International Journal of Computing Sciences Research (ISSN print: 2546-0552; ISSN online: 2546-115X)
Vol. 7, pp. 1133-1151
doi: 10.25147/ijcsr.2017.001.1.123
https://stepacademic.net

Long Paper *

The Relationship between Cyber Security Knowledge, Awareness and Behavioural Choice Protection among Mobile Banking Users in Thailand

Pongsakorn Limna
Rangsit University, Thailand
pongsakorn.l65@rsu.ac.th
ORCID ID: orcid.org/0000-0002-7448-5261
(corresponding author)

Tanpat Kraiwanit
Rangsit University, Thailand
tanpat.k@rsu.ac.th
ORCID ID: orcid.org/0000-0002-5130-6427

Sutithep Siripipattanakul
Kasetsart University, Thailand
fedustt@ku.ac.th
ORCID ID: orcid.org/0000-0002-5477-6723

Date received: August 21, 2022
Date received in revised form: October 3, 2022*;* November 3, 2022
Date accepted: November 3, 2022

Recommended citation:

Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2023). The Relationship between Cyber Security Awareness, Knowledge, and Behavioural Choice Protection among Mobile Banking Users in Thailand. *International Journal of Computing Sciences Research*, *7*, 1133-1151. https://doi.org/10.25147/ijcsr.2017.001.1.123

*****Special Issue on Metaverse and Cybersecurity in the Digital Economy. Guest Editor: Supaprawat Siripipatthanakul, Ph.D., Adjunct Professor and Researcher at Asia eUniversity, Malaysia; Researcher at Manipal GlobalNxt University, Malaysia; Lecturer and Researcher at Bangkok Thonburi University, Thailand.*

Abstract

Purpose – Mobile banking is becoming increasingly popular in Thailand. This study investigates the relationship between cyber security knowledge, awareness, and behavioural choice protection among mobile banking users in Thailand.

Method – A quantitative approach was employed. The questionnaire was developed based on reliable and valid sources. The online questionnaire was adopted to collect the data through convenience sampling of 414 mobile banking users in Thailand. The data were analysed using SPSS Version 27 and ADANCO 2.3 for hypothesis testing.

Results – The results reveal that cyber security knowledge significantly impacts cyber security awareness and behavioural choice protection. Cybersecurity awareness significantly impacts behavioural choice protection. Cyber security awareness significantly mediators between cyber security knowledge and behavioural choice protection.

Conclusion – Cyber security knowledge and awareness are critical for influencing behavioural choice protection among Thai mobile banking users. As a result, banks must develop an effective cybersecurity strategy to meet the needs and expectations of mobile banking users. As a result, there may be an increase in mobile banking users, and high business performance may incur.

Recommendations – This study employed sampling to explain only mobile banking from customers' perceptions. It may not cover other sectors. Hence, there should be increased sampling in a variety of industries. Furthermore, this study consists of a self-administered questionnaire for quantitative analysis. Thus, more insightful analysis through qualitative research could also explain the association between cyber security awareness, cyber security knowledge, and behavioural choice protection among mobile banking application customers or other sectors in Thailand.

Research Implications – This study contributed to the existing literature on cyber security awareness, cyber security knowledge, and behavioural choice protection. Therefore, the findings of this study may help academics expand their research by incorporating additional potential factors. These metrics could guide future cybersecurity research and its outcomes in the digital era.

Practical Implications – The implications could be applied to any sector in explaining the association between cybersecurity awareness, knowledge and behavioural choice protection among mobile banking application customers or other sectors in Thailand.

Keywords – cyber security, awareness, knowledge, behavioural choice protection, mobile banking

INTRODUCTION

The role of technology has increased, and technology now has an enormous impact on people's daily lives. Technology is crucial in the banking industry. As one of the largest financial institutions, banking is always looking for new ways to use technology to improve customer experience and convenience. A mobile phone is a standard technological device that has become a part of everyone's life in the information age. Hence, the growth rate of financial transactions conducted through online platforms has increased. Mobile banking is a new alternative channel for delivering banking services (Devadevan, 2013; Kraiwanit & Srijaem, 2021). Furthermore, the explosive growth of Information and Communication Technologies (ICT) in the financial industry, particularly the banking sector, has transformed how banks deliver customer services. Customers perform banking activities such as checking account balances, making payments, applying for credit, and conducting transactions using hand-held devices through the mobile banking model, a dynamic banking channel of banks (Aldiabat et al., 2019). In addition, mobile banking allows customers to conduct financial transactions from anywhere, at any time, using a mobile handheld device and a data plan. It eliminates the space and time constraints associated with traditional banking activities such as checking account balances or transferring funds from one account to another. Moreover, this technological advancement has become one of the most powerful tools in transforming traditional banking services into an online mass market that reaches a more extensive customer base (Ruangkanjanases & Wongprasopchai, 2018). Despite having many inherent benefits, m-banking has suffered from low and slower customer adoption, making this a critical issue to be studied and explained by many studies worldwide (Aldiabat et al., 2019). Therefore, mobile banking is an essential topic to study.

