УДК 330.46:336.7
JEL Classification G20, G21
DOI https://doi.org/10.33146/2307-9878-2022-2(96)-58-67

Hasibul ISLAM[1]
Pabna University of Science and Technology, Pabna, Bangladesh

Jhansi Bharathi MADAVARAPU[2]
University of Cumberlands, Cumberland, USA

Nayan Kumar SARKER[3]
Pabna University of Science and Technology, Pabna, Bangladesh

Md. Asfaqur RAHMAN[4]
Pabna University of Science and Technology, Pabna, Bangladesh

The Effects of Cyber Threats and Technical Problems on Customer's Attitude Towards E-Banking Services

Abstract. *The study showed the effect of cyber threats or technical problems on customer attitude towards e-banking services. A self-administered questionnaire was used to collect the data, and 400 respondents from eight divisions (Dhaka, Barisal, Rangpur, Chittagong, Khulna, Mymensingh, Rajshahi, and Sylhet) participated in the study. The researcher used a linear regression model to assess the relationship between dependent and independent variables. STATA and SPSS v. 25 program environment were used to conduct the statistical analysis. To determine the reliability of the data, Cronbach's Alpha was conducted and found acceptable internal consistency. Protection method (PM), Purposes of using e-banking (PUE), and Technical problems and challenges (TPC) were the independent variables. The dependent variables were ease of use (EU) and Security reason (SR). The study used two regression models for two dependent variables. The regression model (1) showed a significant effect of SR on PM, and there was no significant effect on SR on PUE and TPC. Another regression model (2) showed a significant effect of EU on PM and PUE, and there was no significant effect of EU on TPC. However, the total variance explained was still low in model 1 (22.6%) and model 2 (44.9). The people of Bangladesh should be aware of e-banking services and technical problems. Future research should be conducted to discover more data and other variables affecting customer attitudes towards e-banking.*

Keywords: *Cyber Threats, E-banking, Security, Ease of Use, Technical Problems.*

Suggested Citation
Islam, H., Madavarapu, J. B., Sarker, N. K., Rahman, A. (2022). The Effects of Cyber Threats and Technical Problems on Customer's Attitude Towards E-Banking Services. *Oblìk ì finansi, 2(96),* 58-67. https://doi.org/10.33146/2307-9878-2022-2(96)-58-67

[1] **Hasibul ISLAM**, Pabna University of Science and Technology, Pabna, Bangladesh.
ORCID 0000-0002-3242-2502
E-mail: hasibulislamshanto143@gmail.com (*Corresponding author*)

[2] **Jhansi Bharathi MADAVARAPU**, University of Cumberlands, Cumberland, USA.
ORCID 0000-0001-8478-6626

[3] **Nayan Kumar SARKER**, Pabna University of Science and Technology, Pabna, Bangladesh.
ORCID 0000-0001-8162-1412

[4] **Md. Asfaqur RAHMAN**, Pabna University of Science and Technology, Pabna, Bangladesh.
ORCID 0000-0001-6358-1744

Хасібул ІСЛАМ
Університет науки і технологій Пабна, м. Пабна, Бангладеш

Джхансі Бхаранті МАДАВАРАПУ
Камберлендський університет, м. Камберленд, США

Наян Кумар САРКЕР
Університет науки і технологій Пабна, м. Пабна, Бангладеш

Асфакур РАХМАН
Університет науки і технологій Пабна, м. Пабна, Бангладеш

Вплив кіберзагроз і технічних проблем на ставлення клієнтів до послуг електронного банкінгу

