A Structural Equation Model of Factors Influencing New Graduates' Privacy Data Protection Behaviors on Electronic Transactions

Theerasak Ponepan[1], Saran Pimthong[2] and Kanchana Pattrawiwat[3]
Major of Applied Behavioral Science Research,
Behavioral Science Research Institute, Srinakharinwirot University, Thailand
Email: [1]theerasak.ponepan@g.swu.ac.th; [2]saranpimthong@gmail.com

Received May 19, 2022; **Revised** June 2, 2022; **Accepted** August 20, 2022

Abstract

This study aimed to test and develop a structural equation model of the factors influencing personal data protection behaviors in new graduates during electronic transactions. The participants were 418 first-time jobbers living in Bangkok and Perimeter areas. Two-stage cluster sampling was applied to randomize the sample group within the administrative zoning. The theoretical foundations of current study was Protection Motivation Theory and an expanded Technology Acceptance Model. The data were collected using twelve constructs of reliable and valid questionnaires, with alpha coefficients ranging from 0.72 to 0.85. The results showed that the developed structural equation model was well consistent with the empirical data, as measured by the goodness of fit indices: χ^2 = 684.99, df = 173, p-value < 0.01, RMSEA = 0.075, SRMR = 0.055, NNFI = 0.96, CFI = 0.97 and GFI = 0.90. The findings revealed that intention had a direct effect on privacy data protection behaviors, while perceived vulnerability, self-efficacy, and subjective norms had the positive indirect effects on privacy data protection behaviors respectively. As a result, before entering social work, education institutes and lecturers should have more practice classes and raise awareness about protecting personal data and digital citizenship security.

Keywords: new graduates; structural equation model; privacy data protection behaviors; electronic transactions

Introduction

Nowadays, advancements in communication technology via the internet have influenced an individual's daily life in a large society. It is commonly used for communication and interaction, such as online conversations, meetings, online shopping, or electronic commerce (e-Commerce), which eliminates the need to visit shopping malls (Aghaei et al., 2012). Thailand's financial institutions and banks (2018) have adapted to support electronic transactions (e-Transactions), electronic exchange of values channels for retail customers are as follows internet banking and mobile banking, including the service of transactions with electronic money (e-Money) both in the form of electronic money cards and payment that are not cards or electronic wallets (e-Wallet) and clearing services. It has grown in importance in international business, and it includes the purchase and sale of goods or services over the internet. As a result, this will help to reduce service costs while also increasing customer convenience.

According to the Financial Consumer Protection Center, Bank of Thailand (2019), a research to investigate internet users' ages, it was found that the use of internet services among people aged between 21 and 29 years old increased by 88 percent when compared to other age groups. They started to purchase products based on social media trends and thus, the risk of personal data breaches among certain age groups was increasing. Furthermore, the data from international research reports (Ernst, 2015; Feng & Xie, 2014) informed that among adolescents aged 20-29, the disclosure of personal information was accountable for 90% while 60% were victims of personal information espionage; by disclosing electronic financial and payment details, the internet users were risk of impersonating for benefits using personal information and financial attacks. Accordingly, personal information is inseparable from personal property. Furthermore, since personal information such as ID card numbers, credit card numbers, bank accounts, telephone numbers, date of birth, etc. are considered valuable assets, data breach may cause problems. For example, identity theft could be detected as a crime regarding financial information. Selling personal data to third parties may result in third-party marketing or political interests (Smith & Lias, 2005). The reports from researches mentioned previously are obtained from a study regarding the theft of personal information for e-Transactions. The findings discovered that the victims were generation Y who were online consumers, and also indicated that the victims who were college students did not prioritize private data protection. The reasons responsible for the issue might be a lack of understanding of personal information protection. Also, there is a scarcity of knowledge and public relations personnel in the field of cyber threats to e-Transactions.

Thus, as a lecturer of subjects related to applied computers derived from the aforementioned problems, the researcher decided to conduct a current study. Furthermore, students will be educated on how to save money on e-transactions and how to use computer programs, there should be the computer and cyber security courses to protect personal information and understand how the personal data are produced when they are learning online. To investigate the factors influencing personal data protection behavior on e-Transactions in first jobbers, the structural equation model is applied. The data from this study is used as a tool to educate new graduates on their real world situation. Furthermore, there is a privacy policy in Thailand that requires the disclosure of data prior to e-Transactions service. Though disclosure of personal information is critical in many countries, websites and applications require personal information protection policies to be notified legally (Freiherr & Zeiter, 2016). The measures to prevent and recognize the problem regarding personal data protection are available so that the right to privacy can be protected while personal information is used for exploitation in various forms and when it is stored in a computer system or e-document. As Thai society is transitioning to a cashless society which result in less cash payment and changed forms of payment (Bank of Thailand, 2018), and due to the outbreak of coronavirus disease 2019 (COVID-19) reported and managed by World Health Organization, the campaign was launched to reduce the use of cash, notes, and coins as a medium to prevent from infectious diseases. Thus, it is critical to promote and instill in students an understanding of and reliance on safeguarding strategies of personal information protection while using e-Transaction services.

Research Objectives

To test and develop a structural equation model of the factors influencing personal data protection behaviors on electronics transactions.

Scope of Research

Research and content scope: This study focuses on the Protection Motivation Theory and an expanded Technology Acceptance Model based.