Technological advancements have altered how ordinary citizens go about their daily lives. Many of these activities are carried out via the Internet. These include tax returns, online banking, job searching, and general socialising (Dlamini & Modise, 2012). The scale of the rise in cybercrimes is alarming. Moreover, cybersecurity is the most concerning issue because cyber threats and attacks are on the rise. Cyber security is a vital combination of security procedures, techniques, tools, and guidelines to protect internet-connected applications and devices. Similarly, it is the processes and techniques used to protect sensitive data, computer systems, networks, and software applications from cyber attacks (Alotaibi et al., 2016; Almaiah et al., 2021). Furthermore, technological adoption is one of the most difficult challenges for the banking industry. Some risks associated with mobile banking or internet banking users are their behaviours. If the risk of internet banking security is real, it can result in financial losses. The financial and banking sectors are more vulnerable to security threats. User acceptance is a critical factor in technology acceptance. Working with internet banking necessitates a certain level of computer literacy. Users may

hesitate to trust a completely automated system (Alghazo et al., 2017). Cybersecurity is a global phenomenon that poses a complex socio-technical challenge to governments while also requiring the participation of individuals. Although cybersecurity is one of the most pressing issues confronting governments today, public awareness and visibility remain low. Although almost everyone has heard of cybersecurity, people's urgency and behaviour do not reflect a high level of awareness. All too often, the internet is regarded as a secure environment for exchanging information, conducting transactions, and controlling the physical world. However, cyber warfare is already in progress, and there is an urgent need to improve preparedness. The inability to frame cybersecurity has resulted in the inability to develop appropriate policies (de Bruijn & Janssen, 2017). Thus, organisations must ensure that users remain secure online by raising cybersecurity awareness and knowledge (Bada et al., 2019; Scholefield & Shepherd, 2019). Thailand, like other countries, has experienced several cyberattacks each year since launching the Thailand 4.0 philosophy in 2016. Fraud, intrusion attempts, and malicious code were the most common threats to public and private organisations (Senarak, 2021). Furthermore, banks have expressed a strong interest in system security, but internet banking crime in Thailand persists, primarily on the customer side (Ingkathawornwong, 2020). Therefore, studying the relationship between cyber security knowledge, awareness, and behavioural choice protection among mobile banking users in Thailand is critical.

Research Objective

This study investigates the relationship between cyber security knowledge, cyber security awareness, knowledge and behavioural choice protection among mobile banking users in Thailand.

Research Question

How does the Partial Least Squares Structural Equation Model (PLS-SEM) model explain the relationship between cyber security knowledge, awareness and behavioural choice protection among mobile banking users in Thailand?

LITERATURE REVIEW

Mobile Banking

Banks are regarded as highly dynamic business entities that provide better terms to clients who choose to use online banking services when linked to a global network. This industry, like many others, transforms the Internet and mobile applications or apps into the most effective channel for providing banking products and services. As a result, there is an increasingly competitive banking sector with increasingly demanding customers (Munoz-Leiva et al., 2017). Furthermore, technological advancements in

telecommunications and information technology (IT) have continued transforming the banking industry. The delivery of financial services has changed dramatically in recent years. The banking industry has become increasingly turbulent and competitive around the world. Banks, aided by technological advancements, have responded to the challenges by implementing a new strategy focusing on building and providing the highest level of customer satisfaction by offering better products and services while minimising operational costs. Mobile banking services are widely used. Understanding the customer adoption process has important implications for bankers and customers (Al-Jabri & Sohail, 2012; Aldiabat et al., 2019; Loetrueangnapha & Kraiwanit, 2019).

Mobile banking (m-banking) is a service provided by a bank or other financial institution that allows customers to conduct a variety of banking operations using a mobile device such as a mobile phone, tablet, or personal digital assistant (Kwateng et al., 2018). Mobile banking or internet banking is one of the most recent and reliable technologies that banks use to connect and service their customers who live far from bank branches. The expansion of mobile banking has increased not only the number of client accounts but also the volume and the total value of the software. Mobile banking is required to continuously improve banking services (Loetrueangnapha & Kraiwanit, 2019). Furthermore, mobile banking has become one of the most important strategies for banks to operate and transact with their customers. It is a key component of bank expansion strategies. Mobile banking applications enable payments, banking, real-time two-way data transmission, and ubiquitous access to financial information and services. Even though mobile phones outnumber personal computers, and mobile banking has become more popular among bankers than e-banking, using mobile phones or tablets to conduct banking transactions or access financial information is not as common as one might expect (Shaikh & Karjaluoto, 2015). The mobile application must be designed in such a way that users can interact with it effectively. One of the critical success factors of such an application is its ability to use an application with such a small device effectively and with good interaction (Hussain et al., 2014).

In Thailand, many young customers are more willing to consider non-traditional financial services than ever. Young adults are becoming new banking customers as they enter the consumer society. These younger generations like to experience new things and expect personalised services. They also expect a diverse range of products tailored to their lifestyle and personal circumstances, and others easily influence them. Banks try to increase the popularity of mobile banking by making it easier for customers to use to remain competitive and maintain customer connections in the digital age. Thailand's mobile banking services have evolved to be more personalised for customers. As a result, mobile banking penetration increased slightly from 1.1 per cent in 2011 to 9.3 per cent in 2014 (Ruangkanjanases & Wongprasopchai, 2018). In addition, based on the data from the Bank of Thailand in 2017, the total number of deposit accounts in Thailand is around 92 million. Still, mobile banking registrations are around 18 million, accounting for only 20% of

total accounts. Although mobile banking is undoubtedly the future of Thai banking, a greater client understanding of mobile banking adoption is still a vital and critical issue to widespread mobile phone penetration, particularly in upper-middle-income economies such as Thailand (Puriwat & Tripopsakul, 2017). The Bank of Thailand surveyed payment transactions via mobile banking services. The results showed that at the end of March 2019, the total number of customer accounts using mobile banking services was 43.882 million. The transaction volume was 347.853 million, and the transaction value was 1.875 billion baht. These figures demonstrate the growing popularity of mobile banking services, which is a positive sign for Thailand's transition to a cashless society (Navavongsathian et al., 2020).