Анотація. *Це дослідження присвячене вивченню впливу кіберзагроз та технічних проблем на ставлення клієнтів до послуг електронного банкінгу. Для збору даних було використано анкету, самостійно розроблену авторами. В анкетуванні взяли участь 400 респондентів з восьми відділів (Дака, Барісал, Рангпур, Чіттагонг, Кхулна, Міменсінгх, Раджшахі та Сілхет). Дослідники використали модель лінійної регресії для оцінки зв'язку між залежними та незалежними змінними. Для проведення статистичного аналізу було використано програмне забезпечення STATA та SPSS версії 25. Оцінка достовірності даних була проведена на основі використання коефіцієнта Альфа Кронбаха та виявила прийнятну внутрішню узгодженість даних. Незалежними змінними були метод захисту (PM), цілі використання електронного банкінгу (PUE) та технічні проблеми та перешкоди (TPC). Залежними змінними були: простота використання (EU) та міркування безпеки (SR). У дослідженні використовувалися дві моделі регресії для двох залежних змінних. Регресійна модель (1) показала значний вплив міркувань безпеки на метод захисту. При цьому не було виявлено істотного впливу цілі використання електронного банкінгу та технічні проблеми та перешкоди. Інша регресійна модель (2) показала значний вплив простоти використання на метод захисту та цілі використання електронного банкінгу. При цьому не було суттєвого впливу простоти використання на технічні проблеми та перешкоди. Проте, загальна пояснена дисперсія все ще була низькою в моделі 1 (22,6%) і моделі 2 (44,9). Таким чином, жителі Бангладеш повинні знати про послуги електронного банкінгу та технічні проблеми, що можуть виникнути притакому обслуговуванні. Необхідно провести подальші дослідження, щоб зібрати більше даних та виявити інші змінні, які впливають на ставлення клієнтів до електронного банкінгу.*

Ключові слова: *кіберзагрози, електронний банкінг, безпека, простота використання, технічні проблеми.*

INTRODUCTION

Because of the tremendous development in cybercrime in the twenty-first century, financial institutions are more concerned about protecting their digital assets, becoming more crucial than ever before. Cybercrime is one of the most pressing concerns facing the world's online banking business today, and it affects every country. Organizations must understand the consequences of cybercrime in order to develop suitable measures. Organizations in the financial sector must be aware of online risks and consider any measures that can aid in raising the level of public awareness about security and ensuring a long-term sustainable financial business environment. The financial integrity of financial institutions and other organizations is not the only thing that can be compromised by cybercrime. Organizations must understand the consequences of cybercrime in order to develop suitable measures. Organizations in the financial sector must be aware of online risks and consider any measures that can aid in raising the level of public awareness about security and ensure a long-term sustainable financial business environment (Prem Khatri, 2019). Information Technology and mobile networks have grown rapidly in recent years, resulting in the establishment of an information society in the modern world. Even though this development allows and facilitates computer users to collect information at their fingertips, some difficulties must be considered. When it comes to working with online banking services, it is vital to understand the behavior of online banking consumers. In today's information-technology-driven society, the worry of losing personal information or becoming a victim of online banking services is still very much alive. Security engineers employ a variety of strategies in order to deliver safe financial platforms. On the other hand, computer fraudsters and criminals are only a few steps ahead.

The adoption of technology by its users has emerged as a critical indicator of the success of that technology (Safeena et al., 2011). For Internet banking to be properly carried out, a basic understanding of computers and the Internet is required, limiting the number of people willing to take advantage of this convenience. Many people, particularly those unfamiliar with computers and the Internet, find it difficult to conduct Internet banking transactions. As a result, Internet banking takes a significant amount of time for new users. In addition, when it comes to financial matters, people have difficulty

placing their trust in a completely automated system such as Internet banking. When something as simple as clicking the wrong button goes wrong, it can cause significant damage. Technology advances regularly and affects practically every part of life, yet nothing that hinders progress is embraced. Everyone considering adopting new technology will acquire and synthesize all available facts to build a belief about using the technology, which will eventually determine whether the individual accepts or rejects the new technology. When users are satisfied with technology, it is more probable that they will adopt it (Akhlaq et al., 2011; Davis, 1986).

