment system, these hypotheses are proposed:

  – *H1:* Transaction procedures (TRP) has a positive impact on perceived security (PES) in e-payment continuance usage.
  – *H2:* Transaction procedures (TRP) has a negative impact on perceived trust (TRU) in e-payment continuance usage.
  – *H3:* Technical protections (TEP) has a positive impact on perceived security (PES) in e-payment continuance usage.
  – *H4:* Technical protections (TEP) has a negative impact on perceived trust (TRU) in e-payment continuance usage.
  – *H5:* Security statements (SES) has a negative impact on perceived security (PES) in e-payment continuance usage.
  – *H6:* Security statements (SES) has a positive impact on perceived trust (TRU) in e-payment continuance usage.
  – *H7:* Personal past experience (PPE) has a negative impact on perceived security (PES) in e-payment continuance usage.
  – *H8:* Personal past experience (PPE) has a positive impact on perceived trust (TRU) in e-payment continuance usage.

- *Perceived Security (PES).* That is the customers' subjective evaluation of the security of the online system [13]. In this study, perceived security is understood as the degree of security customers' evaluation e-payment transactions and services. Kalakota and Whinston [12] confirmed that the resistance and technical strengthening of the online system against the attacks on security are two important factors that impact online system security.
- *Perceived Trust (TRU).* That is the belief that customers with online services will proceed under the expectations of customers and consumers [27]. Perceived trust is identified as one of the most critical elements, impacting online customer usage, and with trust higher levels are more than slantwise to use [21]. In this study, perceived trust is understood as the willingness to use e-payment despite potential risks.
- *E-payment Continuance Usage (ECU).* It performs behavioral patterns reflecting e-payment continued usage, which mentions to post-adoption behavior form [16]. For the viability of long-term of the e-payment system and the rearmost success depending on the continuous use more than the first time use [4].

  Furthermore, the factor of perceived security [23] and the factor of perceived trust [29] also have a negative effect on e-payment continuance usage. Contrastly, perceived security has a negative impact on e-payment continuance usage in Shao and Zhang [23], and perceived trust has a positive impact on e-payment continuance usage in Venkatesh et al. [29]. Thus, under the e-payment system, these hypotheses are proposed:

  – *H9:* Perceived security (PEC) has a negative impact on e-payment continuance usage (ECU).
  – *H10:* Perceived trust (TRU) has a positive impact on e-payment continuance usage (ECU).

3 Research Method

There are two phases in this work: the first phase is the qualitative method used for the preliminary research, and the second is the quantitative method used for a formal analysis. Firstly, from the literature review and the related research, which construct a scale with a draft. Then, the banking system and e-payment experts are discussed, which ensures the scale contents accuracy. Next, a measurement scale in the formal research uses the revision scale. A questionnaire with 7–point Likert: strongly disagree (1) – disagree (2) – somewhat disagree (3) – undecided (4) – somewhat agree (5) – agree (6) – strongly agree (7), which measures the indicators assessment levels. Convenient sampling method use for data collection, based on the survey accessibility. The survey is sent to students who have used e-payment of all kinds in Vietnam via Google docs by sending it directly to their e-mail and Facebook lists. Finally, collection data are analyzed by the method of the maximum likelihood (ML) of the structural equation modelling (SEM) by AMOS and SPSS. In this study, there are 210 valid samples out of 290 samples (80 invalid samples) of 27 items in the scale of the measurement which are used for analysis, as detailed in Table 1.

Table 1 Measurement scales and analysis results

Talent	Indicator	EFA loading	CFA loading
Transaction procedures	TRP1: E-payment system always calls for the user name and password when log-in	0.821	0.584
	TRP2: There are various measures to authenticate	0.867	0.932
	TRP3: There is a step to verify payment before the finalization of the actual payment	0.881	0.939
Technical protections	TEP2: Personal information has not been released to other third parties	0.852	0.877
	TEP3: The payment amount or transaction data displayed is always accurate	0.854	0.842
	TEP4: E-payment transaction data transferred over the Internet is securely protected	0.853	0.843
	TEP5: Payment services are always available at any time in a day	0.859	0.830
	TEP6: Temporary or sudden errors rarely occur during e-payment transactions	0.815	0.809
Security statements	SES2: The site provides security statements	0.868	0.905
	SES3: It is easy to find security statements	0.908	0.919
	SES4: Every concern can be easily found in a help section	0.898	0.916
	SES5: Security statements are drafted in an easily understandable way	0.878	0.920
Personal past experience	PPE1: Having experience of e-payment	0.945	0.976
	PPE2: Getting many benefits from e-payment	0.936	0.947
	PPE3: Starting using e-payment considerably a long time ago	0.942	0.963
Perceived security	PES1: Believing e-payment as secure	0.898	0.881
	PES2: Believing the information relating e-payment transactions as secure	0.876	0.850
	PES3: The information provided is helpful for secure payment transactions	0.849	0.859
Perceived trust	TRU1: Believing each participant. such as seller and buyer, involved in e-payment	0.869	0.915
	TRU2: Believing the security mechanisms of e-payment	0.901	0.931
	TRU3: Believing e-payment services	0.903	0.939

