THE IMPACT OF DATA SECURITY ON THE INTENTION OF VIETNAMESE CONSUMERS TO USE E-WALLETS

Hoang Thi Thu Huong[a], Vu Hoang Nam[a], Nguyen Thi Khanh Chi[a*]

[a]Foreign Trade University, Hanoi, Vietnam
[*]Corresponding author: Email: chintk@ftu.edu.vn

Article history
Received: February 10th, 2023
Received in revised form: March 15th, 2023 | Accepted: March 18th, 2023
Available online: April 28th, 2023

Abstract

E-wallets are used as a form of payment that brings many benefits to users. This article studies the impact of data security on consumer intentions to use e-wallets in the rapidly growing economy of Vietnam. The data consist of 236 observations from a survey of consumers in Vietnam. Covariance-based structural equation modeling (*CB-SEM*) *was employed to test the proposed hypotheses. Research results show that security trust has the greatest impact on the intention to use e-wallets, followed by perceived privacy risk, social influence, and information sensitivity. The study also reveals the role of privacy policies and security concerns in consumer intentions to use e-wallets. Based on the research results, the study provides recommendations for consumers, e-wallet providers, and governmental agencies to increase awareness of and responsibility for information security among the consumers who use e-wallets.*

Keywords: Data security; Intention to use e-wallets; Security risks; Security trust; Social influence.

DOI: https://doi.org/10.37569/DalatUniversity.13.4S.1116(2023)

Article type: (peer-reviewed) Full-length research article

1. INTRODUCTION

Along with the development of information technology (IT), personal data security has received great attention and has been studied by many scientists around the world. The security of personal data is a multidimensional concept that has been studied in many industries and fields, such as the e-commerce industry and the online advertising field, among others. Yousafzai et al. (2005) show that electronic payments can be threatened by cyberattacks on transaction data, or by unauthorized access to data through forged documents. Data security is defined as a barrier in an electronic wallet to protect the privacy of customers and limit access to personal information. In scientific language, data security is the use of encryption algorithms to protect data transmitted over the network and stored on servers (Yang & Papazoglou, 2000).

The world is currently witnessing a strong wave of development in information technology that manifests itself in all aspects of life, the economy, and society, as well as in the development of various economic sectors. Therefore, the intention to use e-wallet applications is a focus of attention among researchers worldwide. Aladwani (2001) argued that information security will be one of the main obstacles to electronic payment services in the future. Gaining the trust of customers regarding privacy and security will be a big challenge for the e-banking sector (Bestavros, 2000). Particularly for consumers in developing countries, if the appropriate information security is not ensured, they will not use online payment services because they are used to face-to-face transactions (Chong et al., 2010). This is consistent with the research of Tu et al. (2018), who found that the information security system has a certain influence on the decisions of consumers to provide personal information to social networking sites and other electronic transaction systems.

Furnell and Karweni (1999) showed that consumers who have better awareness of information security are more willing to use online shopping and payment services. Consumers are not really aware of the data security that e-wallets can provide, as well as the purpose for which e-wallets use such personal information. Therefore, a deeper understanding of personal data security becomes urgent in the current context. Privacy concerns have increased due to opportunistic behavior and misuse of personal information (Xu et al., 2013).

Nonetheless, studies on the effects of data security on the intention of consumers to use e-wallets in transitional economies such as Vietnam, where IT adoption has been rapid and the expansion of noncash payment instruments has been widespread, are still limited. One of the few studies on the use of e-wallets in Vietnam is by Bui (2021) on factors affecting the intention to use e-wallets by consumers in the city of Can Tho. That study shows that the intention to use e-wallets is influenced by perceived reputation, favorable conditions, expected effectiveness, and social influence. This lack of rigorous studies can be explained by the fact that the professions using electronic platforms and information security in transitional economies have only received attention recently. These studies in the existing literature mainly focus on customer perspectives on behavioral intention, usage behavior, adoption, and continued intention to use. Little

research has been conducted on the impact of data security on the intention to use e-wallets in developing countries such as Vietnam.

This study uses a survey of 236 consumers in Vietnam to examine the influence of data security factors on their intentions to use e-wallet applications. The study proposes a theoretical framework to analyze the impact on the intention to use e-wallets by the perception of security risks, security policies, information sensitivity, and social influence on beliefs about information security. It is found that trust in security and privacy policies has a significant impact on the intention of consumers to use e-wallets. Based on these results, the study contributes to the existing literature on consumer intentions to use cashless payments and provides practical implications for Vietnamese businesses.

The remainder of the paper is structured as follows: Section 2 presents a review of the literature and a research model to be used for this study. The research method is described in Section 3. Section 4 presents the research results, which are discussed in Section 5. Section 6 provides theoretical and practical implications. Section 7 concludes the paper by suggesting limitations and recommendations for future research.

2. RESEARCH MODEL

2.1. The concept of data security

Data security is a multidimensional concept and is defined in many ways. According to Watson (1968), information confidentiality is the claim by an individual, group, or organization of the right to determine for themselves when, how, and to what extent their personal information is disclosed to others. Flavián and Guinalíu (2006) define data security in technical terms as the guarantee by a system of the integrity, privacy, authenticity, and non-repudiation of data information. In this study, the integrity of a system refers to the ability to secure information from the risk of being distributed, stored, or modified by a third party without permission. Privacy concerns the extent to which the parties have the right to control and track stored personal data. Authenticity ensures that an action is performed only after the identity of the user has been confirmed. And non-repudiation includes measures to prevent an individual's denial of the performed behavior.

In addition, data security is considered in many studies as the customer's confidence in the service provider's security level in the face of security and privacy breaches (Belanger et al., 2002; Yousafzai et al., 2003). Breaches of security are understood as all circumstances, conditions, and events that destroy, distribute, modify, or even cheat and abuse personal information that cause economic losses to the data network and the parties concerned (Kalakota & Whinston, 1997).

In Vietnam, data security is regulated in Article 46 of the Law on Electronic Transactions (Quốc hội, 2005), which is stated as "Agents, organizations and individuals may not use, provide or disclose information about life secrets information or information of other agencies, organizations and individuals that they receive or control in electronic translation without their consent, unless otherwise provided for by law." The

Cyberinformation Security Law (Quốc hội, 2015) stipulates that "Network information security risk management is the introduction of measures to minimize cyberinformation security risks." Therefore, after collecting information with the consent of customers, firms are responsible for developing a security policy and technical management measures that meet standards with regulations on network information security. If there is a problem, remedial and preventive measures should be taken without delay. Although the concepts mentioned above are relatively simple and easy to understand, in practice, data security varies depending on many factors, including external conditions such as the industrial sector, culture, the environment, and statutory requirements (Culnan & Bies, 2003; Malhotra et al., 2004; Milberg et al., 1995) and internal factors such as personal opinion and experience (Donaldson & Dunfee, 1994). Campbell (1997) also states that concerns about information security depend on each individual's subjective thoughts about fairness and data transparency. Therefore, in certain circumstances, different consumers will have different opinions about the collection, use, and security of business information.

Personal information is information associated with identifying a person (Quốc hội, 2015). EU (2016) introduced a more specific concept of this term. Personal data are considered to be any information that identifies a particular individual. This identification can occur by direct means of communication, or indirectly through the comparison of such information as names, citizen identification numbers, addresses, and online identification numbers. In addition, physical, physiological, genetic, mental, cultural, and social characteristics can also be factors used to identify a person. Besides the above personal information, information about transaction history, bill payment history, and credit will be saved, stored, and placed under the control of e-wallets when consumers make e-wallet transactions. In this respect, protecting consumers' personal information is essential. Consumers need to be clearly and transparently informed about the approach, use, and security measures that e-wallets provide. The peculiarity of a mobile application is that the user will perform a complete transaction over the internet without the need to meet face-to-face. Therefore, a data protection fence must be in place to help customers avoid the pitfalls of online fraud and stolen data being abused for malicious purposes.