Furthermore, the Technology Acceptance Model (TAM) claims that users' acceptance of technology is based on their preferences. Two aspects influence how people use technology: perceived ease of use and perceived utility (or utility). Determining users' attitudes toward new technologies has proven to be one of the most difficult challenges in the technology adoption literature. One of the most difficult topics in the technology adoption literature has been determining users' attitudes about new technologies. The growing number of people who utilize internet banking implies that internet banking is becoming more widely accepted. Several things can influence the level of adoption of online baking. The TAM (Technology Acceptability Model) is a model for describing the level of acceptance of information technology (IT) (Davis, 1989). The perceived usefulness and simplicity of use of information technology are the key variables driving information technology acceptability. Before information technology can be converted into actual application in daily life, both of these characteristics impact the intention to utilize it (Davis 1989). The goal of this study was to assess consumer awareness of cyber risks and e-banking technical issues and their impact on banking services use.

Research Objectives

The main objective of this study is to determine the effect of cyber threats on the consumer behavior of e-banking services. Some other objectives are given below:

- To examine the relationship between protection method (PM) and ease of use (EU) and security reason for the use of e-banking (SR).
- To investigate the relationship between the purpose of using e-banking (PUE) and security reason (SR), and ease of use of e-banking (EU).
- To analyze the association between technical problems and challenges (TPC) and security reasons (SR), and ease of use of e-banking (EU).

LITERATURE REVIEW

Salihu et al. (2019) conducted a study about ease of use on declining the problems of e-banking. The study provides a statistical analysis through a distributed questionnaire to examine the effect of security and ease of use in decreasing issues with electronic banking. Regression analysis demonstrates that security and ease of use of electronic banking services have a negative effect on issues with electronic banking services, which implies that with enhanced security and/or ease of use, their issues are decreased. Security has a negative effect on problems of electronic banking services. The use of technology in e-banking has been rejected, according to Zanoon and Gharaibeh (2013). This will be discussed in this paper by offering some security gaps that are resulting from the low level of customer knowledge in information technology, and that will be studied through the Technology Acceptance Model and other methods.

In light of this, we will offer some suggestions for improvement. Another study on customers' trust in the e-banking system in Bangladesh was conducted by Sadekin et al. (2019). The study findings indicate that customers' trust is primarily dependent on security measures, customer awareness, educational qualification, authentication of e-transactions, e-service quality of banks, and bankers' behavior, among other factors. One or more security safeguards safeguard every step of the online banking process. One of the most significant factors in establishing trust in e-banking is raising the level of customer awareness. People with a low level of education are apprehensive about conducting e-banking transactions. Customers' trust in a product or service is closely tied to problems or difficulties. If customers have difficulty completing an e-transaction, their trust in the company will be diminished. This research also involves investigating a variety of notable successes in e-banking operations to help small-to-medium-sized firms, according to Karim and Gide (2019). (SMEs). These research strategies also contribute to the field by developing reliable assessments of e-banking infrastructure, e-banking success, and future organizational structure in Bangladesh, filling a critical gap.

Ugwuja et al. (2019) examined women agro entrepreneurs' cyber risk exposures and cybersecurity preparation. Women were in danger of having their accounts debited due to failed transactions via mobile applications and POS. They were also vulnerable to social engineering threats such as smishing and vishing. The women took a few precautions when it came to cybersecurity, such as avoiding lonely ATMs and ignoring text messages and emails requesting financial information. Connection to digital financial products and services was influenced by household size, cooperative membership, educational level, and internet access. These findings advocate for additional interventions in the form of legislation that improve customer education to lessen vulnerabilities, particularly among women. Vimala (2016) conducted a study about e-banking security in Indian banks and found that the traditional banking system has no substantial interaction with internet banking. Customers are unaffected by the security of online banking. The current research is being carried out with the use of an appropriate research tool. The responses of 50 customers were used to create an analysis, which was followed by a few suggestions. According to Ahmad and Soleymani (2013), trust has a favorable impact on the uptake of Internet banking is supported by research.

Furthermore, the findings indicate that there are a variety of elements that influence trust in electronic

services. The vast majority of the research has been carried out in Internet-based banking. Ali et al. (2017) critically analyzed and discussed the consequences of cyber dangers while interacting with online banking services, which they conducted as part of their research. According to the study's findings, there is a need to raise customer knowledge of the dangers of cybercrime when dealing with online banking and sensitive financial information.