Cyber Security Knowledge

People are increasingly reliant on internet technologies for day-to-day tasks. The ease of use has increased mass participation in cyber-related activities. However, knowledge of existing tools required for cyber threat protection lags. Even basic cyber security awareness may not translate into sufficient or appropriate cyber security protection knowledge to mitigate cyber risks and hazards. As a result, it is critical to increase cyber security knowledge through training programs that use theoretical lectures and simulators to provide exposure to cyber security protection tools. These would concentrate on operational, usage, and process aspects of improving user knowledge and translating it into effective cyber security mitigation behaviour (Zwilling et al., 2022). Furthermore, knowledge and skills are necessary aspects of competence. It can apply related knowledge, skills, and abilities required to perform critical work functions successfully. The more practice, the more able to perform a specific skill with the required level of proficiency to achieve a particular task. Therefore, to protect their devices from threats, all technology users must have cybersecurity knowledge, emphasising the importance of cybersecurity knowledge and skills in using digital technologies (Misra & Khurana, 2017; Senarak, 2021).

Cyber Security Awareness

The internet has transformed how people manage their lives by connecting with new people through social networks and opening up new economic horizons for transactions via mobile devices for individuals and organisations, including a radical shift in the higher education system and teaching methods. Nonetheless, many people continue to face information security risks from a wide range of threats. Hence, cyber security awareness is essential (Zwilling et al., 2022). Cyber security awareness is a type of security training that is used to inspire, stimulate, establish, and rebuild cyber security skills and expected security practices in a specific audience. Promoting and encouraging Internet users to take precautions and training them on online security measures is essential. Furthermore, it provides these users with cyber security skills in all aspects of cyber security,

ensuring that not only the national network infrastructures but also the users are resilient to cyber-attacks and threats (Dlamini & Modise, 2012). Providing users with training to raise awareness about cyber security is critical. Education, promotion, and other methods are used to raise cyber security awareness. However, these modes must effectively make an impression on users (Alotaibi et al., 2016).

Behavioural Choice Protection

Recognising the high cost of cyber risks, research has increasingly focused on the precautions and behaviours displayed by internet users to protect their devices (Zwilling et al., 2022). The ability to choose, as opposed to being told what to do or given only one option, has been shown to have positive effects. People are more internally motivated and perform better on tasks they have chosen, and they are also more satisfied with their choices and feel more in control (Iyengar & Lepper, 2000). People tend to select only the parts of a message that interest them. One reason is that, like everyone else, decision-makers and policymakers will react differently depending on objectively equivalent descriptions of the same problem. Communication about cybersecurity issues and the urgent need for policies is a difficult task that requires clear and convincing communication. People often point to cybersecurity risk as a way to foresee threats to the state to create a security imagination, a fictionalisation that could foster fear (de Bruijn & Janssen, 2017).

Hypothesis Development

The Relationship between Cyber Security Knowledge, Cyber Security Awareness, and Behavioural Choice Protection

Soomro et al. (2016) discovered that numerous management activities, including the development and implementation of information security policies, awareness, compliance training, the development of effective enterprise information architecture, IT infrastructure management, business and IT alignment, and human resource management, had a significant impact on the quality of information security management. Zwilling et al. (2022) confirmed the relationship between greater cyber knowledge and cyber awareness. In addition, awareness was linked to security tools, but not the number of information people are willing to share. Furthermore, Bada et al. (2019) concluded that knowledge and awareness were necessary but insufficient for changing behaviour and that they must be combined with other influencing strategies. It was critical to instil positive cyber security behaviours, which could lead to thinking becoming a habit and becoming part of a company's cyber security culture. Kruger et al. (2010) confirmed that using a vocabulary test to assess security awareness levels was beneficial. Moreover, Abawajy (2004) indicated that information security awareness training was a powerful way of equipping people with knowledge on specific topics. Almost all participants correctly understood phishing and the risks it posed to both individuals and organisations after completing the

training. Mamonov and Benbunan-Fich (2018) confirmed that the awareness of information security threats improved the strength of newly chosen passwords. Hence, hypotheses can be devised as follows.

H1: Cyber security knowledge significantly influences cyber security awareness.
H2: Cyber security knowledge significantly influences behavioural choice protection.
H3: Cybersecurity awareness significantly influences behavioural choice protection.

The Mediating Effect of Cyber Security Awareness between Cyber Security Knowledge, Behavioural Choice Protection

Ahlan et al. (2015) identified several important factors influencing awareness and their interactions with other factors, such as religious indicators, which can influence peers not only performance but also social pressure. Furthermore, Van der Schyff and Flowerday (2021) indicated that information security awareness was a mediator for some personality traits. It was discovered that information security awareness, in particular, acted as an indirect mediator between openness and the intention to review privacy settings. It was revealed that as users with a high level of openness became more aware of privacy-related threats (via privacy news and events), their desire to review privacy settings increased. It was also discovered that, albeit complementary, information security awareness mediated the relationship between conscientiousness and intention to check privacy settings.