2.2. Perceived privacy risk

Privacy risk is the customer's subjective prediction of the damage caused by opportunistic and abusive behaviors that cause personal information to be spread outside (Xu et al., 2013). For users of mobile banking applications, security risks can come from many sources. The first comes from the banks' information collection, processing and using purposes. It has been stipulated in Article 21 of the Constitution (Quốc hội, 2013), Article 46 of the Law on Electronic Transaction (Quốc hội, 2005), Article 72 of the Law on Information Technology (Quốc hội, 2006) and Section 2 on privacy of personal information in Cyberinformation Security Law (Quốc hội, 2015). The storage and security of personal information are still relatively difficult to control because it is not possible to completely prevent banks from collecting and using information for illegal purposes or exchanging customer information with other parties.

The second source of security risk is the theft of data from the outside. In fact, in many serious cases, customer information has been revealed. The rise of third-party online fraud and vulnerabilities in banks' security technologies have increased consumer security concerns even more. When performing transactions on mobile banking applications, customers inadvertently leave many traces of their names, phone numbers, credit card numbers, shopping needs, living habits, and other information. This leaked information can become an opportunity for hackers to perform indirect fraud by phishing by phone or text messages, or by taking direct control of accounts on the application. With the use of mobile banking applications, customers not only face the risk of personal information leakage but also the possibility of losing financial assets. For example, hackers could withdraw all the money from customers' bank accounts.

In summary, the perception of data security risk is the customer's perception of the risk of e-wallets using information contrary to the initial commitment and the risk of data theft, fraud, and appropriation of information. The higher the degree to which an individual believes in using a technology because of its reliability and security (Bui & Ha, 2020) or the clearer the perception of security risks, the more likely an individual will be to use an e-wallet (Xu et al., 2013). Security awareness plays an important role in building customer trust, which leads to service intention (Yousafzai et al., 2005). Thus, we postulate the following hypotheses:

H1a: Perceived privacy risk directly and negatively affects the intention to use e-wallets.

H1b: Perceived privacy risk indirectly affects the intention to use e-wallets through trusted intermediaries.

2.3. Information sensitivity

Each individual has a personal scale to assess the sensitivity of information (Nowak & Phelps, 1992; Sheehan & Hoy, 2000). Customers are more likely to disclose information if the sensitivity of that information is lower (Malhotra et al., 2004). To measure the sensitivity of information, Yang and Wang (2009) divided their survey respondents into two groups: the first group was asked only for personal information, and the second group was asked for both personal and financial information. For the same purpose, Phelps et al. (2000) separated the types of personal information that users are asked into three categories: (1) demographic information, (2) information about lifestyle and consumption habits, and (3) personal financial information.

Demographic information is information that represents the characteristics of a particular population group, including basic information about age, gender, race, and socioeconomic information such as education level, employment status, marital status, and income level.

Lifestyle information refers to the preferences and habits of consumers. Demographic information is always the most common and has been used by organizations and businesses for a long time. But nowadays, with the expanding personal data exchange

market, more and more lists of consumer habits are being rented or traded between companies to segment the market based on consumer characteristics and customer behavior (Hughes, 1996; Jackson & Wang, 1994; Peppers & Rogers, 1993). In that way, suppliers can make consumption suggestions that target customer needs and increase profits for businesses.

Personal financial information is the most sensitive category of information in Vietnam. A great deal of customers' personal financial information is stored in mobile banking applications, including information about account balances, transaction histories, bill payment histories, and credit card numbers. The files containing such data are all attractive targets for hackers when attacking applications.

Therefore, the more sensitive the information, the more negative its influence on the consumer's intention to disclose personal data (Bansal et al., 2010) and the consumer's confidence in the data security of the product (Bansal et al., 2010; Fishbein & Ajzen, 1975). In addition, the intention to use e-wallets is influenced by the belief factor. In Vietnamese culture, belief is the premise for the intention to perform certain behaviors. Therefore, we propose the following hypotheses:

H2a: Information sensitivity directly and negatively affects the intention to use e-wallet applications.

H2b: Information sensitivity, through the intermediary of security beliefs, indirectly affects the intention to use e-wallets.

2.4. Social influence

Social influence refers to the perception of customers of how much influence people around them have on their intention to perform a particular behavior. This definition is quite similar to the concepts of social influence in the UTAUT (Unified theory of Acceptance and Use of Technology) of Venkatesh et al. (2003), subjective norm in the TPB (Theory of Planned Behavior), social image in the SCT (Social Cognitive Theory), and social factors in the MPCU (Model of Personal computer utilization). However, subjective standards often reflect a larger circle of influence when it comes to compliance with society's common standards. Social influence tends to arise from consultations with relatives, friends, and colleagues, which form a small circle of influence.

In the Vietnamese market, social influence not only refers to the level of agreement or disagreement of society with consumer behavior focused on data security, but it also includes the influence of the increasing number of fraudulent acts on social media networks. Social influence affects the mindset of each individual when using a new product through a technology service (Chaouali et al., 2016). Other studies suggest that social influence affects usage attitudes and the intention to use (Jiwasiddi et al., 2019). In this study, we subsume attitudes into the beliefs of product users and propose the following research hypotheses:

H3a: Social influence has a direct, negative impact on the intention to use e-wallets.

H3b: Social influence through trust mediation indirectly affects the intention to use e-wallets.

2.5. Privacy trust

Trust is an abstract term with many definitions. Liu et al. (2005) defined trust as the degree of faith that an individual has in an organization based on the intentions, actions, and integrity of that business within the scope of online transactions. The definition of Mayer (2005) is the most cited and applied concept. They defined trust as a party's willingness to suffer injury from another party's actions based on the expectation that the other party will take an action that is material to the trustee, regardless of the controllability of the other party. The acceptance of harm implies that the fiduciary is willing to accept the risk that the outcome will not be as expected. Indeed, trust always goes hand in hand with risks. Hosmer (1995) argued that effective trust occurs when customers accept risks and are willing to be harmed by the parties they have placed their trust in. If every action is performed with absolute certainty without any risk, trust is not needed. Therefore, trust is also defined as a measure to assess potential risks (Yousafzai et al., 2003).

With the global development of the internet and mobile technology, trust has become a weak point in e-commerce. Six characteristics of a website that make users trust their choice include: security, supplier reputation, ease of search, fast ordering performance, professionalism, and current design technology. Nevertheless, some scholars argue that the security of a web site is a necessary but not a sufficient condition to promote the online actions of customers (Kini & Choobineh, 1998). In addition, customer confidence is influenced mainly by technology and the performance of the e-transaction interface. The utility of the e-transaction platform is evaluated by users using various metrics, including system speed, installation speed, search features, reliability, connectivity, and availability (Lee & Turban, 2001). Of these, reliability is the most important factor for consumers. Because once personal and financial data have been transmitted online, there is a high risk that the data will be intercepted and stolen by third parties (Clay & Strauss, 2000). Therefore, raising customers' awareness about security systems and information processing is key for organizations and businesses to hold consumers' trust. Liu et al. (2005) apply the theory of rational action (TRA) to build a theoretical framework in which security-related factors directly affect trust. The greater the customer's trust, the greater the customer's confidence, and the stronger the intention to use the product. Based on the previous research, we will test the following hypothesis:

H4: Trust in security has a direct, positive effect on the intention to use e-wallets.

2.6. Privacy policy

According to Article 69 of Decree 52/2013/ND-CP (Chính phủ, 2013), which dates from 2013, a privacy policy is a commitment by an organization or business to protect the personal information of users. Protecting personal information includes

protecting the purpose of collecting the information, the scope of its use, the information storage time, the persons or organizations that may have access to it, and the address of the unit that collects and manages the information. It includes a contact method so that consumers can inquire about the collection and processing of their personal information and the methods and tools for consumers to access and correct their personal data on the e-commerce system of the information collector.