Mansumitrchai and Chiu (2012) observed no statistically significant difference between adopters' and non-adopters attitudes toward security, third-party concern, and financial status in a study on e-banking adoption in the United Arab Emirates (UAE). Mwiya et al. (2017) discovered that perceived utility, the convenience of use, and trust were the most important elements impacting bank customers' views about adopting e-banking services in Zambia. The most important elements impacting their attitudes toward using e-banking services, according to Mwiya et al. (2017), were perceived utility, the convenience of use, and trust.

According to Al-Smadi (2012), avoiding ambiguity has positive and bad consequences. Customers' attitudes were most highly influenced by their perceptions of risks, influencing their purchases. While perceived ease of use and considered usefulness significantly impacted perceptions, customers' attitudes were most strongly influenced by their perceptions of risks. Several factors influence customers' willingness to use e-banking services. Takele and Sira (2013) examined the factors that influenced their success using the TAM, TPB, and PR models. Customers' tendency to use e-banking service channels in Bahir Dar was influenced by attitude, subjective norm, perceived behavioral control, perceived benefit, perceived ease of use, and perceived risk. Alkailani (2016) revealed findings from a study conducted in Jordan that supported the expanded TAM model and demonstrated its resilience in anticipating customers' desire to adopt and use internet banking services in the future.

Hypothesis

H_1 = There is a significant relationship between the security reason of e-banking (SR) and the protection method (PM).

H_2 = There is a significant between the security reason of e-banking (SR) and the purpose of using e-banking (PUE).

H_3 = There is a significant relationship between the security reason of e-banking (SR) and technical problems and challenges (TPC).

H_4 = There is a significant relationship between ease of use of e-banking (EU) and protection method (PM).

H_5 = There is a significant relationship between ease of use of e-banking (EU) and the purpose of using e-banking (PUE).

H_6 = There is a significant relationship between ease of use of e-banking (EU) and technical problem and challenge (TPC).

Conceptual Model

The conceptual model in figure 1 shows that the dependent variables were security reasons and ease of use. The independent variables were the protection method, purposes of using e-banking, and technical problems and challenges. The researcher created this model to analyze the study. The researcher thought that these dependent variables greatly impacted independent variables.

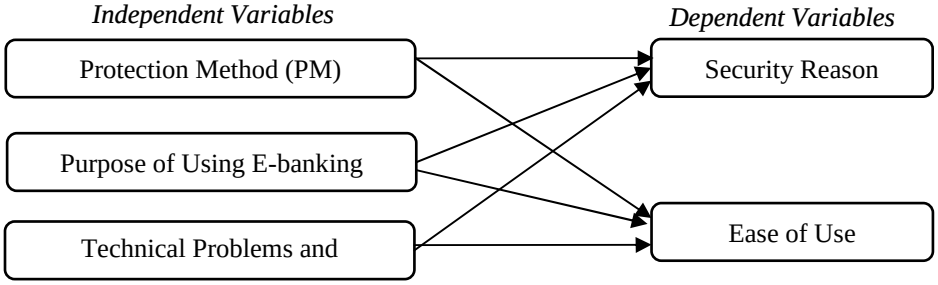

Figure 1. **Conceptual Model of the Study**

RESEARCH METHODOLOGY

To conduct this study, the researcher used a survey questionnaire that involved collecting data from the people of Bangladesh. The primary and secondary data were used to complete this study. A self-administrated questionnaire was used as primary data. Journals, books, newspapers, scientific papers, and magazines are the major secondary data source. The researcher collects 400 data to conduct this study. For this study, the researcher employed a convenience sampling method. The study's sample was gathered from eight Bangladeshi divisions (Dhaka, Chittagong, Rangpur, Barisal, Khulna, Mymensingh, Rajshahi, and Sylhet). For the empirical analysis of this study, data were acquired using self-administered questionnaires. The impact of factors was determined using the STATA and SPSS v. 25 computer environments.