H4: Cyber security awareness is the significant mediator between cyber security knowledge and behavioural choice protection.

Conceptual Framework

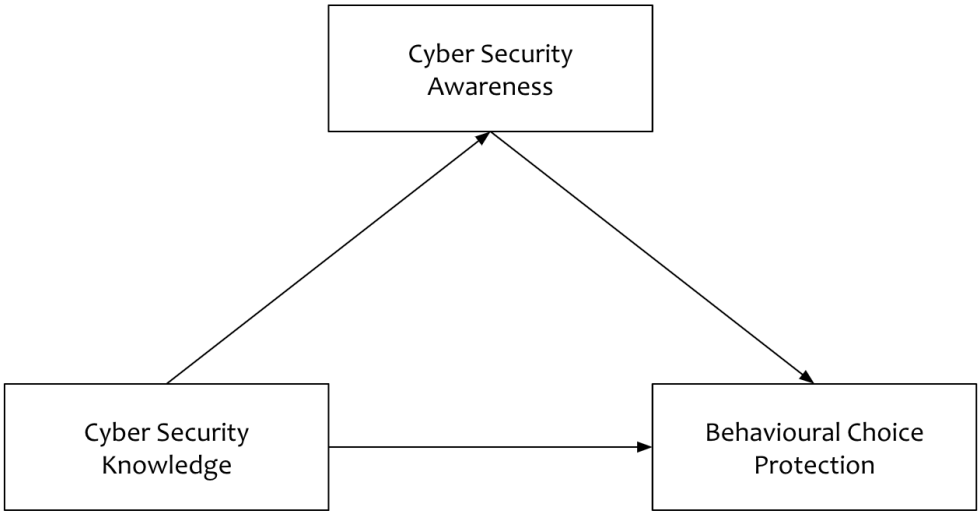

Figure 1. Conceptual Framework, based on the study of Zwilling et al. (2022)

RESEARCH METHODOLOGY

Research Method

This quantitative research employed closed-ended questionnaires (Likert's Rating Scale) for data collection. The questionnaire items were developed by the researchers based on previous research. Moreover, the questionnaire was tested on 30 respondents (pre-testing) for a dedicated questionnaire. Measuring instruments' reliability and validity were also evaluated. According to Si Dha et al. (2022), it is crucial to comprehend that the validity of an instrument refers to how well it measures the researcher's conceptual framework or hypothesis. The main variables in this study were evaluated using a five-point Likert's Rating Scale with the following classifications: strongly agree with a value of 5, agree with a value of 4, neutral with a value of 3, disagree with a value of 2, and strongly disagree with a value of 1. An analysis of the demographics of those who responded to the survey questions was based on the research of Chana et al. (2021), Limna et al. (2022), and Siripipatthanakul et al. (2022). The questionnaire items in cybersecurity awareness, knowledge and behavioural choice protection constructs were based on the study of Zwilling et al. (2022).

Population and Sample

The study's target population was unknown. The samples were Thai mobile banking application users. The researchers conducted a traditional survey with a 95% confidence level. According to Napawut et al. (2022) and Sitthipon et al. (2022), a minimum of 385 cases with a p-value of 0.05 could be obtained through convenience sampling for the inferential statistics. Therefore, the data collection for this study included 414 participants from Thailand's five distinct geographical regions.

Data Collection

The researchers gathered data from five regions of Thailand (Northern, Eastern, Northeastern, Central and Southern-Western) using self-administered questionnaires and convenience sampling. Before distributing online questionnaires, the researchers clarified the purpose of the study and solicited the respondents' participation. The online survey was collected between June 10th and August 10th, 2022.

Data Analysis

For descriptive statistical analysis (frequency and percentage), the demographic characteristics of the respondents were analysed using SPSS Version 27. The values for each variable and questionnaire item were calculated using the mean and standard

deviation. The Cronbach's Alpha was set at 0.6 to determine the main variables set's reliability following the recommendation of Phetnoi et al. (2021) and Jandawapee et al. (2022). The validity test was conducted using the factor loadings and was set at 0.6 following the study of Bootsumran et al. (2021). The researchers employed a partial least square structural equation model (ADANCO 2.3) to confirm the conceptual model, and the completed data were analysed to test the hypotheses. SRMR was set to less than 0.08, and AVE was charged at 0.5, followed by the study of Jaipong et al. (2022), Limsangpetch et al. (2022), and Siripipattanakul et al. (2022).

RESULTS

Four hundred fourteen (414) Thai mobile banking users completed online questionnaires. The majority of respondents were female (59.7%), from the Central part (47.6%), single (68.1%), older than 41 years old (26.1%), had a bachelor's degree (51.9%), worked as an employee (34.5%), and earned more than 50,000 baht (19.8%). Table 1 shows item loadings, mean, standard deviation (SD), Cronbach's Alpha, and average variance extracted (AVE). The Cronbach's Alpha was set at 0.6 to determine the main variables set's reliability. Additionally, the validity test was conducted using the factor loadings and was set at 0.6.