Population and area Scope: The first jobbers aged between 20-29 years old of company employees in Bangkok and perimeter areas. The samples covered 418 first jobbers from Bangkok, Nonthaburi and Pathumthani province used two-stage cluster sampling.

Timing Scope: During August to November 2021.

Literature Review and Theoretical Background

Privacy Data Protection Behaviors (PDPB)

Data privacy and privacy information management in the ethical issues of the information age is the basic concept of personal data protection. The concerns of information privacy have arisen among Americans since the use of personal information in organizations (Smith et al., 1996). Milne and Culnan (2004) defined consumer online privacy protection as the method to avoid the damage and theft of personal and financial information from electronic devices. In the digital age these days, information technology becomes more crucial and impacts most everyone's daily life. And due to the emergence of advanced technology especially e-transaction services which grow in popularity, personal data becomes more vulnerable to threats. Though e-Transaction is fast and convenient, potential threats can arise since the disclosure of users information is required in order to access the service (Chellappa, & Sin, 2005). According to a study by Diamond & Vartiainen (2007) to investigate the use of behavioral economics to synthesize theoretical data used in current study, behavioral economics refers to a study of factors that affect an individual in decision making. There are a variety of factors, including emotions, feelings, experiences, and biases that influence persons in their decision making. For example, health behavior economics believes that regular exercise and eating vegetarian lead to better health in the future; the person might perceive this message but decide not to follow healthy behavior practices. As a result, it is important to study behavioral economics concepts in order to understand people's long-term behavioral, motivational changes, and sustainable behavior.

This study employed Protection Motivation Theory (PMT) to determine an individual's motivation and perceived risk exposure. The finding will lead to the principles of safeguarding personal information during e-Transaction processes. In addition, Buchanan et al.(2007) divided the components of privacy protection from e-commerce into two categories: 1) general caution (GEN) practice and 2) technical protection (TECH). General caution refers to the observance of regulations in accordance with the general personal data protection principle, and the examples are password protection, non-disclosure of personal data in social media, always logging out when finished, reading the privacy policy, and license agreement related to privacy data (Paine et al., 2007). Meanwhile, technical protection are, for example, opting out of online marketing, deleting internet cookies, clearing the browser history, jailbreaking or rooting the operating system, applying two-factor authentication, and e-mail setting (Ernst, 2015).

Protection Motivation Theory (PMT)

PMT proposed by Rogers (1983) investigates the processes of inducing fear and the stimulation attitude. The interaction theory of the Health Belief Model (Rosenstock, 1974) and Bandura's Self-Efficacy Theory (1977) are also considered. The two models stated that communication could frighten them and influence their thoughts and behavior. A person would have two cognitive responses once he or she was given negative or malicious information namely threat appraisal and coping appraisal, both of which could lead to irrational adjustments. According to PMT, (Rogers, 1983; Plotnikoff et al., 2010) threat appraisal is defined as Perceived Vulnerability (VUL) and Perceived Severity (SEV). The coping appraisal is built around three key constructs namely Response Efficacy (RES), Self-efficacy (SEL) and Response cost (COST) are as follows. VUL indicated that it is the discussion of the perception of disease risk or a person's belief about the tendency of having a disease. If the risk of a missed opportunity influences your behavior, it implies that the risk awareness practice motivates your intention. According to Malhotra et al. (2004) defined risk awareness of users' personal information, violation without permission from e-Transactions service providers and perceived security risks that the users may experience as a result of the computer system while using the services (VUL1). Furthermore, users who use applications believe they are at risk of being violated by bugs or failure in the system. They also explain that they feel insecure and are concerned about the issues seems to be even frightful (VUL2). SEV, the study regarding beliefs in information and data protection behavior is a signal that alerts people to potential threats, injuries, or life-threatening situations. Lee & Larsen (2009) stated that users are vulnerable to violation caused by data insecurity. The drawback of failure in personal information protection systems are damage caused to a person or potential loss such as money or not being able to access e-Transactions (SEV1) due to the invasion conducted by external entities who breach the owner’s privacy. The perceptions of the severity of the potential risks may occur to the individual (SEV2) (Boerman et al., 2021). RES is the outcome of personal expectations when complying with the recommendations to reduce potential threats and risks in the form of information specific news and practical guidelines. It implied that people who assist in understanding tend to change their behaviors and are more open to practical suggestions. According to Ng et al. (2009) was found that the perceptions of the individuals following procedures, regulations, or manuals should be addressed by personal information. Furthermore, computer knowledge and professional compliance expectations from the general suggestion (RES1) and the advanced method according to the recommended practice (RES2) are mentioned in study conducted by Yoon et al. (2012). Lastly, SEL, which is a belief in one's ability to follow instructions and produce the expected results. According to Compeau & Higgins (1995) and Chen & Chen (2015) defined self-efficacy in information security as an individual's belief and capability on computer self-efficacy with the intention to protect privacy when using applications (SEL1). The expectation of one's competence in information security based on computer skills and e-Transactions experience, security breach incidents that prepare you to deal with or face threats (SEL2), and general controllability all relate to a person's perception of control over potential e-Transactions threats (SEL3). Response cost (COST), this factor emphasizes the received opportunity costs by an individual in performing a recommended coping behavior in terms of monetary (COST1) and time with effort expended (COST2) (Ifinedo, 2012). According to PMT, COST decreases an individual's intention to practice a coping response.