Instrument Design

The protection method was determined using a five-point Likert scale. Respondents were asked to express their thoughts on security code, two-factor authentication, password protection, transaction security, database security, and file security. Using E-banking was also determined by Likert scale data. It had some factors, bill pay management, fund transfer, online ticket booking,

online shopping, income tax, service tax, and insurance premium. A five-point Likert scale determined technical problems and challenges, hacking attacks, unencrypted data, spoofing and loss of human touch, malware, phishing, illegal activities, and transaction activities. In addition, the other two variables asked for a response to Likert scale questions were security reason and ease of use. Likert scale (1-Strongly Disagree, 2- Disagree, 3- Neither Disagree, Nor Agree, 4- Agree, 5-Strongly Agree).

Normality Test

The normality test on the collected data is shown in Table 1. The test for normality provided by Kolmogorov-Smirnova and Shapiro–Wilk, as advanced by Shora and Kartono (2020). According to the test, the p-value for all of the variables is less than 0.05. As a result, the study rejects the null hypothesis, implying that the data were normally distributed in the study.

Table 1

Shapiro-Wilk Test

Variable	Observation	W	V	z	Prob>z
EU	400	0.961	10.797	5.661	0.000
SR	400	0.965	9.715	5.410	0.000
TPC	400	0.979	5.821	4.191	0.000
PUE	400	0.980	5.400	4.012	0.000
PM	400	0.896	28.619	7.981	0.000

Reliability Test

Cronbach's Alpha is a measure that is used to assess reliability. Table 3 shows the reliability test by using Cronbach's Alpha. If the Cronbach's Alpha (α) is greater than 0.9, internal consistency is Excellent. If the Cronbach's Alpha (α) is greater than or equal to 0.8 and less than 0.9, internal consistency is Good. If the Cronbach's Alpha (α) is greater than or equal to 0.7 and less than 0.8, internal consistency is Acceptable. If the Cronbach's Alpha (α) is greater than or equal to 0.6 and less than 0.7, internal consistency is Questionable. If the Cronbach's Alpha (α) is greater than or equal to 0.5 and less than 0.6, internal consistency is Poor. If the Cronbach's Alpha (α) is less than 0.5, internal consistency is Unacceptable (Hair et al., 2003). The researcher analyzed the Cronbach's Alpha and found Cronbach's Alpha (α) = 0.7607. The average inter-item covariance was 0.3981324, which means internal consistency is Acceptable.

Multicollinearity Test

Various criteria for appropriate levels of VIF have been presented in the literature about multicollinearity. Typically, a value of 10 is used as the maximum level of VIF (Hair et al., 1995; Kennedy, 1992; Marquardt, 1970;). The guideline of a VIF of 10 equates to a tolerance of .10. However, in other studies, a maximum VIF value of 5 (Rogerson, 2001) and even 4 (Pan & Jackson, 2008) has been suggested. The researcher found that the VIF value for PM, PUE, and TPC is less than three and the tolerance level is greater than 0.4; the table is given in the appendix section. So, multicollinearity is not problematic.

Regression Models

Since the data collected was ordinal, a Likert scale was used to create a composite score by computing the mean of all items for each latent variable (Subedi, 2016). Linear regression was used after finding the mean for all variables. Regression analysis was chosen to show the relationships between dependent and independent variables (Sarstedt & E. Mooi, 2014). The researcher proposed the following model to determine the relationship between independent and dependent variables.

$$Y_1 = \beta_0 + \beta_1 PM + \beta_2 PUE + \beta_3 TPC + \varepsilon$$

$$Y_2 = \beta_0 + \beta_1 PM + \beta_2 PUE + \beta_3 TPC + \varepsilon$$

Where:

- Y_1= Security Reason (SR);
- Y_2= Ease of Use (EU);
- PM= Protection Method (PM);
- PUE= Purposes of Using E-banking (PUE);
- TPC= Technical problems and challenges (TPC);
- ε = Error term;
- β= Beta.

ANALYSIS AND FINDINGS

Table 2 shows the demographic profile of the respondents. There were 38.5% of the respondents from Rajshahi, which was the highest of all the total 400 respondents. The lowest respondents are from Mymensingh, 0.8% of all the respondents. In the gender information, 56.3% of the respondents were male, and the remaining 43.8% were female. The occupation information showed that the highest number of respondents were students (66.3%). In the age information, there were 20 to 30 years old people who were the higher respondent (70.3%) in the study. In the case of monthly income-related information, 68.3% of respondents selected they had an income of below 20000. 60.3% of the people have savings accounts, and 39.8% of the people have a current account.