Table 1. Item Loadings, Cronbach's Alpha, and Average Variance Extracted (n=414)

Items	Factor Loadings	Mean	SD.
Cyber Security Knowledge (CSK) Cronbach's Alpha = 0.802, AVE = 0.504			
CSK1: Lack of proper training and awareness of security issues concerning staff leads to high threat and data loss, especially in mobile banking.	0.631	4.65	0.623
CSK2: Internal compromise is more dangerous/undetectable as compared to external.	0.685	4.70	0.616
CSK3: Due to the countermeasure banking segment is more eye-catching for Intruders, whereas its mobile banking atmosphere has more vulnerabilities.	0.719	4.64	0.617
CSK4: Usage of unregistered or unlicensed software is an easy way to backdoor in mobile banking.	0.679	4.70	0.622
CSK5: Proper authentication mechanism leads to customer satisfaction and enhances users' confidence.	0.825	4.76	0.520
CSK6: Avoiding sharing personal IDs can also minimise security breaches.	0.704	4.87	0.378

Table 1. Item Loadings, Cronbach's Alpha, and Average Variance Extracted (n=414) (cont.)

Items	Factor Loadings	Mean	SD.
Cyber Security Awareness (CSA) Cronbach's Alpha = 0.791, AVE = 0.618			
CSA1. Cyber Security of mobile banking is essential to the community or society.	0.868	4.78	0.558
CSA2. Awareness of the Cyber Security of mobile banking is essential for the community or society, especially for my family, friends and relatives.	0.775	4.83	0.431
CSA3. Cyber Security of mobile banking is mandatory for the users.	0.797	4.78	0.553
CSA4. Before using mobile banking applications, basic training is essential for the community, especially youngsters.	0.696	4.57	0.729
Behavioural Choice Protection (BCP) Cronbach's Alpha = 0.793, AVE = 0.550			
BCP1: Cyber Security recommends protecting your valuable data using a dense/strong password.	0.772	4.68	0.602
BCP2: According to Cyber Security policy, numerous password adjustments can heighten the secure environment.	0.610	4.56	0.805
BCP3: Using recommended antivirus software or firewall can attain a supreme level of data protection.	0.788	4.55	0.654
BCP4: Using municipal systems or unspoilt net password is equivalent to a honeypot, which is high risk and not recommended.	0.714	4.68	0.623
BCP5: Usage of registered or recommended hardware/software can be advantageous and maximise the data protection from Malware.	0.806	4.79	0.465

Table 2. R-Squared (n=414)

Construct	Coefficient of Determination (R^2)	Adjusted R^2
Cyber Security Knowledge	0.4104	0.4089
Cyber Security Awareness	0.4783	0.4758

According to Table 2, the coefficient of determination to predict cyber security knowledge equals 0.4104 or can be explained by predictors of about 41.04%. The coefficient of determination to predict cyber security awareness equals 0.4783 or can be explained by predictors of about 47.83%. The adjusted R-square to explain cyber security knowledge and cyber security awareness equals 0.4089 and 0.4758, respectively.

Table 3. Effect Overview (n=414)

Effect	Beta	Indirect Effect	Total Effect	Cohen's f^2
CSK → CSA	0.6406		0.6406	0.6960
CSK → BCP	0.5898	0.0928	0.6826	0.3931
CSA → BCP	0.1449		0.1449	0.0237

Table 3 shows the effect overview, including effects, Beta, indirect effect, total effect and Cohen's f^2. The high beta values mean higher predictive power.

Table 4. Total Effects Inference (n=414)

Effect	Original Coefficient	Standard Bootstrap Results					Percentile Bootstrap Quantiles		
		Mean Value	Standard Error	T-Value	P-Value (2-Sided)	P-Value (1-Sided)	0.5%	2.5%	97.5%
CSK → CSA	0.6406	0.6432	0.0494	12.9607	0.0000	0.0000	0.4970	0.5480	0.7351
CSK → BCP	0.5898	0.5916	0.0448	13.1498	0.0000	0.0000	0.4634	0.5000	0.6763
CSA → BCP	0.1449	0.1497	0.0580	2.4984	0.0126	0.0063	-0.0026	0.0333	0.2708

CSK = Cyber Security Knowledge; CSA = Cyber Security Awareness; BCP = Behavioural Choice Protection

Table 4 shows the total effect influence. The relationship between factors and outcomes is shown in the effects. The higher original coefficients mean the higher predictor powers. The standard bootstrap results comprise mean, standard error, T-value, p-value (2-tailed) and p-value (1-tailed). The percentile Bootstrap Quartiles comprise 0.5%, 2.5% and 97.5%, respectively. The significance level of 95% is accepted at p-values less than 0.05. The significance level of 99% is accepted at a p-value less than 0.01. And the significance level of 99.9% is accepted at a p-value less than 0.001.