Thus, this study proposes the hypothesis as follow: Hypothesis 1 to 4 (H1-4): VUL, SEV, RES, and SEL will have a positive effect on behavioral intention (BI) to protect personal information. Hypothesis 5 (H5): COST will have a negative effect on BI to protect personal information

Technology Acceptance Model (TAM)

Davis et al. (1989) proposed the TAM to describe technology user behavior in terms of predicting technology adoption; there are five key constructs: perceived usefulness (PU), perceived ease of use (PEOU), attitude toward using, behavioral intention (BI), and actual system use. It is founded on the Stimulus-Organism-Response (SOR) model. Mehrabian and Russell (1974) developed a model concept based on environmental psychology for assessing perceptions from the individual's internal systems that are related to the user's motivation to use a system and actual system use. The researchers used the TAM concept to synthesize the causal variables and apply them to personal data protection behaviors. It is made up of the following five variables: 1) System Characteristics (SYS), Yao and Linz, (2008) informs a person's perception and opinion of the features, managing the manual setup of personal information in financial transactions, and controlling the disclosure of personal information to be secure on a computer program. It was influenced by the perceived ease and usefulness of personal information protection divided features of the program such as data set speed, access levels, and personal data verification (SYS1). Furthermore, an interesting user interface related to interesting expressions in symbolic graphics, using simple explanations and vocabulary, colors, and appropriate letter design (SYS2) (Büchi et al., 2017). 2) Subjective Norms (SN), this study employed the subjective norm concept (Fishbein & Ajzen, 1975) to examine social influenced by the opinions of family members, relatives, close friends, colleagues, and supervisors regarding the same issues from advice, solicitation, and discussion to manage personal data settings (SN1). Furthermore, the influence from people who are expertise in technology known as IT Bloggers may become influencers to share the significant benefits and to support personal information settings management (SN2). 3) PU have developed and improved Davis's method (1989), the components are divided into two categories: generating benefits or being useful to yourself (PU1) and increasing productivity in personal information security (PU2). 4) PEOU, the perception of methods and instructions to manage personal information protection settings are based on the methods proposed by Venkatesh & Davis (1996). The study divided the perception of the perceived ease of management of personal data protection settings on e-Transactions into two aspects: easy to learn (PEOU1) and simplicity in personal data protection settings management method (PEOU2) and 5) Attitude (ATT) in term employed by Fishbein & Ajzen (1975) to make predictions of the actual behavior expressed by an individual. This study is divided into two parts regarding attitudes toward personal data protection on e-Transactions: behavioral belief (ATT1) and evaluation of outcomes after managing personal information protection settings (ATT2).

Thus, this study proposes the hypothesis as follow: Hypothesis 6 to 7 (H6-7), SYS will have a positive effect on POEU and PU in setting and protecting personal information. H8, SN will have a positive effect on PU in setting and protecting personal information. H9, PU will have a positive effect on ATT and H10, PU will have a positive effect on behavioral intention (BI) to protect personal information. H11, PEOU will have a positive effect PU and H12, PEOU will have a positive effect on ATT to setting and protecting personal information. H13, ATT will have a positive effect on BI to protect information. Moreover, Behavioral Intention (BI) to PDPB on e-Transactions. In this study, the expression of intention, effort, commitment, readiness, and willingness to practice in accordance with the personal data settings management with the aim to contribute to changes and to convey their behavior are referred to as the intention to protect personal data. Thus, the hypothesis proposed for this study was Hypothesis 14 (H14): BI will have a positive effect on PDPB.

Research Methodology

Instruments

The study was conducted according to the guidelines of the Declaration of Helsinki, the Belmont Report, and the International Conference on Harmonization in Good Clinical Practice (ICH-GCP), approved by the Ethics Committee of Srinakharinwirot University (protocol number SWUEC-G-299/2563X)

A research tool employed in the current study for data collection were questionnaires. Observed variables for each latent variable were used to construct survey questions: PMT (Ifinedo, 2012; Park & Lee, 2014) is the primary measurement tool developed from the motivations for online privacy protection behavior. Meanwhile, TAM is used based on studies of Venkatesh & Davis (2000) to predict user behavior while using information systems, and PDPB employed a measurement tool proposed by Buchanan et al. (2006) to assess online privacy concerns and protection while using the services available on e-commerce. There are three sections in the survey questionnaire. The first section consists of demographic data. The summated rating scale was included in the second section where the participants would be required to provide answers related to PDPB on e-Transactions. There are six rating scales ranging from "most true" (6) to "not at all true" (1), with negative statements indicating opposite characteristics. The final section, their opinions and attitudes consists of eleven sets of determinant factors influencing personal data protection behavior. Six scales summated ranging is also included in this section as followed the content, issues and structures related to the theory of motivation and technology acceptance model.

The content validity was examined by three professors from Srinakharinwirot University's Behavioral Science Research Institute and three experts from the Department of Information Technology to verify the appropriateness of the test items. The Index of Item-Objective Congruence (IOC) introduced by Rovinelli and Hambleton (1976) was used in this study, and the criteria for the question item was 0.60 or above. The recommendations after revision by the experts were used to revise and supplement the contents of some measurement questions, and the overall questionnaire compositions for each observed variable were determined. Furthermore, to calculate a preliminary survey for reliability tests for each of the scales, Cronbach's alpha coefficient was applied. Nunnally's (1994) criteria confirmed that the Cronbach's alpha coefficient employed to the test item was 0.70 or above. The results from 100 respondents during the trial session, and alpha coefficient is calculated using the SPSS program for Windows to confirm the reliability of the measuring tool and reliability test results. The findings revealed in alpha coefficients range from 0.723 to 0.854, with a total alpha coefficient of 0.941. There are a total 182 items in the questionnaire.