Furthermore, this content must be clearly communicated to the users before or at the time of information collection, or displayed in a conspicuous place on the e-commerce website if data are collected online. The privacy policy provided by the above decree is similar to the term "information control ability of users" in many studies. Indeed, consumers would feel less concerned about data security if a company's policy ensured they had more control over their personal information. In other words, information control is understood as a user's perception of how the business collects, stores, and uses customers' personal information. However, according to Xu et al. (2013), the ability to control information also includes the following elements: (1) the company's privacy policy, (2) awareness of data collection, (3) voluntary provision of information, and (4) openness of information use (parties with access rights, scope of use, etc.). Therefore, in this study, a bank's privacy policy is understood as the method by which the bank allows users to control the information they provide.

A security seal is a type of third-party certification for a company's commitment to security. Users are still not well aware of the security level of the business because they have not given this issue a priority and are not aware of the characteristics of the security tokens on the web.

A 2021 report by Cisco shows that 76% of customers feel more confident about the security of business data if there is a publication on the website about the privacy policy (Cisco, 2021). Therefore, privacy policy has been of wide concern and is an important factor affecting customers' intentions to use the service. Privacy policy, through the intermediary variable of trust, affects the intention to trust electronic payment services (Yousafzai et al., 2005). Liu et al. (2005) also have a similar view. The issue of privacy policy has not been taken seriously in Vietnam. Therefore, we hypothesize that the privacy policy serves as a moderating variable, as follows:

H5a: A privacy policy moderates positively the relationship between the perception of data security risk and the intention to use e-wallets.

H5b: A privacy policy moderates positively the relationship between information sensitivity and the intention to use e-wallets.

H5c: A privacy policy moderates positively the relationship between social influence and the intention to use e-wallets.

H5d: A privacy policy moderates positively the relationship between security beliefs and the intention to use e-wallets.

2.7. Privacy concerns

Privacy concerns can be understood as a user's concerned response to the risk of leakage and loss of personal data in online transactions due to the abuse of privacy (Xu et al., 2013). In the context of increasingly serious information leaks, consumers are becoming more concerned about the disclosure, exchange, and illegal sale of data between organizations. Awad and Krishnan (2006) found that users express strong concern for the security of their personal data but have not taken actions to protect their information. Individuals do not stop providing personal data even when they fear that their information will be misused.

Diana et al. (2008) stated that current security concerns have even surpassed fear in motivating consumers to take action to protect their data. The higher the level of concern, the more customers prioritize reading and learning about the privacy policies of businesses (Milne & Culnan, 2004). At the same time, users also tend to refuse to participate in services on online platforms if they feel privacy concerns. In fact, Vietnamese consumers express strong concerns about information being revealed through online transactions. According to a report of the Department of E-commerce and Digital Economy (2021), 33% of respondents answered that a major obstacle in online shopping is concern about information leakage and up to 43% of people have not shopped online because of this concern. Moreover, concerns about leaked information are among the top ten reasons why users did not make online purchases in 2017 and 2018.

No one will benefit if the privacy concerns of users persist or increase. If customers refuse to provide information, they cannot enjoy the convenient and fast services that e-banking brings. At the same time, refusal to provide information also makes it difficult for banks to build a complete and accurate customer database, hindering the development of appropriate strategies to attract potential customers. Customers will not feel satisfied when using the application, and banks will not earn as much profit as expected.

Xu et al. (2013) showed that security concerns have a direct, negative impact on the disclosure of information. The concern factor is created from the sensitivity as well as the perception of information and awareness of security risks. In this study, we argue that security concern influences the relationship between the intention to use e-wallets and other variables. In Vietnam, according to studies on the intention to use e-wallets (Bui, 2021), all factors can directly affect the intention to use e-wallets and the consumer's intention to use them without any prior experience. The concern factor acts as a catalyst for these immediate causes. Thus, the proposed hypotheses are as follows:

H6a: Privacy concerns negatively moderate the relationship between the perception of data security risk and the intention to use e-wallets.

H6b: Privacy concerns negatively moderate the relationship between information sensitivity and the intention to use e-wallets.

H6c: Privacy concerns moderate the relationship between social influence and the intention to use e-wallets.

H6d: Privacy concerns negatively moderate the relationship between trust in security and the intention to use e-wallets.

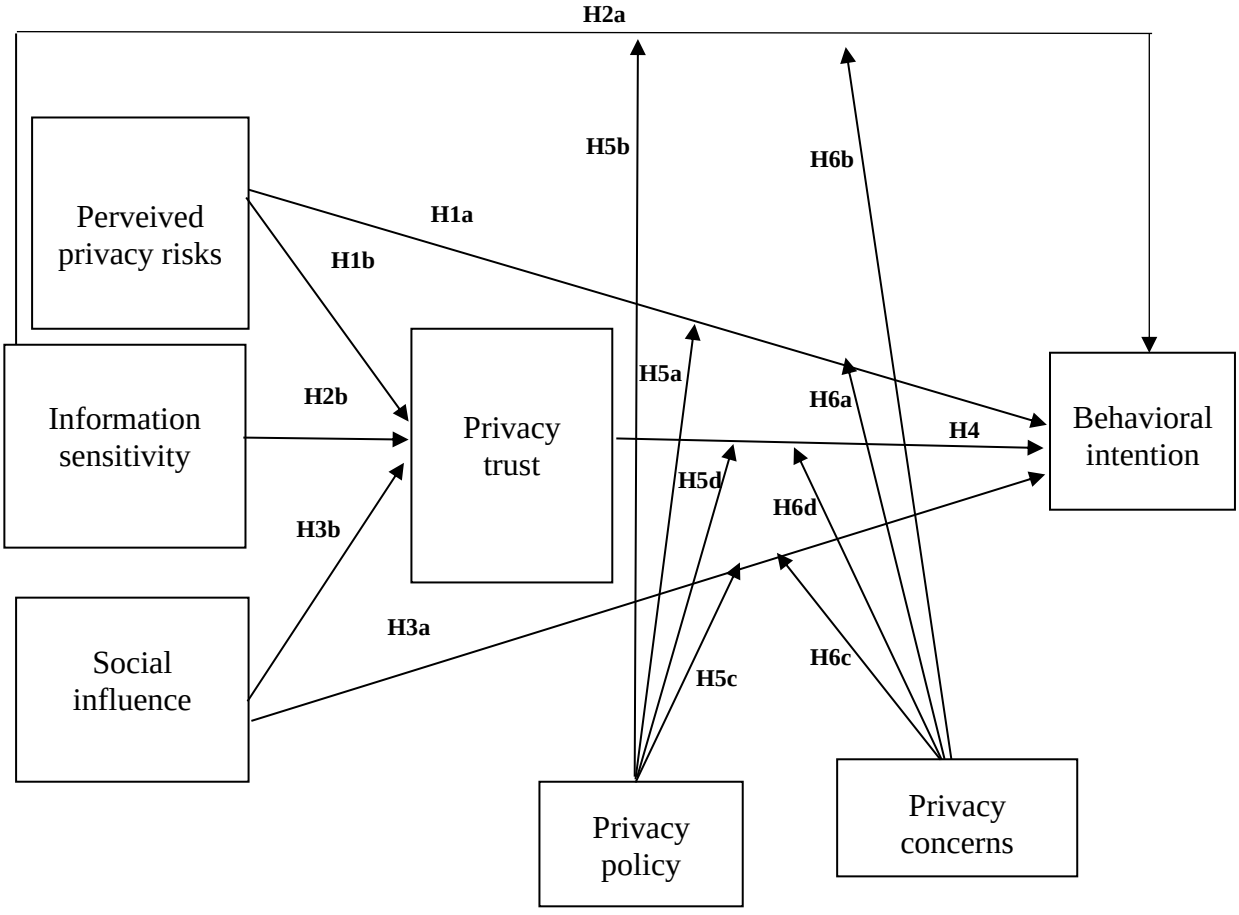

Figure 1. Proposed research model

In the research models on data security, a common point is to predict and test factors related to information security on e-commerce platforms that affect the intention to use the services on those platforms and the behavior of providing personal information. Each model offers different factors to explain data security. In this article, we generalize these factors into the following three elements: perceived privacy risk, information sensitivity, and social influence. These factors are the premise for creating privacy trust. Privacy trust is the intermediate variable leading to behavioral intention to use e-wallets. Privacy policy and privacy concerns are coordinating variables that have the role of strengthening or weakening the relationship of perceived privacy risk, information sensitivity, and social influence on the dependent variable, intention to use e-wallets. Based on these relationships, we propose the research model in Figure 1.