Table 2

Respondents Demographic

Demographic Information		Frequency	Percent
Location	Barisal	15	3.8%
	Chittagong	21	5.3%
	Dhaka	152	38.0%
	Khulna	21	5.3%
	Mymensingh	3	0.8%
	Rajshahi	154	38.5%
	Rangpur	13	3.3%
	Sylhet	21	5.3%
Sex	Female	175	43.8%
	Male	225	56.3%
Occupation	Banker	15	3.8%
	Businessman	24	6.0%
	Government Employee	15	3.8%
	Non-government Employee	24	6.0%
	Other	25	6.3%
	Student	265	66.3%
	Teacher	32	8.0%
Age	20 to 30	281	70.3%
	30 to 40	44	11.0%
	40 to 50	12	3.0%
	Below 20	63	15.8%
Monthly Income	20,000-30,000	39	9.8%
	30,000-40,000	35	8.8%
	40,000-50,000	21	5.3%
	Above 50,000	32	8.0%
	Below 20,000	273	68.3%
Types of Bank Account	Current Account	159	39.8%
	Savings Account	241	60.3%
	Total	400	100.0

Correlation Analysis

Pearson product-moment correlation was used for this study to determine the relationship between variables in table-3. There was a moderate positive correlation between ease of use and security reasons to use e-banking, with the r-value of 0.520. The r-value of ease of use and technical problem and challenges was 0.196, which shows a low correlation between variables. There was a moderate positive correlation between ease of use and purposes of using e-banking with a value of 0.553. The r-value of the protection method and ease of use was 0.651, which showed a moderated positive correlation between variables. There was a low positive correlation between security reasons and technical problems and challenges with the r-value of 0.141. The correlation value of security reasons and purposes of using e-banking was 0.351, which showed a weak relationship between variables. There was a moderate correlation between security reasons and protection methods, with a value of 0.473. There was a low correlation between technical problems and challenges and the purpose of using e-banking with the r-value of 0.174. The r-value of technical problem and challenges and protection method was 0.333, which showed a weak correlation between the variables. Lastly, there is a moderate correlation between purposes of using e-banking for security reasons and protection methods with the value of 0.4937.

Table 3

Correlation Analysis

Variables	EU	SR	TPC	PUE	PM
EU	1.000				
SR	0.520	1.000			
TPC	0.196	0.141	1.000		
PUE	0.553	0.351	0.174	1.000	
PM	0.651	0.473	0.333	0.668	1.000

Regression Analysis

Model 1

Table 4 indicates that model 1 was significant with a value of 0.000. The F value was 38.625, and the R2 value was 0.226, which shows the regression model fits this study. There was a significant association between the dependent variable (Security Reason) and independent variables (Technical problems and challenges, Purposes of Using E-banking, and Protection Method).

A linear regression test was used to determine the relationship between the dependent variable (Security Reason) and independent variables (Technical problems and challenges, Purposes of Using E-banking, and Protection Method). The coefficient of TPC was -0.14. It was negative and statistically not significant. This means there was a negative impact on TPC and SR. An increase of one unit of TPC will decrease by 0.014 the SR. The coefficient of PUE was 0.07. It was positive and statistically significant. This means there was a positive impact on PUE and SR. An increase of one unit of TPC will increase by 0.07 the SR. The coefficient of PM was 0.485. It was positive and statistically significant. This means there was a positive impact on PM and SR. An increase of one unit of PM will increase by 0.485 the SR.