Data collection and analysis

The data were collected using a postal survey and online survey where possible concurrently. The participants aged between 20 to 29 years old of company employee and the participants who use e-Transaction service more than 5 times per month during the past six months were selected. The subject of this study is the first jobber in Bangkok and vicinity areas with rising number of mobile payment users (Bank of Thailand, 2018), who live in administrative zoning including Nonthaburi and Pathumthani province were selected randomly using two-stage cluster sampling the survey was conducted from August to November 2021. After sorting out the incomplete questionnaires, a total of 418 participants responded and returned the questionnaire with complete answers. In factor analysis, sample size criteria (Hair et al., 2010) were used to calculate the sample size of 15-20 times per one observed variable. This study focused on twenty-four observation variables; as a result, the parameter is appropriate for measurement and the Structural Equation Model (SEM) technique. The LISREL program is applied for data analysis to obtain descriptive statistics, construct validity testing, skewness and kurtosis from a test of univariate normality for continuous variables (Jöreskog et al., 2016). Finally, all data analyses were statistically significant with the level of 0.05 in this study.

Results

Demographic characteristics

The summary of the demographic profile, the average age of respondents was 25.33 years old. Regarding gender, the majority of participants were female (61.00%), followed by male (31.10%), and LGBT (7.90%) respectively. The majority of respondents completed a bachelor’s degree (89.20%) and the respondents reported that they used e-Transactions services more than

15 times per month. In terms of marital status, the majority of respondents was single (75.60%), and most of the participants resided and worked in Bangkok (62.92%).

Measurement Model

Hair et al. (2010) encouraged the measurement model for each latent variable related to the set of observed variables to be assessed. The validity of the structural relationship model between the latent variables was also confirmed as well as the convergent validity and discriminant validity of the measurement model; they all satisfied each criterion and they are considered appropriate for measurement. Factor loadings (λ) with first order confirmatory factor analysis (CFA) is employed to determine the internal consistency reliability and to examine the quality of the questionnaire or measuring item. Meanwhile, formula Fornell and Larcker (1981) of composite reliability (CR) and Average Variance Extracted (AVE) in Microsoft Excel is used for calculation. Based on the criteria introduced by Jöreskog et al., (2016), the CR was 0.70 or above and the AVE was 0.50 or above. This study applied the LISREL program to examine the relationship between latent variables and the model's set observation variables using the model's goodness of fit index method (Kline, 2015), where the outcome was not statistically significant (p-value > 0.05) as shown in chi-square test (χ^2). In addition, the model adjustments were made by removing each item with a small number of factor loading values until the model conforms to the goodness fit index criteria. Finally, the factor loadings values were reported for each latent variable to find the CR values, and the internal consistency reliability of items was measured. The reliable questionnaire revealed that the CR ranged from 0.718 to 0.804. In addition, the mean variance of the questionnaires was verified, and the discriminant validity of the questions with AVE values ranging from 0.511 to 0.618 was found as illustrated in Table 1.

Table 1 The results of the quality analysis of the construct validity questionnaire.

Latent variables	Number of items	p-value	λ	CR	AVE
1. PDPB	12	0.408	0.431–0.838	0.782	0.552
2. VUL	6	0.261	0.420–0.914	0.751	0.559
3. SEV	6	0.743	0.429–0.776	0.732	0.524
4. RES	6	0.706	0.405–0.828	0.718	0.516
5. SEL	8	0.244	0.425–0.921	0.745	0.529
6. COST	5	0.218	0.437–0.790	0.724	0.511
7. SYS	6	0.453	0.458–0.931	0.787	0.530
8. SN	5	0.457	0.471–0.943	0.779	0.546
9. PU	5	0.491	0.436–0.846	0.727	0.534
10. PEOU	5	0.374	0.501–0.857	0.748	0.551
11. ATT	4	0.803	0.424–0.861	0.733	0.528
12. BI	4	0.518	0.570–0.911	0.804	0.618

Descriptive statistics and normality analysis

Table 2 indicates the descriptive statistics for the observed variables' average value or mean (M), standard deviation (SD), and the results of normality analysis: The average value of observed variable for each latent variable can be ranged from 3.586 to 3.987. Of all the observed variables of PDPB, technical protection had the highest average value (M = 3.755, SD = 0.835). Meanwhile, the causal variables were found where protection intention was score the highest (M = 3.987, SD = 0.824). Furthermore, the univariate test for continuous variables of the observed variables about skewness and kurtosis indexes was not statistically significant with p–values ranging from 0.091 to 0.823. As a result, the finding revealed that the observed variables were complied with a normal distribution. Moreover, the multicollinearity test should be performed to ensure that the correlation coefficient between the observed variables and Pearson's product moment correlation coefficient (r) results do not exceed 0.85 (Jöreskog et al., 2016) prior to reporting the structural model. As correlation was examined, a positive correlation between $0.140 \leq r \leq 0.792$ was discovered, and all levels were statistically significant at 0.01.