3. RESEARCH METHOD

3.1. The scale

The research model consists of seven basic research concepts: (1) perceived privacy risk, (2) information sensitivity, (3) privacy policy, (4) social influence, (5) privacy trust, (6) privacy concern, and (7) behavioral intention. These concepts represent latent factors, which are measured through observed variables. One latent factor can be measured through three to four observed variables. Based on previous studies, the observed variables were adjusted in accordance with the research context and environment in Vietnam.

A questionnaire was prepared using a set of statements (Table 1). The complete set of statements was pre-tested by interviewing 30 consumers. The feedback obtained from the pretest served as the basis for evaluating the quality of the statements and the way they are presented and communicated.

Table 1. Observed factors and variables

Variables	Statements	References
Perceived privacy risk (PR)		
PR1	You think that using an e-wallet application poses a risk of exposing or losing personal information.	Featherman and Pavlou (2003), Venkatesh et al. (2012)
PR2	You think that using an e-wallet application as an account is a financial risk.	
PR3	You may encounter unexpected problems when providing information on the e-wallet application.	
PR4	When using e-wallets, your account can be impersonated and fraudulently taken over.	
Information sensitivity (IS)		
IS1	E-wallet applications store a lot of sensitive information about identity.	Xu et al. (2013)
IS2	The e-wallet application requires a lot of sensitive information about personal assets.	
IS3	The e-wallet application requires a lot of sensitive information about consumption habits.	
Social influence (SI)		
SI1	People who influence your behavior think that attention should be paid to information security when using e-wallets.	Venkatesh et al. (2012)
SI2	The people who are important to you (family, friends, and colleagues) think that information security should be emphasized when using e-wallets.	
SI3	Social media networks exhibit many acts of impersonation and fraud, making you pay attention to information security.	

Table 1. Observed factors and variables (cont.)

Variables	Statements	References
Privacy concern (PC)		
PC1	You are worried that e-wallets store too much security information.	Xu et al. (2013)
PC2	You are worried about having to provide information for an e-wallet.	
PC3	You are worried that your information will be leaked.	
Privacy policy (PP)		
PP1	E-wallets notify you before collecting your information.	Liu et al. (2005)
PP2	The e-wallet provides a notice of the purpose for using your information.	
PP3	The e-wallet commits to not provide information to third parties without your permission.	
PP4	E-wallets guide you on information security principles.	
Privacy trust (PT)		
PT1	You believe that the e-wallet security policy is trustworthy.	Xu et al. (2013)
PT2	You believe that your personal information will not be used by e-wallets for other purposes.	
PT3	You believe that the technology of the e-wallet application always ensures the safety of customers' personal data.	
PT4	You are completely assured when providing information on the e-wallet application.	
Behavioral intention (BI)		
BI1	You intend to start or continue using e-wallets in the near future.	Venkatesh and Davis (2000), Liu et al. (2005)
BI2	You prefer to first use the e-wallet application when you have a transaction need.	
BI3	You will recommend the e-wallet application to your family and friends.	

A 5-level Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree), was used in this study. In principle, a measurement is more precise if a scale with more rating levels, such as 7 or 9 points, is used. However, having too many rating levels often confuses respondents. For example, a Likert scale with 7 points, having two levels of 3 (partly disagree) and two levels of 5 (agree), may confuse respondents. Therefore, we decided to use a 5-level Likert scale in this study.

In addition to the group of statements representing the main variables of interest, the questionnaire includes two sections of questions to collect demographic information about the respondents: (1) demographic questions (gender, age, income, and user's education level), and (2) habits of using mobile banking applications (banking, frequency, and usage experience).

3.2. Research sample

This study uses a random sampling method to conduct the consumer survey. According to the rules of exploratory factor analysis (EFA), the sample size must be at least five times larger than the number of observed variables (Hair et al., 2010). Based on the requirements of multivariable regression analysis, the formula for calculating the minimum sample size is $n = 50 + 8 \times p$, where p is the number of latent variables (Tabachnick & Fidell, 2007). As the number of observed variables is 24 and the number of latent variables is 7, the minimum sample size according to the EFA rule is $5 \times 24 = 120$. To meet the requirements of multivariate regression analysis, the minimum sample size is $n = 50 + 8 \times 7 = 106$.

The investigation process is divided into two phases, with a preliminary survey in Phase 1 and a final survey in Phase 2. The Phase 1 survey was conducted online by sharing the survey form on social networks such as Facebook and in different groups and forums with individuals who have used e-wallets or who are potential users of e-wallets. At the end of Phase 1, we obtained 85 valid results for the preliminary analysis and evaluation of the scale, from which to calibrate the scale and eliminate inappropriate observed variables. Phase 2 was then conducted. Data were obtained in a one-month survey from October to the end of November 2022. A sample of 236 valid responses was obtained. Validity conditions (that no questions are omitted) were confirmed for these responses.

3.3. Data analysis method

The collected data were cleaned, coded, analyzed, and evaluated using SPSS AMOS 22.0. The study used the covariance-based linear structural modeling (CB-SEM) approach because the proposed research model is based on the results of previous studies. Using CB-SEM is the optimal solution. First, we used Cronbach's alpha and the total correlation coefficient to test the reliability of the scale. Cronbach's alpha provides a measure of the internal consistency of the factors (Saunders, 2007). Next, we used exploratory factor analysis to detect the convergent value (unidirectionality) of the latent factors by reducing a group of many observed variables to latent variables that still explain the data (Hair et al., 2010). The method of confirmatory factor analysis was used to test the fit of the model with the actual data and research concepts (Hair et al., 2010). After the scale was tested for suitability, we analyzed the linear structural model using the path analysis technique with a 5% significance level. Criteria for assessing the fit of the CB-SEM model were defined as in confirmatory factor analysis (chi-square/df less than 3, GFI (goodness of fit index), TLI, NFI (normed fit index), CFI (comparative fit index) greater than 0.9, and RMSEA (root mean square error of approximation) less than 0.08) (Hair et al., 2010). Finally, we used the t-test average comparison method for each group of mobile banking application users based on demographics and e-wallet usage habits, with a confidence level of 95%.

4. RESEARCH RESULTS

4.1. Reliability and validity analysis

Statistics on the demographic characteristics of the respondents, including gender, age, income, and education level, are presented in Table 2.

Table 2. Characteristics of the respondents

Characteristic	Category	Quantity	Percentage (%)
Sex	Male	112	47.5
	Female	124	52.5
	Total	236	100.0
Age	Less than 18 years old	8	3.4
	18 – 25 years old	178	75.4
	26 – 35 years old	46	19.5
	36 – 45 years old	4	1.7
	Total	236	100.0
Average monthly income	Less than 2 million dong	24	10.2
	2 – 5 million dong	26	11.0
	5 – 10 million dong	53	22.5
	10 – 15 million dong	60	25.4
	More than 15 million dong	73	30.9
	Total	236	100.0
Education level	High school	66	28.0
	Bachelor's	154	65.3
	Master's	15	6.4
	Other	1	0.4
	Total	236	100.0

Source: Compiled by authors.