(*continued*)

Table 1 (*continued*)

Talent	Indicator	EFA loading	CFA loading
E-payment continuance usage	ECU1: Using e-payment more often than others	0.836	0.857
	ECU2: Using currently and will continue to use e-payment	0.862	0.964
	ECU3: Believing e-payment use will increase	0.851	0.899

4 Research Result

4.1 Data Description

Gender. They include 54.3% of males and 46.7% of females. *Education.* They incude students account for 76.7%, 10.0% vocational training, college and associate degree are 8.6% and 4.7%. *Study Year.* They take junior students amount to 36.7%, 30.5% sophomore, 19.1% senior, and 13.7% freshman. *Expense a Month.* They take 42.9% for spending about VND 2.5–3 million, VND 2–2.5 million amounts to 32.4%, VND 1.5–2 million, over 3 million and below 1.5 million are 11%, 9%, and 4.7%, respectively. *Total Amount of an E-order.* It is 70% of VND 0.1–0.5 million, 22.4% of below VND 0.1 million, and 7.6% of over VND 0.5 million. *Types of Goods.* Books and stationery are 57.1%, 33.1%, 32.9%, and 31.7% for e-devices and accessories, home appliances, and health and beauty, respectively. *Numbers of E-payments.* 41% of 4–6 times, 1–3 times, and 7–10 times are 31.5% and 22.3%, over 10 times is 5.2%. *E-payment Type.* e-wallet is 63.3%, 33.8% for ATM transfer, and 16.7% for e-banking. *Bank Account.* State-owned banks represent 45.6%, joint-stock commercial banks are 38.9%, and 15.5% for the other banks. *E-wallet Account.* 78.2% use *MoMo*, other e-wallets, *Zalo pay* and *Moca* are 14.5%, 12.8% and 9.0%, respectively.

4.2 Exploratory Factor Analysis and Confirmatory Factor Analysis

The first exploratory factor analysis (EFA) has enucleated seven factors from 27 items. The variables combine into seven groups of elements in the rotated component matrix as in the theory: transaction procedures, perceived trust, perceived security, security statements, technical protections, personal past experience, and e-payment continuance usage. The factor loading of all items in EFA range between 0.588 and 0.940 (Table 1). Notwithstanding, the total variance extracted (TVA) = 82.66% could explain the data difference of 82.66%. Therefore, the measurement scale can be used for the next analysis: the confirmatory factor analysis and the structural equation modelling.

The first confirmatory factor analysis (CFA) continues to eliminate three observational variables, including TEP1 of *technical protections* factor, SES1 and SES6 of *security statements* factor, whereas the factor loading of CFA < 0.50. Next, the second CFA with 24 items manifests that the measurement scale the indexes: $\chi^2/dF = 1{,}775$; TLI = 0.946; CFI = 0.963; RMSEA = 0.041; GFI = 0.902, which can be accepted.

Table 2 Data and coefficients of square correlation

	Mean	S.D.	TRP	TEP	SES	PPE	TRU	PES	ECU
TRP	4.467	1.480	0.835*						
TEP	2.996	1.073	0.020	0.840*					
SES	5.492	1.050	0.034	0.091	0.915*				
PPE	5.098	1.277	0.013	0.078	0.040	0.962*			
TRU	5.075	1.421	0.019	0.081	0.091	0.047	0.928*		
PES	3.402	1.496	0.040	0.006	0.005	0.005	0.093	0.863*	
ECU	5.498	0.996	0.043	0.045	0.049	0.097	0.087	0.037	0.908*

**AVE: Average Variance Extracted; S.D.: Std. Deviation*

Thus, the data assort with the measurement model. The factor loading of all items in CFA range from 0.584 to 0.976 (Table 1). Another side, these factors composite reliability (CR): transaction procedures, perceived trust, perceived security, security statements, technical protections, personal past experience, and e-payment continuance usage range between 0.869 and 0.974 (> 0.5), as detailed in Table 2.