Table 2 Descriptive statistics and normality analysis.

Latent variables	Observed variables	M	SD	Skewness & Kurtosis	
				Chi-square	p-value
1. PDPB	Precautions in general (GEN)	3.746	0.890	2.927	0.231
	Technical protection (TECH)	3.755	0.835	1.482	0.477
2. VUL	e-Transaction providers (VUL1)	3.678	0.990	5.309	0.091
	e-Transaction users (VUL2)	3.679	1.075	5.315	0.093
3. SEV	Theft of money (SEV1)	3.708	1.062	5.278	0.125
	Privacy infringement (SEV2)	3.652	1.083	5.113	0.178
4. RES	General principles (RES1)	3.687	1.069	5.136	0.173
	Advanced recommendations (RES2)	3.605	0.996	3.225	0.199
5. SEL	Computer and network knowledge (SEL1)	3.743	1.038	3.740	0.154
	Incidents of Security Breach (SEL2)	3.586	1.023	5.210	0.096
	Control the situation (SEL3)	3.714	1.065	3.859	0.145
6. COST	Money (COST1)	3.853	1.055	4.203	0.122
	Time and effort expanded (COST2)	3.736	0.968	4.612	0.119
7. SYS	Features (SYS1)	3.853	1.055	4.467	0.106
	User Interface (SYS2)	3.736	0.864	4.674	0.097
8. SN	Close friends (SN1)	3.952	0.934	4.460	0.108
	IT Bloggers (SN2)	3.778	1.052	3.847	0.146
9. PU	Self-interest is beneficial (PU1)	3.841	0.860	4.596	0.099
	Increase your productivity (PU2)	3.766	0.935	1.431	0.489
10. PEOU	Easy to learn (PEOU1)	3.785	1.046	3.727	0.155
	Simplicity (PEOU2)	3.643	1.038	1.789	0.409
11. ATT	Belief in behavior (ATT1)	3.831	0.947	4.039	0.133
	Outcomes Evaluation (ATT2)	3.819	0.862	1.772	0.412
12. BI	Protection Intention (BI1)	3.987	0.824	0.389	0.823

Testing the structural model

The criteria for conformity with the empirical data was also taken into account. After the adjustment was made to the model, the presented values refer to the coefficient and standardized coefficient within the six out of seven fit indices rates seems to be in acceptable ranges, where only the p-value was not in an acceptable range but χ^2/df rates seem to be in an acceptable range or lower than five (3.959) for the large sample size testing (Kline, 2015). The root mean squared error of approximation (RMSEA) was 0.075, and the standard root mean squared residual (SRMR) was 0.055, as stated in the fit criterion of the SEM to measure the absolute fit, χ^2= 684.99, df =173,

$p < 0.01$. The comparative fit index (CFI) measure by CFI was 0.97, the non–normed fit index (NNFI) or Tucker–Lewis Index (TLI) was 0.96, and the goodness of fit index (GFI) was 0.90, which satisfy all criteria (Kline, 2015).

Results of the analysis of the structural model of PDPB

The standardized estimation of path coefficients and path analysis of the structural model is depicted in Figure 1. The standardized path coefficient value (β) between latent variables and its observed variables in current research indicated that all of the coefficient outputs with the t–value test were statistically significant at 0.01 (t–value > 2.576) (Jöreskog et al, 2016) as follows; 1) a high positive impact on PDPB with β = 0.83 and β = 0.81 was found in the latent of PDPB for GEN and TECH observed variables which indicates that general protection factor was relatively important (Comrey & Lee, 2013); 2) regarding VUL latent, the outcomes of VUL1 and VUL2 (β = 0.63 and β = 0.71) significantly demonstrated a positive impact on VUL, especially in the factor related to e–Transaction service of users; 3) the latent SEV had shown a positive coefficient impact of β = 0.54 and β = 0.72 for SEV1 and SEV2, respectively, and the factor related to privacy infringement was significant; 4) in terms of RES latent, the results for RES1 and RES2 (β = 0.63 and β = 0.52) significantly demonstrated a positive impact on RES, particularly since RES1 was a strong positive coefficient; 5) regarding SEL latent, the results for SEL1, SEL2, and SEL3 (β = 0.49, β = 0.54, and β = 0.74) significantly demonstrated a positive impact on SEL relevant to computer and network skills and the situation controlling factor in particular; 6) the latent COST revealed a strong positive coefficient with β = 0.77 and β = 0.70 and the factor related to monetary or perceived costs was significant; 7) in terms of SYS latent, the results for SYS1 and SYS2 (β = 0.79 and β = 0.49) indicated an appreciably highly positive impact on SYS, especially from the feature factor available in the application from the study of the TAM model; 8) the latent SN revealed a strong positive coefficient impact with β = 0.81 and β = 0.28 for SN1 and SN2, respectively, where close friend is a more important factor; 9) for PU latent, the results for PU1 and PU2 (β = 0.69 and β = 0.84) indicated a significant positive impact on PU. PU2 in particular was a high positive coefficient. 10) The latent PEOU had a positive coefficient impact with β = 0.36 and β = 0.72 for PEOU1 and PEOU2, respectively, with the simplicity as a more important factor; and finally, 11) the results from investigating ATT1 and ATT2 (β = 0.44 and β = 0.94) demonstrated a highly positive impact on

ATT, with ATT2 with the strongest positive coefficient for evaluating outcomes to protect personal information.