There was a significant positive association between SR and PM. The standard error of PM was 0.069, showed higher confidence, and the p-value of PM was 0.000, which was less than 0.05. There was no significant impact of SR on PUE. The standard error of PUE was 0.068 also showed higher confidence, and the p-value of PUE was 0.302, which was greater than 0.05. There was no significant impact of SR on TPC. The standard error value of TPC was .0.045, which also showed high confidence, and the significance value of TPC was 0.75, which was greater than 0.05

Table 4

Linear Regression (Model 1)

SR	Coefficient	Standard Error	t value	p value	[95% Confidence	Interval]	Sig
TPC	-.014	.045	-0.32	.75	-.103	.074	
PUE	.07	.068	1.03	.302	-.063	.204	
PM	.485	.069	7.03	0	.349	.621	***
Constant	1.693	.235	7.20	0	1.231	2.156	***

Mean dependent var	3.915	SD dependent var	1.077
R-squared	0.226	Number of obs	400
F-test	38.625	Prob > F	0.000
Akaike crit. (AIC)	1099.085	Bayesian crit. (BIC)	1115.051

**** p<.01, ** p<.05, * p<.1*

Therefore, H_1 was accepted because there was a significant impact on SR and PM; the p-value was less than 0.05. H_2 and H_3 were rejected because there was no significant impact on SR and PUE, and the TPC p-value was greater than 0.05.

Model 2

Table 5 indicates that model 2 was significant with a value of 0.000. The F value was 107.515, and the R2 value was 0.449, which shows the regression model fits this study. There was a significant association between the dependent variable (Ease of Use) and independent variables (Technical problems and challenges, Purposes of Using E-banking, and Protection Method).

A linear regression test was used to determine the relationship between the dependent variable (Ease of Use) and independent variables (Technical problems and challenges, Purposes of Using E-banking, and Protection Method). The coefficient of TPC was -0.01. It was negative and statistically not significant. This means there was a negative impact on TPC and the EU. An increase of one unit of TPC will decrease by 0.01 in the EU. The coefficient of PUE was 0.209. It was positive and statistically significant. This means there was a positive impact on PUE and EU.

An increase of one unit of TPC will increase by 0.209 in the EU. The coefficient of PM was 0.492. It was positive and statistically significant. This means there was a positive impact on PM and EU. An increase of one unit of PM will increase by 0.492 in the EU.

There was a significant positive association between EU and PM. The standard error of PM was 0.05, showed higher confidence, and the p-value of PM was 0.000, which was less than 0.05. There was a significant impact of the EU on PUE. The standard error of PUE was 0.05 also showed higher confidence, and the p-value of PUE was 0.000, which was less than 0.05. There was no significant impact of the EU on TPC. The standard error value of TPC was 0.033, which also showed high confidence, and the significance value of TPC was 0.761, which was greater than 0.05.

Table 5

Linear Regression Model 2

EU	Coefficient	Standard Error	t value	p value	[95% Confidence	Interval]	Sig
TPC	-.01	.033	-0.30	.761	-.074	.054	
PUE	.209	.05	4.21	0	.111	.306	***
PM	.492	.05	9.78	0	.393	.59	***
Constant	1.363	.171	7.96	0	1.026	1.7	***

Mean dependent var	4.143	SD dependent var	0.930
R-squared	0.449	Number of obs	400
F-test	107.515	Prob > F	0.000
Akaike crit. (AIC)	845.515	Bayesian crit. (BIC)	861.481

**** p<.01, ** p<.05, * p<.1*

Therefore, H_4 and H_5 were accepted because there was a significant impact on EU, PM, and PUE; the p-value was less than 0.05. H_6 was rejected because there was no significant impact of EU and TPC; the p-value was greater than 0.05

CONCLUSIONS

According to an IBM X-Force Threat Intelligence Index survey, the financial industry had the largest cyberattacks out of all industries in the preceding three years until 2018. It is estimated that the banking industry alone was responsible for approximately a quarter of all cyberattacks. Furthermore, when it comes to coping with cyber assaults and their ramifications, the financial services industry bears the most financial burden. According to the 2019 Accenture research on the cost of cybercrime, the average cost of cybercrime per firm in the financial services industry was a whopping $18.5 million, significantly more than the average cost of cybercrime per company in any other vertical.