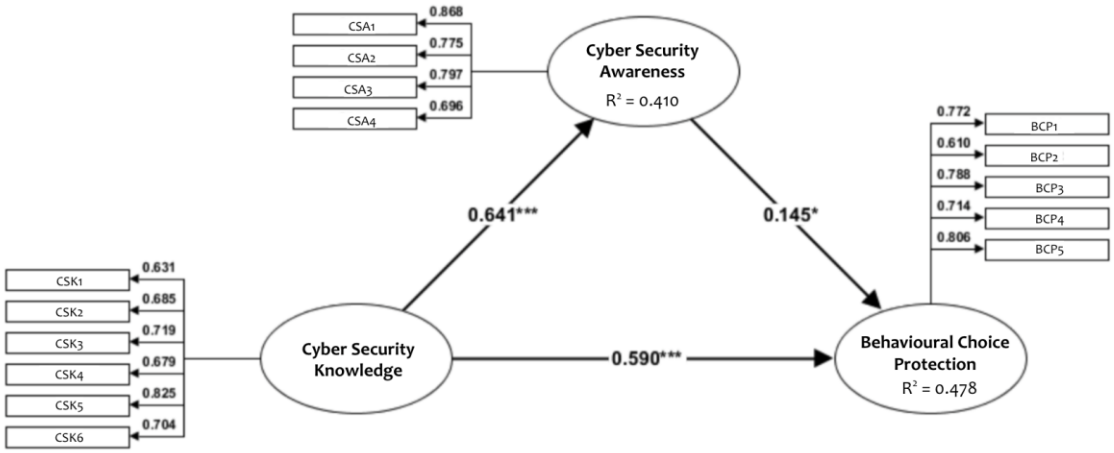

Figure 2. PLS-SEM Model of the Study (SRMR=0.0853)

According to Figure 2, cyber security knowledge can predict cyber security awareness at β=0641, p<0.001 (two tails at 0.0000 and one tail at 0.0000). Cyber security knowledge can predict behavioural choice protection at β=0.590, p<0.001 (two tails at 0.0000 and one tail at 0.0000). Cyber security awareness can predict behavioural choice protection at β=0.145, p<0.05 (two tails at 0.0126 and one tail at 0.0063). Cyber security awareness is a significant mediator between cyber security knowledge and behavioural choice protection by 41.0% (R^2=0.410). Overall, the relationship phenomenon can be explained by 47.8% (R^2=0.478).

Assumptions

Table 5. Summary of Hypothesis Testing

Hypotheses	Results	Actions
H1: Cyber Security Knowledge → Cyber Security Awareness	β=0.6406 at p<0.001	Supported
H2: Cyber Security Knowledge → Behavioural Choice Protection	β=0.5898 at p<0.001	Supported
H3: Cyber Security Awareness → Behavioural Choice Protection	β=0.1449 at p<0.05	Supported
H4: Cyber Security Awareness is the Mediator between Cyber Security Knowledge and Behavioural Choice Protection	R^2=0.410 at p<0.05	Supported

Overall, the relationship phenomenon can be explained by 47.8% (R^2=0.478).

Table 5 shows the summary of hypothesis testing. Cyber security knowledge significantly influences cyber security awareness. Cyber security knowledge significantly influences behavioural choice protection. Cybersecurity awareness significantly influences behavioural choice protection. Moreover, cyber security awareness is the significant mediator between cyber security knowledge and behavioural choice protection. Therefore, H1, H2, H3, and H4 in this study are all supported. Overall, the relationship phenomenon can be explained by about 47.8% (R^2=0.478).

DISCUSSION

The study's PLS-SEM model confirmed the proposed conceptual framework. The findings indicate that cyber security knowledge can predict cyber security awareness and behavioural choice protection. Cyber security awareness can predict behavioural choice protection. Moreover, cyber security awareness is a significant mediator between cyber security knowledge and behavioural choice protection. Moreover, the findings supported the previous research of Bada et al. (2019) and Zwilling et al. (2022) that cyber security knowledge significantly influences cyber security awareness and behavioural choice protection. Knowledge and awareness about cyber security were necessary but insufficient for changing behaviour, and they needed to be combined with other influencing strategies. It was critical to instil positive cyber security behaviours, which could lead to thinking becoming a habit and becoming part of a company's cyber security infrastructure. Furthermore, the findings supported Mamonov and Benbunan-Fich (2018) that the awareness of information security threats improved behavioural choice protection, such as increasing the strength of newly chosen passwords. The findings supported the previous research of Van der Schyff and Flowerday (2021) that security awareness acted as a mediator for some personality traits. It was discovered that information security awareness, in particular, acted as an indirect mediator between openness and the intention to review privacy settings. As users with a high level of openness became more aware of privacy-related threats (e.g. via privacy news and events), their desire to review privacy settings increased. Moreover, information security awareness, albeit in a complementary fashion, mediated the relationship between conscientiousness and intention to review privacy settings. Therefore, cyber security knowledge and awareness are vital for influencing behavioural choice protection among Thai mobile banking users. Hence, banks should devise an effective cybersecurity strategy to meet mobile banking users' needs and expectations. As a result, the number of mobile banking users may increase. High business performance will occur.

CONCLUSION

Cyber security knowledge and awareness are crucial to influencing the behaviour of Thai mobile banking users in terms of protection. To meet the needs and expectations of

mobile banking users, therefore, banks must develop an effective cyber security strategy. Consequently, there may be a rise in mobile banking users, and business performance may increase. Cyber security knowledge could be increased by enhancing perceptions that personal sharing IDs can also minimise security breaches. Cyber security awareness could be increased by enhancing awareness of the Cyber Security of mobile banking because it is essential for the community or society, especially for my family, friends, and relatives. Behavioural choice protection could be increased by enhancing perceptions about the usage of registered or recommended hardware and software can be advantageous and maximise data protection from Malware. Therefore, to develop behavioural choice protection, cyber security knowledge and awareness should be paid attention to in the banking industry and any sector.