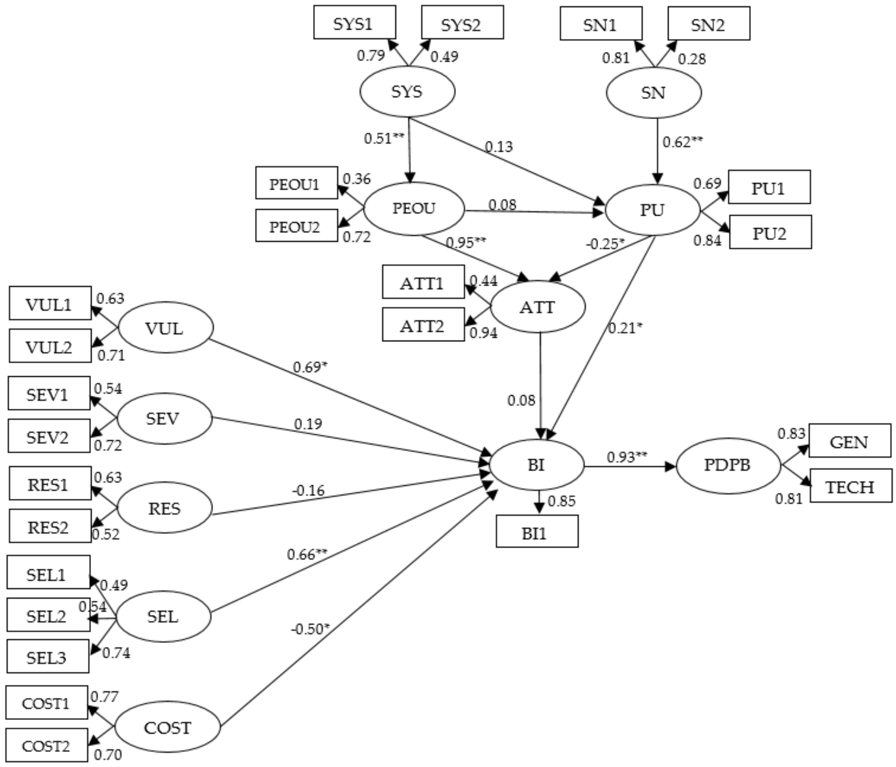

Figure 1 The path coefficient findings as a result of the proposed research model.

When the finalized model as shown in Figure 1 was compared to the hypothetical research model, the outcomes demonstrated that all of the t-value tests were statistically significant at 0.05 (*) and the 0.01 level (**). Formalized paraphrases have shown that the relationship between BI and PDPB had the highest t-value score (t-value = 18.53), while the relationship between PEOU and ATT was the lowest. Almost all the hypotheses in this study were supported by the relationship between variables as follows: the Protection Motivation Theory (PMT) was applied to indicate the positive relationship between VUL --> BI (β = 0.69) and SEL --> BI (β = 0.66). Thus, hypotheses (H1 and H4) are confirmed. Furthermore, the causal factors on behavioral intention (BI) to protect personal information found in current study are self-efficacy, and perceived vulnerability. While, a negative relationship between COST --> BI (β = -0.50) was supported by hypothesis H5. According to the findings of TAM Model, hypotheses H6 confirmed the positive relationship between SYS --> PEOU (β = 0.51). Positive relationships between SN and PU (β = 0.62) within H8 are raised to support the hypothesis. Hypotheses H10 are accepted since there was a positive relationship between PU --> BI (β = 0.21). Hypotheses were supported to confirm the positive relationship between PEOU --> ATT (β = 0.95) for H12. Furthermore, hypothesis is supported (H14) as there were positive relationships between BI --> PDPB (β = 0.93, t-value = 18.53), and it indicated a positive effect rates on PDPB induced by BI to protect personal information.

Moreover, the findings regarding path coefficient (β) of PDPB from the standardized total and indirect effects output (Jöreskog et al, 2016) for the analysis of the direct effects (DE), indirect effects (IE), and total effects (TE) between the variables in the model included the coefficient of determination (R^2) as demonstrated in Table 3. From the findings, it indicated that PDPB had a direct and static positive effect on BI (β = 0.93) and the positive indirect effect VUL obtained β = 0.67, SEL (β = 0.64), SN (β = 0.22) and PU (β = 0.20). For a negative indirect effect from COST (β = -0.48) .Their variables which includes SEV, RES, SYS, PEOU and ATT are responsible for approximately 94 percent (R^2= 0.94) of the increased variance for PDPB, and it pointed out that the variables in this model provided relatively high scores for PDPB. Similarly, BI had a direct and static positive effect on VUL where β = 0.69, SEL (β = 0.66) and COST (β = -0.50) and the positive indirect effect from SN β = 0.22) revealed approximately 94% of the increased variance. Furthermore, PU latent had a direct and static positive effect on SN (β = 0.62) and approximately 68 percent (R^2= 0.68) of the increased variance of PU was obtained. SYS revealed a single direct and static positive effect on PEOU latent with β = 0.51. In addition, it was found the direct and static positive effect that ATT had on PEOU (β = 0.95) as well as an indirect effect on SYS (β = 0.44), and approximately 71 percent of the increased variance for ATT was obtained as show in Table 3.

Table 3 Direct, indirect, and total effects between the variables in the model.