The survey respondents include roughly equal numbers of males and females. The 124 female respondents account for 52.5% of the 236 respondents. There are 178 respondents in the 18-to-25 age group, accounting for 75.4%. The age group from 26 to 35 ranks second with 46 respondents. The group of those under 18 years old and the group from 36 to 45 years old only account for small percentages, 3.4% and 1.7%, respectively. Regarding average monthly income, 73 of the 236 respondents (30.9%) reported a monthly income of over 15 million VND. The group with monthly incomes from 10 to less than 15 million VND has 60 respondents, accounting for 25.4%. The third group has monthly incomes from 5 to less than 10 million VND, accounting for 22.5% of the total. The two groups with monthly incomes of less than 2 million VND and from 2 to less than 5 million VND have 24 and 26 respondents, corresponding to 10.2% and 11.0%,

respectively. The education level and age statistics are similar. The majority of the respondents said that they are at the high school level (66/236) or bachelor's degree level (154/236), corresponding to 28.0% and 65.3% of the total, respectively. A few respondents have a master's degree (6.4%) or another level of education (0.4%).

There is diversity in gender, age, income, and education level of the surveyed respondents. The following analysis results may represent different groups of the respondents. However, the difference in survey characteristics is also the reason why the research results may not be consistent with the actual situation of the groups with few survey responses.

The results of testing the reliability of the research data are presented in Table 3. Reliability analysis results show that all observed variables are greater than 0.5. The average variance extracted (AVE) is greater than 50%. The composite reliability of all factors is above 0.7. The calculation of the combined confidence and the location variance is based on the observed boundary load factor. Thus, three scales in the primary model achieve the necessary reliability and convergence.

Table 3. Scale reliability test results

Factor	Number of observed variables	Load Factor (Distribution Range)	Average Variance Extracted	Composite Reliability
Perceived privacy risk (PR)	4	0.839 – 0.897	79.50%	0.926
Information sensitivity (IS)	3	0.720 – 0.789	56.80%	0.797
Social influence (SI)	3	0.631 – 0.788	50.30%	0.751
Privacy trust (PT)	4	0.774 – 0.835	66.20%	0.887
Privacy concern (PC)	3	0.783 – 0.863	68.50%	0.867
Privacy policy (PP)	4	0.686 – 0.753	50.90%	0.806
Behavioral intention (BI)	3	0.647 – 0.787	53.20%	0.772

The study's scales were evaluated by the method of confirmatory factor analysis with the critical model.

The results of the data analysis using AMOS 22 software show the following valuable indicators: chi-square/df = 1.472 < 3, CFI = 0.965 > 0.9, TLI = 0.958 > 0.9, GFI = 0.897 < 0.9, RMSEA = 0.045 < 0.08, and PCLOSE = 0.798.

Therefore, the index chi-square/df = 1.472 is less than 3, CFI = 0.965, TLI = 0.958 are all greater than 0.9, RMSEA = 0.045 less than 0.08, except that GFI = 0.897 is less than 0.9 but greater than 0.8 and approximately reaches 0.9, accepting the threshold of 0.8 according to studies by Homburg and Baumgartner (1995) and Doll et al. (1994). The weights of each observed variable are all greater than 0.5.

The composite reliability estimate of each construct was also satisfactory, as they are above 0.700, which also indicates the reliability of all the constructs (Table 3). The study used the average variance extracted and the factor loading score as a measure of convergent validity. All the standard factor loadings were more than the required cut-off limit of 0.50. The average variance extracted of each construct was also above 0.50, which establishes convergent validity. Table 4 confirms the existence of discriminant validity and shows the distinctness of the research constructs, according to the suggestion of Nguyen et al. (2019).

Table 4. Fornell and Larcker Criterion Analysis

Construct	PR	IS	SI	PT	PC	PP	BI
Perceived privacy risk	0.892						
Information sensitivity	0.734	0.754					
Social influence	0.611	0.602	0.709				
Privacy trust	0.672	0.673	0.716	0.814			
Privacy concern	0.590	0.574	0.589	0.685	0.828		
Privacy policy	0.750	0.762	0.768	0.785	0.666	0.713	
Behavioral intention	0.730	0.706	0.732	0.729	0.701	0.720	0.729

Notes: PR–Perceived privacy risk, IS–Information sensitivity, SI–Social influence, PT–Privacy trust, PC–Privacy concern, PP–Privacy policy, BI–Behavioral intention.

4.2. Testing the research hypotheses

To test the proposed research hypotheses about the level of impact of the independent variables on the dependent variables, we use structural equation modeling (SEM) with cognitive variables of perceived privacy risk, information sensitivity, social influence, privacy trust, and behavioral intention to use e-wallets.

Table 5. Impact of the independent variables on the dependent variables

Relationship			Standardized coefficient (beta)	Standard error	Critical value	p-value	Hypothesis
PR	→	PT	-0.278	0.082	-3.207	0.001	Accept
IS	→	PT	0.377	0.13	3.831	0.000	Accept
SI	→	PT	0.174	0.187	1.683	0.092	Accept
PR	→	BI	-0.225	0.05	-2.681	0.007	Accept
IS	→	BI	0.114	0.076	1.239	0.215	Reject
SI	→	BI	0.233	0.111	2.378	0.017	Accept
PT	→	BI	0.578	0.056	6.429	0.000	Accept

Notes: PR–Perceived privacy risk, IS–Information sensitivity, SI–Social influence, PT–Privacy trust, BI–Behavioral intention.

The results of the SEM analysis of the survey data in Table 5 show that chi-square/df = 1.412 is less than 3; GFI = 0.929, CFI = 0.978, TLI = 0.973, and IFI = 0.960 are all greater than 0.9; and RMSEA = 0.042 is less than 0.05. These results show that the model is compatible with the collected data. The results of the regression coefficients on the effects of the independent variables on the dependent variables presented in Table 5 show that five relationships are statistically significant at a p-value of 0.05 and one relationship is statistically significant at a p-value of 0.1.

The privacy trust (PT) factor is influenced by three factors: perceived privacy risk (PR), information sensitivity (IS), and social influence (SI). The results show that, at a 5% significance level, the perception of privacy risk has a negative effect on trust in security, with a standardized beta coefficient of $\beta PR = -0.278$. The information sensitivity has the same effect on privacy trust, with $\beta IS = 0.377$ and a p-value of less than 0.05. The social influence factor (p-value = 0.092) has no effect on the security trust factor at the 5% level of statistical significance. It is only significant at the 10% level of statistical significance, and the beta number $\beta SI = 0.174$. The three factors of perceived privacy risk (PR), information sensitivity (IS), and social influence (SI) contribute 17.6% to the change in the security trust factor ($R^2 = 0.176$). Therefore, these findings support hypotheses H1b, H2b, and H3b.

The intention to use an e-wallet is influenced by four factors: privacy trust (PT), perceived privacy risk (PR), information sensitivity (IS), and social influence (SI). The factors of perceived privacy risk (PR), social influence (SI), and privacy trust (PT) have standardized beta coefficients of $\beta PR = -0.225$, $\beta SI = 0.233$, and $\beta PT = 0.578$, respectively. They are all significant at the 5% level (p-values are less than 0.05). Information sensitivity (IS) has no effect on the intention to use e-wallets at the 5% significance level. Perceived privacy risk (PR), social influence (SI), and privacy trust (PT) explain 51.5% of the change in the intention to use e-wallets ($R^2 = 0.515$). Therefore, hypotheses H1a, H3a, and H4 are accepted. Hypothesis H2a is rejected.