RESEARCH IMPLICATION

The implications could be applied to any sector in explaining the association between cybersecurity awareness, knowledge and behavioural choice protection among mobile banking application customers or other sectors in Thailand. In addition, this study contributed to the existing body of literature on cybersecurity awareness, knowledge, and behavioural choice protection. The findings of this study may help academics expand their research by incorporating additional potential factors. These metrics could guide future cybersecurity research and its outcomes in the digital era.

LIMITATIONS AND RECOMMENDATIONS

This study employed sampling to explain only mobile banking from customers' perceptions. It may not cover other sectors. There should be increased sampling in a variety of industries. This study also consists of a self-administered questionnaire for quantitative analysis. Thus, more insightful analysis through qualitative research, including observations and focus groups, could also explain the association between cyber security awareness, knowledge and behavioural choice protection among mobile banking application customers or other sectors in Thailand.

ACKNOWLEDGEMENT

The authors acknowledge Professor Dr. Khalid Hussain for his encouragement and suggestion on the validity of the questionnaire during the instrumentation process.

DECLARATIONS

Conflict of Interest

There is no conflict of interest.

Informed Consent

It may not be applicable because the respondents were asked to participate in answering the questionnaire before questionnaire distribution.

Ethics Approval

It may not be applicable because the respondents were asked to participate in answering the questionnaire before questionnaire distribution. Moreover, no human or animal subjects were involved in this study.

REFERENCES

Abawajy, J. (2014). User Preference of Cyber Security Awareness Delivery Methods. *Behaviour & Information Technology*, *33*(3), 237-248.

Aldiabat, K., Al-Gasaymeh, A., & K.Rashid, A. S. (2019). The Effect of Mobile Banking Application on Customer Interaction in the Jordanian Banking Industry. *International Journal of Interactive Mobile Technologies, 13*(02), 37–49.

Alghazo, J. M., Kazmi, Z., & Latif, G. (2017). Cyber Security Analysis of Internet Banking in Emerging Countries: User and Bank Perspectives. In *2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences*, pp. 1-6. IEEE.

Al-Jabri, I. M., & Sohail, M. S. (2012). Mobile Banking Adoption: Application of Diffusion of Innovation Theory. *Journal of Electronic Commerce Research*, *13*(4), 379-391.

Almaiah, M. A., Al-Zahrani, A., Almomani, O., & Alhwaitat, A. K. (2021). Classification of Cyber Security Threats on Mobile Devices and Applications. *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*, 107-123. Springer, Cham.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A Review of Using Gaming Technology for Cyber-Security Awareness. *International Journal for Information Security Research, 6*(2), 660-666.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). *Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?*, pp. 1-11. https://doi.org/10.48550/arXiv.1901.02672.

Bootsumran, L., Siripipatthanakul, S., & Phayaphrom, B. (2021). Factors Influencing Consumers' Purchase Intention at Pharmacies in Thailand. *Journal of Management in Business, Healthcare and Education*, *1*(1), 1-16.

Chana, P., Siripipatthanakul, S., Phayaphrom, B., & Nurittamont, W. (2021). Effect of the service marketing mix (7Ps) on patient satisfaction for clinic services in Thailand. *International Journal of Business, Marketing and Communication, 1*(2), 1-12.

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies. *Government Information Quarterly*, *34*(1), 1-7.

Devadevan, V. (2013). Mobile Banking in India–Issues & Challenges. *International Journal of Emerging Technology and Advanced Engineering*, *3*(6), 516-520.

Dlamini, Z., & Modise, M. (2012). Cyber Security Awareness Initiatives in South Africa: A

Synergy Approach. *International Conference on Cyber Warfare and Security* (pp. 98-107). Academic Conferences International Limited.

Hussain, A., Abubakar, H. I., & Hashim, N. B. (2014). Evaluating Mobile Banking Application: Usability Dimensions and Measurements. *Proceedings of the 6th International Conference on Information Technology and Multimedia*, pp. 136-140.

Ingkathawornwong, P. (2020). Internet Banking Security: Human-Centered Issues in the Context of Thailand. *Humanities, Arts and Social Sciences Studies*, 20(1), 163-218.

Iyengar, S. S., & Lepper, M. R. (2000). When Choice is Demotivating: Can One Desire Too Much of a Good Thing? *Journal of Personality and Social Psychology*, *79*(6), 995–1006. doi.org/10.1037/0022-3514.79.6.995.

Jaipong, P., Siripipatthanakul, S., Sitthipon, T., Kaewpuang, P., & Sriboonruang, P. (2022). An Association Between Brand Trust, Brand Affection and Brand Loyalty: The Case of a Coffee Brand in Bangkok Thailand. *Advance Knowledge for Executives*, 1(1), No. 1, 1-14. Available at SSRN: 4143568.

Jandawapee, S., Siripipatthanakul, S., Phayaphrom, B., & Limna, P. (2022). Factors Influencing Intention to Follow the Preventive COVID-19 Protocols Among Thai People. *International Journal of Behavioral Analytics*, 2(1), 1-15.

Kraiwanit, T., & Srijaem, P. (2021). Evaluation of Internet Transaction Fraud in Thailand. *Indian Journal of Economics & Business*, *20*(1), 195-204.

Kruger, H., Drevin, L., & Steyn, T. (2010). A Vocabulary Test to Assess Information Security Awareness. *Information Management & Computer Security, 18*,(5), 316-327. https://doi.org/10.1108/09685221011095236

Kwateng, K. O., Atiemo, K. A. O., & Appiah, C. (2018). Acceptance and Use of Mobile Banking: An application of UTAUT2. *Journal of Enterprise Information Management*,*32*(1), 118-151. https://doi.org/10.1108/JEIM-03-2018-0055.