Latent variables	Assigned variables	DE	IE	TE
BI	VUL	0.69*	–	0.69*
R^2 = 0.94	SEV	0.19	–	0.19
	RES	-0.16	–	-0.16
	SEL	0.66**	–	0.66**
	COST	-0.50*	–	-0.50*
	SN	–	0.22*	0.22*
	SYS	–	0.03	0.03
	PU	0.21*	-0.01	0.20*
	PEOU	–	0.03	0.03
	ATT	0.08	–	0.08
PU	SN	0.62**	–	0.62**
R^2 = 0.68	SYS	0.13	0.04	0.17
	PEOU	0.08	–	0.08
PEOU, R^2 = 0.26	SYS	0.51**	–	0.51**
ATT	SN	–	-0.15	-0.15
R^2 = 0.71	SYS	–	0.44**	0.44**
	PU	-0.25*	–	-0.25*
	PEOU	0.95**	-0.02	0.93**
PDPB	VUL	–	0.67*	0.67*
R^2= 0.94	SEV	–	0.18	0.18
	RES	–	-0.16	-0.16
	SEL	–	0.64**	0.64**
	COST	–	-0.48*	-0.48*
	SN	–	0.22*	0.22*
	SYS	–	0.03	0.03
	PU	–	0.20*	0.20*
	PEOU	–	0.03	0.03
	ATT	–	0.08	0.08
	BI	0.93**	–	0.93**

Discussion and suggestion

The significance of the findings was to describe what the first jobbers should do to protect data privacy on e-Transactions, especially in terms of general and technical protection factors. The behavioral intention of this group was related to the evaluation of personal information protection affected by PDPB (Bulgurcu et al., 2010), and the H14 hypothesis was confirmed. PDPB effectively explained the individual's intention to adopt precautions and measures to protect personal data, for instance, improving computer and networking skills, understanding of personal confidentiality on e-Transactions applications, and expressing commitment to comply with information security regulations. This study looks into the factors that are responsible for the compliance with PDPB. From a component of the PMT Theory research mode, the VUL from e-Transactions service providers and users were discovered where users' personal information was obtained without permission or when important personal data is disclosed and transmitted to third parties or external institutions. For SEL the evaluation of computer networking skills and experience with e-Transactions were examined. The factors which are the findings of this study indicated a positive effect and support BI (Ifinedo, 2012) to confirm hypotheses H1 and H4. In PMT, this research data was confirmed that the coping appraisal of COST has a negative effect on BI (Yoon, 2012) by hypotheses H5, in terms of the effort involved in updating security software and protective technology has a negative effect on intention. According to the findings, SYS demonstrated a positive influence on PEOU of the TAM Model. The outcomes also indicated users' characteristics, perceptions, and opinions regarding the knowledge of computer systems or applications in which they can customize to manage security settings of personal information and the security of personal information disclosure are controlled. Users can simply understand the positive interaction between the system and user needs, the accuracy and fast processing mode, the manifestation and attraction of the system that has a positive effect on PEOU (Giovanis et al., 2012) to set up and to protect personal information, thus hypotheses H6 was confirmed. In terms of the SN component, the findings found that family, close friends, and colleagues influenced the PU component (Venkatesh and Davis, 2000) in setting and managing personal information, therefore hypothesis H8 was validated. Furthermore, PU refers to the advantages brought to the individual on personal information management which benefited their lives and increased the effectiveness of personal data security, particularly increasing personal information security result in positive effect and support ATT and BI (Davis, 1989) to setting up and protecting personal information, thus hypotheses H10 was confirmed. PEOU proposed by hypotheses H12 stating that the system is not complicated and does not require many steps to manage data protection settings affect the efficacy of data security in the applications; thus, it supported PU and ATT (Venkatesh & Davis, 1996) in terms of setting and protecting personal information.

The findings of this study demonstrated that PMT and the TAM Model adaptation were effective for the PDPB on e-Transactions among the first jobbers. Thus, future research might employ qualitative methods such as in-depth interviews with key informants, focus groups, and participant observation to find in-depth information and to complement the performance of research approaches.

Conclusion

From the research model, PMT and TAM Model were applied to identify factors that influenced privacy data protection behaviors (PDPB) on e-Transactions. The findings found that perceived vulnerability, self-efficacy and subjective norms have a significant influence on behavioral intention to protect personal information as well as perceived usefulness and attitude toward setting and personal information protection. There was an impact that PDPB had on intention. As a result, the findings supported the hypotheses, which were then supported by the applied theories and methodology developed. In addition, according to the findings found in the TAM model, perceived ease of use was influenced by system characteristics for managing the manual setup of personal information security on financial applications whereas subjective norms had an influence on perceived usefulness as well. Furthermore, perceived ease of use influenced attitude, and perceived usefulness influenced intention in terms of setting and personal information protection as confirmed by the hypothesis.

Knowledge from Research

The findings of current study with the aim to educate the fresh graduates of the use of applications before entering the real world situation. In particular, self-efficacy and perceived vulnerability having a strong impact from PDPB and behavioral intention to setting up and protecting personal information. These results imply that student will make more networking and computer skills for personal data protection, information security and practical guidelines to setting up and providing protection to personal information were found. For example, the knowledge of advanced computer device maintenance, password setting, and unlocking smartphone screen, rather than e-Transactions when using public Wi-Fi networks are the effective indicators of personal data protection behavior. In addition to providing computer and financial literacy, lecturers and educational institutes should provide their learners with curriculum related to personal data protection and security, the knowledge of data privacy, and personal training in advance, including the knowledge of applications in practice as well as the access to reliable information sources according to PDPB guidelines on e-Transaction services. It equipped the lecturers with an institute related assessment model to educate about the effectiveness and the awareness of PDPB.