4.3. Hypothesis testing

To further clarify the role of privacy trust (PT), the study evaluates whether it interferes with the relationship between the independent variables (PR, IS, and SI) and the dependent variable (BI). The results of the analysis are presented in Table 6.

Table 6. Tests of the role of the mediating variable

Relationship	Standardized coefficient (beta)	Standard error	p-value	Hypothesis
PR → PT → BI	-0.161	0.002	0.001	Accept
IS → PT → BI	0.218	0.001	0.000	Accept
SI → PT → BI	0.101	0.090	0.092	Accept

Source: Data analysis results obtained using AMOS software.

Notes: PR–Perceived privacy risk, IS–Information sensitivity, SI–Social influence, PT–Privacy trust, BI–Behavioral intention.

Table 6 shows that the privacy trust (PT) factor acts as a mediating variable in the relationship between perceived privacy risk (PR) and the behavioral intention to use e-wallets (BI). PT also mediates the relationship between information sensitivity (IS) and the intention to use e-wallets (BI). The standardized beta coefficients are $\beta = -0.161$ and $\beta = 0.218$, respectively, at the 5% level of statistical significance. At the 10% significance level, the privacy trust factor (PT) mediates the relationship between social influence (SI) and behavioral intention to use e-wallets (BI). The standardized beta coefficient is $\beta = 0.101$. Therefore, hypotheses H1c, H2c, and H3c are accepted.

Table 7. Direct, indirect, and combined effects between three independent and dependent variables in the model

Dependent variable	Action type	PR	IS	SI	PT
PT	Direct	-0.278	0.377	0.174	-
	Indirect	-	-	-	-
	Sum	-0.278	0.377	0.174	-
BI	Direct	-0.225	-	0.233	0.578
	Indirect	-0.161	0.218	0.101	-
	Sum	-0.386	0.218	0.334	0.578

Source: Data analysis results obtained using AMOS software.

Notes: PR–Perceived privacy risk, IS–Information sensitivity, SI–Social influence, PT–Privacy trust, BI–Behavioral intention.

Table 7 summarizes the impact of factors on the intention to use e-wallets. These effects are either direct or indirect. Privacy trust (PT) has the largest direct impact on the behavioral intention to use e-wallets (BI) with $\lambda = 0.578$. The information sensitivity factor (IS) also has a direct impact on the intention to use e-wallets (BI) with $\lambda = 0.233$. Meanwhile, the social influence factor (SI) affects the behavioral intention to use e-wallets (BI) through an indirect impact with $\lambda = 0.218$. The perceived privacy risk factor (PR) has both a direct and an indirect impact on the intention to use e-wallets (BI) with $\lambda = -0.386$.

These results show that perceived privacy risk (PR), information sensitivity (IS), social influence (SI), and privacy trust (PT) have significant effects on the intention to use a digital e-wallet (BI). In order to evaluate the role of the moderating variables, privacy policy (PP) and privacy concerns (PC), in the research model and to test the remaining proposed hypotheses, the authors analyzed the impact of the moderating variables on the relationships of the proposed constructs. The results are shown in Table 8.

Table 8 shows that the privacy policy (PP) and privacy concerns (PC) modifiers affect the relationships between the independent and dependent variables. Specifically, at the 5% significance level, privacy policy (PP) has a moderating effect on the relationship between privacy trust (PT) and behavioral intention (BI) to use a digital wallet, with $\beta = 0.0978$. Privacy concerns (PC) has a moderating effect on the relationship between information sensitivity (IS), social influence (SI), and privacy trust (PT) on the intention

to use an e-wallet with beta coefficients of β = 0.2377, 0.1409, and 0.2060, respectively. Privacy policy (PP) and privacy concerns (PC) have no impact on the other relationships. Therefore, hypotheses H5d, H6b, H6c, and H6d are accepted. Hypotheses H5a, H5b, H5c, and H6a are rejected.

Table 8. Impact of the moderating variables on the research model

Relationship			Beta coefficient	Standard error	p-value	Hypothesis
PR_PP	→	BI	-0.0035	0.0548	0.9630	Reject
IS_PP	→	BI	0.0331	0.0544	0.5435	Reject
SI_PP	→	BI	0.0171	0.0600	0.7755	Reject
PT_PP	→	BI	0.0978	0.0483	0.0440	Accept
PR_PC	→	BI	0.0323	0.0737	0.6611	Reject
IS_PC	→	BI	0.2377	0.0558	0.0000	Accept
SI_PC	→	BI	0.1409	0.0586	0.0171	Accept
PT_PC	→	BI	0.2060	0.0613	0.0009	Accept

Source: Results of data analysis with SPSS software.

Notes: [Independent variable] _PP, [Independent variable] _PC: Impact of the moderating variable PP, PC on the relationship of [Independent variable] => [Dependent variable BI].

To assess the difference in the intention to use e-wallets based on the categorical variables, the study used the t-test and the analysis of variance (ANOVA) method for different groups of the survey respondents.

For demographic variables, by gender, there are two groups of Male and Female. By age, there are four groups: From 18 years old and above; From 18 to 25 years old; From 26 to 35 years old; From 36 - 45 years old and Over 45 years old. By income, there are five groups: Under 2 million; From 2 to under 5 million; From 5 to under 10 million; From 10 to under 15 million and Over 15 million. By educational level, there are four groups: High school; Bachelor; Master and other.

The six e-wallet application usage groups are Momo, Zalopay, Shopee Pay, Moca, Money Wallet, Payoo Wallet, and other. The six groups by frequency of use are daily, weekly, monthly, from 1 to 3 months, unused, and others.

The results of evaluating the differences between the categorical variables in the intention to use e-wallets are presented in Table 9.

The t-test and analysis of variance results show no difference in the intention to use e-wallets between the survey categories of gender, education level, and frequency of e-wallet use. However, there are differences among the group of application users by age and average monthly income. All groups have a high tendency to use e-wallets. The age group with the largest average value (4.0833) is the one between the ages of 36 and 45. In terms of average monthly income, the group with incomes over 15 million VND has

the highest average value (3.9132). The group with the lowest average value is the group with incomes below 2 million VND (mean = 3.4722).

Table 9. Differences in the intention to use e-wallets by categorical variable

Criterion	Type of inspection	Levene's test	Independent sample t-test	Noticeable difference
		p-value	p-value	
Sex	t-test inspection	0.380	0.234	No
Age	Analysis of variance	0.027	0.028	Yes
Education level	Analysis of variance	0.466	0.896	No
Average monthly income	Analysis of variance	0.378	0.029	Yes
Frequency of using e-wallet apps	Analysis of variance	0.181	0.253	No

Source: Data analysis using SPSS AMOS software.

5. DISCUSSION

The study shows that all factors have a direct, indirect, or aggregate impact on the intention to use e-wallets. Trust in security has the greatest aggregate influence on the intention to use e-wallets, which is followed by the perceived privacy risk, social influence, and information sensitivity factors. The study also points out the role of mediating variables, which moderate the relationships between the independent and dependent variables.

Privacy trust is affected by the three factors of perceived privacy risk, information sensitivity, and social influence. Information sensitivity and social influence have a positive impact on trust in data security. This result is contrary to the results of the study on the relationship of security and trust with behavioral intention in e-commerce by Liu et al. (2005). In our study, the elements constituting the security of personal data are a prerequisite for building trust. Data security helps customers understand how online transactions take place, thereby building trust in the service. Bansal et al. (2010) argued that the more sensitive the information, the more negative its influence on consumer intentions to disclose personal data. Chaouali et al. (2016) and Jiwasiddi et al. (2019) found that social influence has a negative influence on attitudes toward using technology products and services. Contradictory results from this study can be explained by the research context and the characteristics of the respondents who participated in the survey. Currently, Vietnamese consumers, especially those in younger generations, understand the problems that can occur when disclosing confidential information. As consumers become more concerned about security risks, they will be less likely to use e-wallet applications due to a lack of trust. Consumers are also increasingly concerned about personal information that may be exposed and its social impact. Compared to the convenience of time and the process of using e-wallets, this problem cannot be taken lightly. Many people think that paying with cash or going to banks can be riskier, leading to more trust in the security of e-wallet applications.