Moreover, the values of average variance extracted (AVE) are from 0,835 to 0.926, as indicated in Table 1. Thus, the convergence value is gained from the measurement scale. Furthermore, the square correlation coefficient (r^2) is smaller than the AVE value for each factor, respectively. Hence, the measurement scale is an outstanding value.

4.3 Structural Equation Modelling

The maximum likelihood (ML) of the structural equation modelling (SEM) accommodates that the indexes of scale: $\chi^2/dF = 1{,}959$; TLI = 0,945; CFI = 0,953; RMSEA = 0,048; GFI = 0,901, can be accepted. Accordingly, the data in the theoretical model is a well-proportioned fit. Meanwhile, antecedent factors – *transaction procedures* and *technical protections* have a positive impact on *perceived security*. There is a negative relationship from *security statements* to *perceived security* with γ coefficient = −0.098 ($p > 0.05$), the relationships from *perceived security* to the other factors are statistically significant ($p < 0.05$), except for *personal past experience* ($p = 0.734$). Thus, hypotheses *H1*, *H2*, and *H3* are supported, while hypotheses *H5* and *H7* are rejected. Likewise, *personal past experience* and *security statements* have the positive impact on *perceived trust* with γ coefficient = 0.399 ($p < 0.001$) and 0.347 ($p < 0.001$), respectively.

However, the relationship between *transaction procedures* and *perceived trust* is not statistically significant ($p > 0.05$). Hence, hypotheses *H6* and *H8* are accepted, while hypothesis *H4* is rejected. Furthermore, intermediate factors – the negative path from *perceived security* to *e-payment continuance usage* is statistically significant ($p < 0.001$), so hypothesis H09 is accepted. Furthermore, the data accept the positive path from *perceived trust* to *e-payment continuance usage* with γ coefficients = 0.370 ($p < 0.001$). Thus, hypothesis H10 is accepted. Pleasantly, the relationships of all paths with continuance usage of e-payment are strongly accepted (Table 3).

Table 3 SEM and hypotheses testing results

H	Path	Beta	SE	p	Result
H1	PES ← TRP	0,249	0.102	0.002	Supported
H2	TRU ← TRP	−0.172	0.093	0.012	Supported
H3	PES ← TEP	0.383	0.098	***	Supported
H4	TRU ← TEP	−0.108	0.089	0.102	Rejected
H5	PES ← SES	−0.098	0.105	0.203	Rejected
H6	TRU ← SES	0.347	0.099	***	Supported
H7	PES ← PPE	0.024	0.076	0.734	Rejected
H8	TRU ← PPE	0.399	0.072	***	Supported
H9	ECU ← PES	−0.307	0.049	***	Supported
H10	ECU ← TRU	0.370	0.046	***	Supported

*** *p-value < 0.001; S.E.: Standard Error*

4.4 Result Discussion

The research results demonstrated that the perceived security negative and the positive perceived trust influence on the continuance usage of e-payment are comparatively large, with $\gamma = 0.370$ and -0.307. The relationships from antecedents of transaction procedures and technical protections to the factor of perceived security are positive, and the path from transaction procedures to perceived trust is negative (Fig. 1).

The relationships between antecedents such as security statements and personal past experience and the factor of perceived security are harmful and not statistically significant, but the path from security statements and personal past experience to perceived trust is positive. One explanation of this notion could be that the security statements issued can not convince the users that e-payment is free from risk. In addition, the customer care services of some enterprises are considered to be relatively poor in the event of an incident, due to failure to handle or delay in handling queries. This result indicated that personal past experience and security enunciations have a positive impact on perceived trust as in Kim et al. [13], Oney et al. [19].

Practically, there are seven out of 10 hypotheses are supported. Especially, the structural equation modelling also manifested that antecedent factors of personal past experience, technical protections, security statements, and transaction procedures, and intermediate factors of perceived security and perceived trust may be explained 26% ($R^2 = 0.26$) the outcome factor – e-payment continuance usage. This finding is comparable with Limayem et al. [16] amounted to 26% of continuance usage.