Limna, P., Sitthipon, T., Siripipattanakul, S., Jaipong, P., & Auttawechasakoon, P. (2022). The Mediating Effect of Job Satisfaction Between the Relationship of Ethical Change Management and Organisational Performance in Thailand. *Review of Advanced Multidisciplinary Sciences, Engineering & Innovation*, *1*(1), 1-15.

Limsangpetch, V., Siripipatthanakul, S., Phayaphrom, B., & Limna, P. (2022). Modelling Knowledge Management on Business Performance Through Mediating Role of Organisational Innovation Among IT Staff in Bangkok, Thailand. International *Journal of Behavioral Analytics,* 2(2), 1-17.

Loetrueangnapha, N., & Kraiwanit, T. (2019). Financial Transactions Through Banking Agency Selections In Thailand. *International Journal* of *Business and Management,* 7(1), 63-73. DOI: 10.20472/BM.2019.7.1.005.

Mamonov, S., & Benbunan-Fich, R. (2018). The Impact of Information Security Threat Awareness on Privacy-Protective Behaviors. Computers *in Human Behavior*, *83*, 32-44. https://doi.org/10.1016/j.chb.2018.01.028.

Misra, R. K., & Khurana, K. (2017). Employability Skills among Information Technology Professionals: A Literature Review. *Procedia Computer Science*, *122*, 63-70.

Munoz-Leiva, F., Climent-Climent, S., & Liébana-Cabanillas, F. (2017). Determinants of

Intention to Use the Mobile Banking Apps: An Extension of the Classic TAM Model. *Spanish Journal of Marketing-ESIC*, *21*(1), 25-38.

Napawut, W., Siripipatthanakul, S., Phayaphrom, B., Siripipattanakul, S., & Limna, P. (2022). The Mediating Effect of E-WOM on the Relationship Between Digital Marketing Activities and Intention to Buy Via Shopee. *International Journal of Behavioral Analytics, 2*(2), 1-13.

Navavongsathian, A., Vongchavalitkul, B., & Limsarun, T. (2020). Causal Factors Affecting Mobile Banking Services Acceptance by Customers in Thailand. *The Journal of Asian Finance, Economics and Business*, *7*(11), 421-428.

Phetnoi, N., Siripipatthanakul, S., & Phayaphrom, B. (2021). Factors Affecting Purchase Intention Via Online Shopping Sites and Apps During COVID-19 in Thailand. *Journal of Management in Business, Healthcare and Education*, *1*(1), 1-17.

Puriwat, W., & Tripopsakul, S. (2017). Mobile Banking Adoption in Thailand: An Integration of Technology Acceptance Model and Mobile Service Quality. *European Research Studies Journal, 20*(4B), 200-210.

Ruangkanjanases, A., & Wongprasopchai, S. (2018). Adoption of Mobile Banking Services: An Empirical Examination between Generation Y and Generation Z in Thailand. *International Journal of Organizational Business Excellence*, *1*(1), 1-12.

Scholefield, S., & Shepherd, L. A. (2019). Gamification Techniques for Raising Cyber Security Awareness. In *International Conference on Human-Computer Interaction* (pp. 191-203). Springer, Cham.

Senarak, C. (2021). Cybersecurity Knowledge and Skills for Port Facility Security Officers of International Seaports: Perspectives of IT and Security Personnel. *The Asian Journal of Shipping and Logistics*, *37*(4), 345-360.

Shaikh, A. A., & Karjaluoto, H. (2015). Mobile Banking Adoption: A Literature Review. *Telematics and Informatics*, *32*(1), 129-142.

Si Dah, N., Siripipatthanakul, S., Phayaphrom, B., & Limna, P. (2022). Determinants of Employee Innovation: A Case of NGOs and CSOs in Mae Sot, Thai-Myanmar Border. *International Journal of Behavioral Analytics, 2*(1), 1-15.

Siripipattanakul, S., Siripipatthanakul, S., Limna, P., & Auttawechasakoon, P. (2022). The Relationship Between Website Quality, University Image, e-WOM and Intention to Follow the University Website. *Psychology and Education Journal*, *59*(2), 529-544. Retrieved from SSRN: 4120462.

Siripipatthanakul, S., Limna, P., Siripipattanakul, S., & Auttawechasakoon, P. (2022). The Relationship Between Content Marketing, E-Promotion, E-WOM and Intentions to Book Hotel Rooms in Thailand. *Asia Pacific Journal of Academic Research in Business Administration*, *8*(2), 35-42.

Sitthipon, T., Limna, P., Jaipong, P., Siripipattanakul, S., & Auttawechasakoon, P. (2022). Gamification Predicting Customers' Repurchase Intention Via E-Commerce Platforms Through Mediating Effect of Customer Satisfaction in Thailand. *Review of Advanced Multidisciplinary Sciences, Engineering & Innovation, 1*(1), 1-14.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information Security Management Needs

More Holistic Approach: A Literature Review. *International Journal of Information Management*, *36*(2), 215-225.

Van der Schyff, K., & Flowerday, S. (2021). Mediating Effects of Information Security Awareness. *Computers & Security*, *106*, 102313. https://doi.org/10.1016/j.cose.2021.102313.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62(1), 82-97.