This study shows that perceived privacy risk, information sensitivity, social influence, and privacy trust have a significant impact on consumer intentions to use e-wallets. Trust in e-wallet security has the greatest and most direct impact on the intention to use e-wallets, which is in line with the findings of Liu et al. (2005) on the positive impact of trust on the intention to use e-wallets. Privacy trust is an intermediary factor in the relationship between the intention to use e-wallets and the other independent variables. Perceived privacy risk has both direct and indirect effects on the intention to use e-wallets. Both impact coefficients are negative, indicating a negative relationship between the two factors. This result is in line with the expectations of this and previous studies. Information sensitivity and social influence are positively related to the intention to use e-wallets. This result is in contrast to the study of factors affecting information disclosure behavior on social networks by Xu et al. (2013), who found that high sensitivity of information heightens concerns about security, thereby making users afraid to disclose information. The reason for this contradiction may be due to the way of thinking. When e-wallets require more sensitive information and more acts of property fraud occur, consumers expect that e-wallet applications will bring higher security. The improved e-wallet applications will give priority to using e-wallets. Information sensitivity does not have a direct impact on the intention to use e-wallets. Perhaps consumers feel that it is normal and appropriate to provide this personal information. With the rapid development of technology and fierce market competition, e-wallet applications designed to attract customers must strengthen consumer confidence.

6. IMPLICATIONS

6.1. Theoretical implications

Firstly, the study systematizes the theories related to data security and its influence on the intention to use e-wallet applications. In addition, the theoretical basis of e-wallet applications and the intention to use them are summarized in this study.

Secondly, the study provides evidence on appropriate factors for data security in accordance with the research context in a transitional economy such as Vietnam. The factors constituting data security include (1) perceived privacy risk, (2) information sensitivity, and (3) social influence.

Thirdly, this study summarizes previous studies, seeks to learn from their achievements, and identifies limitations. This contributes to the theoretical basis for further research to expand this study's findings. The research results show the level of impact of the security factors and reveal various causes that differ from those of previous studies. The context of the Vietnamese economy can explain these differences.

Next, this study highlights the moderating role of privacy concerns and privacy policies in managing e-wallets.

Finally, this study suggests a theoretical framework to analyze the effects of data security factors on the intention to use e-wallets. It also points out limitations for future studies to improve and overcome these limitations.

6.2. Practical implications

This study has determined the impact of security factors on consumer intentions to use e-wallets. Firstly, customers should actively learn about the security policies of banks and relevant laws. For example, customers should understand the terms and conditions posted on the homepage of the e-wallets they intend to use. Customer investigations may include data collection and the search for privacy policies, the responsibilities of the parties involved, and a feedback and complaint mechanism if a violation is detected. Customers should actively learn and acquire knowledge and security principles to use e-wallets, as many e-wallet applications post customer instructions with detailed information on security principles. Fraudulent acts will occur from time to time and depend on different e-wallet brands. Consumers should improve their general security knowledge and follow instructions to update the appropriate software. Secondly, consumers should regularly monitor news related to information security issues. The first step is to grasp the fundamentals of data security. The behavior of financial criminals is changing and becoming more sophisticated. Therefore, consumers need to regularly follow news on official websites to stay updated. Customers need to be alert and learn from their own experiences. In addition, they must constantly listen to recommendations from experts in the cybersecurity industry, from e-wallet documentation, and from government agencies. Moreover, state management agencies should inspect and review the security systems and policies of e-wallet providers more regularly. The coordination mechanism among line ministries and agencies should be streamlined to ensure proper network security. Organizations that provide e-wallets should have a public, clear, and easy-to-understand privacy policy. In addition, it is necessary to build a reasonable information collection system, increase investment in research, upgrade the information security system, increase training, improve the quality of human resources, and promote propaganda to increase customer confidence in security. Finally, to ensure privacy when using e-wallets, the government should regulate e-commerce transactions and e-payments. Otherwise, businesses need to be clearly aware of suspicious transactions in order to monitor and detect early signs of fraud.

7. LIMITATIONS AND AREAS FOR FURTHER RESEARCH

The study has some limitations that need to be addressed in future studies. Firstly, the surveyed respondents were mainly university students. Students have a high demand to use e-wallet applications. The statistics are, however, limited in terms of age, industry, income levels, and e-wallet applications. Therefore, we have not been able to compare security levels across e-wallets to know which one is performing best. Secondly, the intention to use e-wallets has not been explained in detail in this study. The focus of the study is on the impact of security factors rather than generalizing other positive factors that affect consumer intentions to use e-wallets, such as perceived usefulness, ease of use, or perceived enjoyment. Moreover, using e-wallet applications has gradually become an inevitable habit and a trend in the daily lives of most young consumers. All of the above conditions reduce the role of privacy factors in influencing the intention to use e-wallets. Future studies should investigate the impact of security factors on the satisfaction and loyalty of users. Thirdly, because the survey time was relatively short and the sample size

was small, no comparison over time was possible. Future studies should conduct surveys with larger sample sizes in different areas and over different time intervals. It will then be possible to draw more comprehensive and complete conclusions about the use and security status of mobile banking applications.

REFERENCES

Aladwani, A. M. (2001). Online banking: A field study of drivers, development challenges, and expectations. *International Journal of Information Management*, *21*(3), 213-225. https://doi.org/10.1016/S0268-4012(01)00011-1

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, *30*(1), 13-28. https://doi.org/10.2307/25148715

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138-150. https://doi.org/10.1016/j.dss.2010.01.010

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3-4), 245-270. https://doi.org/10.1016/S0963-8687(02)00018-5

Bestavros, A. (2000). Banking industry walks 'tight rope' in personalization of web services. *Bank Systems & Technology*, *37*, 54-56.

Bui, N. V. (2021). Factors affecting consumer's intention to use e-wallets in Can Tho City: Application of partial least squares structural equation modeling (PLS-SEM). *Can Tho University Journal of Science*, *57*(5), 242-258. https://doi.org/10.22144/ctu.jvn.2021.162

Bui, N. V., & Ha, N. K. G. (2020). The impact of perceived brand globalness on consumers' purchase intention and the moderating role of consumer ethnocentrism: An evidence from Vietnam. *Journal of International Consumer Marketing*, *32*(1), 47-68. https://doi.org/10.1080/08961530.2019.1619115

Campbell, A. J. (1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Direct Marketing, 11*(3), 44-57.

Chaouali, W., Yahia, I. B., & Souiden, N. (2016). The interplay of counter-conformity motivation, social influence, and trust in customers' intention to adopt Internet banking services: The case of an emerging country. *Journal of Retailing and Consumer Services*, *28*(1), 209-218. https://doi.org/10.1016/j.jretconser.2015.10.007

Chính phủ. (2013). *Nghị định 52/2013/NĐ-CP* (Decree 52/2013/ND-CP). https://thuvienphapluat.vn/van-ban/Thuong-mai/Nghi-dinh-52-2013-ND-CP-thuong-mai-dien-tu-187901.aspx

Chong, A. Y.-L., Ooi, K.-B., Lin, B., & Tan, B. I. (2010). Online banking adoption: An empirical analysis. *International Journal of Bank Marketing*, *28*(4), 267-287. https://doi.org/10.1108/02652321011054963

Cisco. (2021). *Building consumer confidence through transparency and control*. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf (Accessed 24 January 2023).