4.5 Theoretical and Practical Implication

Research results expropriated the theoretical basis for the theories of IT adoption, such as TAM or UTAUT, the theories of perceived security, and perceived trust. Besides, the

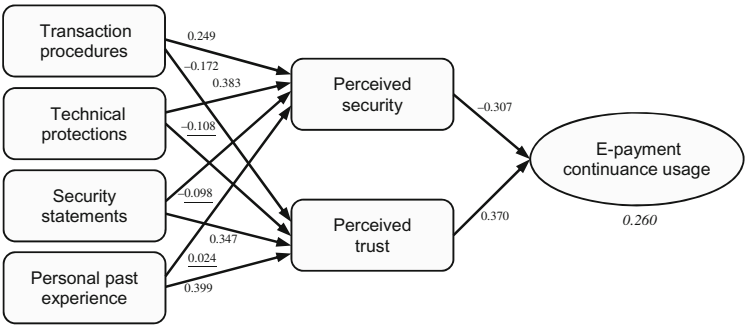

Fig. 1. Research model and testing results

research results also indicated several factors that can take the important role in influencing on e-payment continuance usage. Perceived trust impact most on continuance usage in e-payment usage contexts. Thus, web commerce sites, online payment method providers and web browser developers should encourage customers to have more experience to use their system. Hands-on experience gained through use and training may help reduce the uncertainty and create favorable user perceptions. Moreover, security statements should be written simply and understandably. Security statements should also be placed markedly, thus, customers can easily find them.

Especially, perceived security affects negatively on e-payment continuance usage. Hence, better technical protections should be implemented to foster e-payment system security. In fact, web commerce sites, online payment method providers and web browsers have become more aware of the importance of security. They have been investing in the latest and modern technology to ensure the security of e-payment transactions. In addition, transaction procedures is also an important factor when evaluating about the security of e-payment system. They should pay attention to improve the website interface as well as e-payment application, hence, customers can feel comfortable during the payment transactions.

5 Conclusion

The work results illustrated that antecedent factors measurement scale, intermediate factors, and continuance usage of e-payment is evidenced by reliability. The exploratory factor analysis and the confirmatory factor analysis of all items manifested that all factor loading of items loaded high-value concerns. Therefore, the scale of the measurement is indicated convergence and distinguishing value. Especially, the maximum likelihood of the structural equation modelling accommodated these relationships among constructs, including transaction procedures, perceived trust, perceived security, security statements, technical protections, personal past experience, and e-payment continuance usage. Interestingly, transaction procedures play an essential role in increasing the perceived security, while security statements and personal past experience have been the principal roles of rising perceived trust. The results investigated the roles of multifarious beliefs in anticipating continuance usage of e-payment, so furnishing support for

inflating beliefs set in the e-payment context. Generally, the study findings fertilize the phenomenon understanding of continuance usage. Future studies may be possible to add more elements, such as personal or social related factors, to the model. It is also possible to expand more subjects in the study, students and office workers.

Acknowledgment. We would like to say acknowledge to three blind reviewers for their helpful comments on this research. We also would like to say thank for these comments and supports of Prof. Sanjay Misra on this work.

References

1. Abrazhevich, D.: Electronic Payment Systems: A User-Centered Perspective and Interaction Design. Technische Universiteit Eindhoven (2004)
2. Aladwani, A.M.: Online banking: a field study of drivers, development challenges, and expectations. Int. J. Inf. Manag. **21**(3), 213–225 (2001)
3. Bauer, R.A.: Consumer behavior as risk taking. In: AMA Proceeding, Chicago (1960)
4. Bhattacherjee, A.: Understanding information systems continuance: an expectation-confirmation model. MIS Q. **25**(3), 351–370 (2001)
5. Chellappa, R.K., Pavlou, P.A.: Perceived information security, financial liability and consumer trust in electronic commerce transactions. Logist. Inf. Manag. **15**(5), 358–368 (2002)
6. Davis, F.D., Bagozzi, R.P., Warshaw, P.R.: User acceptance of computer technology: a comparison of two theoretical models. Manage. Sci. **35**, 982–1003 (1989)
7. Featherman, M., Pavlou, P.: Predicting e-services adoption: a perceived risk facets perspective. Int. J. Hum. Comput. Stud. **59**(4), 451–474 (2003)
8. Gao, L., Waechter, K.A.: Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation. Inf. Syst. Front. **19**(3), 525–548 (2015). https://doi.org/10.1007/s10796-015-9611-0
9. Gefen, D., Karahanna, E., Straub, D.: Trust and TAM in online shopping: an integrated model. MIS Q. **27**(1), 51–90 (2003)
10. Hackbarth, G., Grover, V., Mun, Y.Y.: Computer playfulness and anxiety: positive and negative mediators of the system experience effect on perceived ease of use. Inf. Manag. **40**, 221–232 (2003)
11. Hwang, R.J., Li, J.F., Hsiao, Y.K.: A wireless-based authentication and anonymous channels for GSM system. J. Comput. **17**, 31–36 (2006)
12. Kalakota, R., Whinston, A.B.: Electronic Commerce: A Manager's Guide. Addison-Wesley, Boston (1997)
13. 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. **9**, 84–95 (2010)
14. Laudon, K., Traver, C.: E-Commerce: Business Technology Society. Pearson (2021)
15. Liao, C., Liu, C.C., Chen, K.: Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: an integrated model. Electron. Commer. Res. Appl. **10**, 702–715 (2011)
16. Limayem, M., Hirt, S.G., Cheung, C.M.: How habit limits the predictive power of intention: the case of information systems continuance. MIS Q. **31**(4), 705–737 (2007)
17. Linck, K., Pousttchi, K., Wiedemann, D.G.: Security issues in mobile payment from the customer viewpoint. In: ECIS Proceedings, p. 62 (2006)
18. Nguyen, T.D., Huynh, P.A.: The roles of perceived risk and trust on e-payment adoption. In: Anh, L.H., Dong, L.S., Kreinovich, V., Thach, N.N. (eds.) ECONVN 2018. SCI, vol. 760, pp. 926–940. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-73150-6_68