References

Aghaei, S., Nematbakhsh, M. A., & Farsani, H. K. (2012). Evolution of the world wide web: From WEB 1.0 TO WEB 4.0. *International Journal of Web & Semantic Technology*, *3*(1), 1-10.

Bandura, A. (1977). Self-Efficacy:Toward a Unifying Theory of Behavioral Change. *Psychology. Review, 84,* 191-215.

Bank of Thailand. (2018). *Annual Report of Mobile Banking Transactions*. Bank of Thailand. https://www.bot.or.th/Thai/Statistics/PaymentSystem_Reports/Q2_2560.pdf

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American society for information science and technology, 58*(2), 157-165.

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: the importance of Internet skills for online privacy protection. Information, *Communication & Society, 20*(8), 1261-1278.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 523-548.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research, 48*(7), 953-977.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information technology and management*, *6*(2), 181-202.

Chen, H. T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13-19.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 189-211.

Comrey, A. L., & Lee, H. B. (2013). *A first course in factor analysis*. Psychology.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319–340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management science, 35*(8), 982–1003.

Diamond, P., & Vartiainen, H. (2007). *Behavioral economics and its applications*. Princeton.

Ernst, C. H. (2015). Privacy Protecting Behavior in Social Network Sites. In *Factors driving social network site usage* (pp. 57–81). Springer Gabler.

Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy–protecting behaviors. *Computers in Human Behavior, 33*, 153–162.

Fishbein, M. & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Addison–Wesley.

Fornell, C., & Larcker, D. F. (1981). *Structural equation models with unobservable variables and measurement error: Algebra and statistics.*

Freiherr, A. V., & Zeiter, A. (2016). Implementing the EU general data protection regulation: a business perspective. *European Data Protection Law Review, 2,* 576.

Giovanis, A. N., Binioris, S., & Polychronopoulos, G. (2012). An extension of TAM model with IDT and security/privacy risk in the adoption of internet banking services in Greece. *EuroMed Journal of Business, 7,* 24–53

Hair, J. F. J., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. (2010). *Multivariate data analysis upper saddle river*: Pearson Prentice–Hall.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83–95

Jöreskog, K.G., Olsson, U.H., & Wallentin, F.Y. (2016). *Multivariate analysis with LISREL*. Springer.

Kline, R.B. (2015). *Principles and Practice of Structural Equation Modeling*. The Guilford.

Lee, Y., & Larsen, K.R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti–malware software. European *Journal of Information Systems, 18*(2), 177–187.

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.

Mehrabian, A. & Russell, J.A. (1974) *An Approach to Environmental Psychology*. MIT.

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.

Milne, G.R., Labrecque, L.I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs, 43*(3), 449-473.

Ng, B.Y., Kankanhalli, A., & Xu, Y.C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Nunnally, J.C. (1994). *Psychometric Theory* (3rd ed.). Tata McGraw-Hill Education.

Paine, C., Reips, U.D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'Privacy Concerns' and 'Privacy Actions'. *International Journal of Human-Computer Studies, 65*(6), 526-536.

Park, C., & Lee, S.W. (2014). A study of the user privacy protection behavior in online environment: Based on protection motivation theory. *Journal of Internet Computing and Services, 15*(2), 59-71.

Plotnikoff, R.C., Lippke, S., Trinh, L., Courneya, K.S., Birkett, N., & Sigal, R.J. (2010). Protection motivation theory and the prediction of physical activity among adults with type 1 or type 2 diabetes in a large population sample. *British Journal of Health Psychology, 15*(3), 643-661.

Rogers, R.W. (1983). Cognitive and psychological processes in fear appeals and attitude change: *A revised theory of protection motivation. Social psychophysiology: A sourcebook*, 153-176.

Rosenstock, I.M. (1974). Historical origins of the health belief model. *Health Education Monographs, 2*(4), 328-335.

Rovinelli, R.J., & Hambleton, R.K. (1976). On the use of content specialists in the assessment of criterion-referenced test item validity. *Tijdschrift Voor Onderwijs Research, 2,* 49-60.

Smith, A. D., & Lias, A. R. (2005). Identity theft and e-fraud as critical CRM concerns. International *Journal of Enterprise Information Systems (IJEIS), 1*(2), 17-36.

Smith, H.J., Milberg, S.J., & Burke, S.J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167-196.

The Financial Consumer Protection Center, Bank of Thailand. (2019). *Fin-fraud*. Bank of Thailand. https://www.1213.or.th/th/finfrauds/OnlineCrime/Pages/OnlineCrime.aspx

Venkatesh, V., & Davis, F.D. (1996). A model of the antecedents of perceived ease of use: Development and test. *Decision Sciences, 27*(3), 451-481.

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

Yao, M.Z., & Linz, D.G. (2008). Predicting self-protections of online privacy. *Cyber Psychology & Behavior, 11*(5), 615-617.

Yoon, C., Hwang, J.W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education, 23*(4), 407-416.