Clay, K., & Strauss, R. P. (2000). Trust, risk and electronic commerce: Nineteenth century lessons for the twenty-first century. *Proceedings of the 93rd Annual Conference on Taxation, Santa Fe, November 9-11, 2000*, 53-63.

Cục Thương mại điện tử và Kinh tế số (Department of E-commerce and Digital Economy). (2021). *Sách trắng thương mại điện tử 2021*. Bộ Công Thương.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323-342. https://doi.org/10.1111/1540-4560.00067

Diana, R. A., Yonelinas, A. P., & Ranganath, C. (2008). The effects of unitization on familiarity-based source memory: Testing a behavioral prediction derived from neuroimaging data. *Journal of Experimental Psychology: Learning, Memory, and Cognition, 34*(4), 730-740. https://doi.org/10.1037/0278-7393.34.4.730.

Doll, W. J., Xia, W., & Torkzadeh, G. (1994). A confirmatory factor analysis of the end-user computing satisfaction instrument. *MIS Quarterly, 18*(4), 453-461. https://doi.org/10.2307/249524

Donaldson, T., & Dunfee, T. W. (1994). Toward a unified conception of business ethics: Integrative social contracts theory. *Academy of Management Review, 19*(2), 252-284. https://doi.org/10.2307/258705

EU. (2016). *General Data Protection Regulation*. https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html#:~:text=Regulation%20(EU)%202016%2F679%20of%20the%20European%20Parliament%20and,(OJ%20L%20119%2C%204.5. (Accessed 26 February 2021).

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451-474. https://doi.org/10.1016/S1071-5819(03)00111-3

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research.* Addison-Wesley.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management & Data Systems*, *106*(5), 601-620. https://doi.org/10.1108/02635570610666403

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. https://doi.org/10.2307/3151312

Furnell, S. M., & Karweni, T. (1999). Security implications of electronic commerce: A survey of consumers and businesses. *Internet Research*, *9*(5), 372-382. https://doi.org/10.1108/10662249910297778

Hair, Jr., J. F., Black, W., Babin, B., Anderson, R., Tatham, R., & Black, W. (2010). *Multivariate Data Analysis* (7th ed.). Prentice-Hall International.

Homburg, C., & Baumgartner, H. (1995). Beurteilung von kausalmodellen: Bestandsaufnahme und anwendungsempfehlungen. *Marketing Zeitschrift für Forschung und Praxis*, *17*(3), 162-176. https://doi.org/10.15358/0344-1369-1995-3-162

Hosmer, L. T. (1995). Trust: The connecting link between organizational theory and philosophical ethics. *Academy of Management Review*, *20*(2), 379-403. https://doi.org/10.2307/258851

Hughes, A. M. (1996). *The complete database marketer: Second-generation strategies and techniques for tapping the power of your customer database*. McGraw-Hill.

Jackson, R., & Wang, P. (1994). *Strategic database marketing.* McGraw-Hill.

Jiwasiddi, A., Adhikara, C. T., Adam, M. R. R., & Triana, I. (2019). Attitude toward using Fintech among millennials. *Proceedings of the 1st Workshop on Multimedia Education, Learning, Assessment and its Implementation in Game and Gamification in Conjunction with COMDEV 2018, Medan Indonesia, 26 January 2019.* https://doi.org/10.4108/eai.26-1-2019.2283199

Kalakota, R., & Whinston, A. B. (1997). *Electronic commerce: A manager's guide*. Addison-Wesley.

Kini, A., & Choobineh, J. (1998). Trust in electronic commerce: Definition and theoretical considerations. *Proceedings of the Thirty-First Hawaii International Conference on System Sciences*, *4*, 51-61.

Lee, M. K. O., & Turban, E. (2001). A trust model for consumer internet shopping. *International Journal of Electronic Commerce*, *6*(1), 75-91. https://doi.org/10.1080/10864415.2001.11044227

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern – A privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*(2), 289-304. https://doi.org/10.1016/j.im.2004.01.003

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355. https://doi.org/10.1287/isre.1040.0032

Mayer, R. E. (2005). Principles of multimedia learning based on social cues: Personalization, voice, and image principles. In R. E. Mayer (Ed.), *The Cambridge handbook of multimedia learning* (pp. 201-212). Cambridge University Press. https://doi.org/10.1017/CBO9780511816819.014

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, *38*(12), 65-74. https://doi.org/10.1145/219663.219683

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15-29. https://doi.org/10.1002/dir.20009

Nguyen, T. P. T., Nguyen, V. A., & Pham, T. T. A. (2019). Impact of corporate social responsibility on reputation, trust, loyalty of the customers in the banking sector – Evidence in Dalat city. *VNUHCM Journal of Economics, Business and Law*, *3*(3), 220-235. https://doi.org/10.32508/stdjelm.v3i3.562

Nowak, G. J., & Phelps, J. E. (1992). Understanding privacy concerns: An assessment of customers' information-related knowledge and beliefs. *Journal of Direct Marketing*, *6*(4), 28-39. https://doi.org/10.1002/dir.4000060407

Peppers, D., & Rogers, M. (1993, August 22). Viewpoints: Viewer privacy in the interactive age. *New York Times*.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27-41. https://doi.org/10.1509/jppm.19.1.27.16941

Quốc hội. (2005). *Luật Giao dịch điện tử* (Law on Electronic Transaction). https://vanban.chinhphu.vn/default.aspx?pageid=27160&docid=29675

Quốc hội. (2006). *Luật Công nghệ thông tin* (Law on Information Technology). https://chinhphu.vn/default.aspx?pageid=27160&docid=29137

Quốc hội. (2013). *Hiến pháp* (Constitution). https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Hien-phap-nam-2013-215627.aspx

Quốc hội. (2015). *Luật An toàn thông tin mạng* (Cyberinformation Security Law). https://vanban.chinhphu.vn/default.aspx?pageid=27160&docid=183196

Saunders, C. (2007). Using social network analysis to explore social movements: A relational approach. *Social Movement Studies*, *6*(3), 227-243. https://doi.org/10.1080/14742830701777769

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, *19*(1), 62-73. https://doi.org/10.1509/jppm.19.1.62.16949

Tabachnick, B. G., & Fidell, L. S. (2007). *Experimental designs using ANOVA*. Thomson/Brooks/Cole.

Tu, C. Z., Yuan, Y., Archer, N., & Connelly, C. E. (2018). Strategic value alignment for information security management: A critical success factor analysis. *Information and Computer Security*, *26*(2), 150-170. https://doi.org/10.1108/ICS-06-2017-0042

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 186-204. https://doi.org/10.1287/mnsc.46.2.186.11926.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425-478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157-178. https://doi.org/10.2307/41410412

Watson, Jr., T. J. (1968). The considerations of data security in a computer environment. *IBM Journal of Research and Development*, *4*(5), 9432.

Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. *Electronic Commerce Research*, *13*(2), 151-168. https://doi.org/10.1007/s10660-013-9111-6

Yang, J., & Papazoglou, M. P. (2000). Interoperation support for electronic business. *Communications of the ACM*, *43*(6), 39-47. https://doi.org/10.1145/336460.336473

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *40*(1), 38-51. https://doi.org/10.1145/1496930.1496937

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2003). A proposed model of e-trust for electronic banking. *Technovation*, *23*(11), 847-860. https://doi.org/10.1016/S0166-4972(03)00130-5

Yousafzai, S. Y., Pallister, J. G. & Foxall, G. R. (2005). Strategies for building and communicating trust in electronic banking: A field experiment. *Psychology & Marketing*, *22*(2), 181-201. https://doi.org/10.1002/mar.20054