19. Oney, E., Guven, G.O., Rizvi, W.H.: The determinants of electronic payment systems usage from consumers' perspective. Econ. Res.-Ekonomska Istraživanja **30**, 394–415 (2017)
20. Park, J., Lee, D., Ahn, J.: Risk-focused e-commerce adoption model: a cross-country study. J. Glob. Inf. Technol. Manag. **7**, 6–30 (2004)
21. Pavlou, P.A.: Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. Int. J. Electron. Commer. **7**, 101–134 (2003)
22. Rahman, S.: Introduction to E-commerce technology in business. GRIN (2014)
23. Shao, Z., Zhang, L.: What promotes customers' trust in the mobile payment platform: an empirical study of alipay in China. In: CONF-IRM Proceedings, p. 45 (2018)
24. Shon, T.H., Swatman, P.M.: Identifying effectiveness criteria for Internet payment systems. Internet Res. **8**(3), 202–218 (1998)
25. Suwunniponth, W.: Customers' intention to use electronic payment system for purchasing. Image **3**, 39994 (2015)
26. Swick, N.K.: Benefits & risks of electronic payment systems (2010). https://thatcreditunionblog.wordpress.com
27. Tsiakis, T., Sthephanides, G.: The concept of security and trust in electronic payments. Comput. Secur. **24**, 10–15 (2005)
28. Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User acceptance of information technology: toward a unified view. MIS Q. **27**(3), 425–478 (2003)
29. Venkatesh, V., Thong, J.Y., Chan, F.K., Hu, P.J.H., Brown, S.A.: Extending the two-stage information systems continuance model: incorporating UTAUT predictors and the role of context. Inf. Syst. J. **21**, 527–555 (2011)
30. We are social. Digital 2020 Vietnam report (2021)
31. Wu, J.H., Wang, S.C.: What drives mobile commerce?: An empirical evaluation of the revised technology acceptance model. Inf. Manag. **42**, 719–729 (2005)
32. Yang, Q., Pang, C., Liu, L., Yen, D., Tarn, J.: Exploring consumer perceived risk and trust for online payments: an empirical study in China's younger generation. Comput. Hum. Behav. **50**, 9–24 (2015)
33. Yaokumah, W., Kumah, P., Okai, E.: Demographic influences on e-payment services. Int. J. Econ. Bus. Res. **13**(1), 44–65 (2017)
34. Shaba, M., Roland, A., Simon, J., Misra, S., Ayeni, F.: A real-time sentimental analysis on e-commerce sites in Nigeria using machine learning. In: Shaba, M., Roland, A., Simon, J., Misra, S., Ayeni, F. (eds.) HIS 2021. LNNS, vol. 420, pp. 452–462. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-96305-7_42
35. Vietnam E-commerce Association: Vietnam e-commerce (2021)
36. Q&Me: Vietnam e-commerce report, Ho Chi Minh City (2018)
37. Venkatesh, V., Davis, F.D.: A theoretical extension of the technology acceptance model: four longitudinal field studies. Manag. Sci. **46**, 186–204 (2000)
38. Venkatesh, V., Bala, H.: Technology acceptance model 3 and a research agenda on interventions. Decis. Sci. **39**, 273–315 (2008)
39. Venkatesh, V., Thong, J., Xu, X.: Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS Q. **36**(1), 157–178 (2012)
40. Afolabi, A.O., Oluwatobi, S., Emebo, O., Misra, S., Garg, L.: Evaluation of the merits and demerits associated with a diy web-based platform for e-commerce entrepreneurs. In: Garg, L., et al. (eds.) ISMS 2020. LNNS, vol. 303, pp. 214–227. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-86223-7_19