The banking industry is particularly vulnerable because of the high monetary worth of the data it holds. When hackers steal financial data and banking passwords, they either sell the information to high-bidders or use it to siphon off millions of dollars. Because of the increased digital presence of banks, the potential attack surface for these institutions has only risen in size. The digital transformation of this industry, which has included mobile applications, internet banking, and other online services, has also made it vulnerable to future attacks. While these digital banking solutions have made it easier for clients to obtain financial services, they have also introduced security holes that bad hackers can easily exploit. Banks and cybersecurity must work together to ensure data protection and safety for all parties involved. There are many technical problems and challenges faced by the people of Bangladesh while using E-banking services. So that the researcher tests the hypothesis based on the aim of this study. The researcher used regression analysis to test the hypothesis.

The regression model (1) showed a positive relationship between using e-banking for security reasons and the protection method. That means people's use of e-banking is strongly influenced by the protection methods used for e-banking safety. On the other hand, there was no significant impact on using e-banking for security reasons and using e-banking. People use e-banking for various reasons though they do not have sufficient knowledge about e-banking technical threats. There was no significant impact on security reasons and technical problems and challenges. People do not become aware of cyber threats of e-banking.

The regression model (2) showed a positive relationship between ease of use and protection method. Protection methods make it easier to use e-banking and create a positive relationship using e-banking. Ease of use affects the purposes of using e-banking. There was no significant impact on the ease of use and technical problems and challenges. That means technical problems and challenges negatively affect the ease of use of e-banking.

	Hypothesis	Accept/reject (H_0)	Accept/reject (H_1)
H_1	There is a positive relationship between using e-banking for security reasons and protection method	Reject	**Accept**
H_2	There is a positive relationship between using e-banking for security reasons and the purpose of using e-banking	Accept	Reject
H_3	There is a positive relationship between using e-banking for security reasons and technical problems and challenges	Accept	Reject
H_4	There is a positive relationship between ease of use of e-banking and protection method	Reject	**Accept**
H_5	There is a positive relationship between the ease of use of e-banking and the purpose of using e-banking	Reject	**Accept**
H_6	There is a positive relationship between ease of use of e-banking and technical problem and challenges	Accept	Reject

Recommendations

Based on the findings, the researcher recommends the followings:

- Educating online banking users about the tools and techniques used when dealing with online banking services will help increase their level of confidence.
- The use of secure application software must be introduced, or its use should be increased to increase the number of layers of protection for online banking.
- It is necessary to develop more sophisticated and robust systems to monitor the activities of computer fraudsters and cybercriminals hackers to make certain that they do not gain unauthorized access to the financial information of online customers.
- In order to achieve this goal, users of online banking services must be made more aware of available online threats, and the banking industry must take positive steps to accomplish this goal.
- Strong passwords and different user name combinations for different sites and accounts should be used by those who conduct online banking transactions.
- Customers who use e-banking should be better informed about the importance of using a secure online banking environment.

Furthermore, all users must take precautions to avoid being subjected to security threats.

4 References

1. Khatri, P. (2019). The importance of cyber security in banking. *The Global Treasurer.*
2. Salihu, A., Metin, H., Hajrizi, E., & Ahmeti, M. (2019). The effect of security and ease of use on reducing the problems/deficiencies of Electronic Banking Services. *IFAC-PapersOnLine, 52*(25), 159-163.
3. Ugwuja, V. C., Ekunwe, P. A., Henri-Ukoha, A. (2019). Cyber risks in electronic banking: exposures and cybersecurity preparedness of women agro-entrepreneurs in South-South Region of Nigeria. In *2019 Sixth International Conference*, September 23-26, 2019, Abuja, Nigeria 295693, African Association of Agricultural Economists (AAAE).
4. Vimala, V. (2016). An Evaluative Study on Internet Banking Security among Selected Indian Bank Customers. *Amity Journal of Management Research 1*(1), 63–79.
5. Ahmad, M. N., & Soleymani, S. A. (2013). Impact of Trust on Internet Banking Adoption: A Literature Review.
6. Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017). The effects of cyber threats on customer's behavior in e-Banking services. *International Journal of e-Education, e-Business, e-Management and e-Learning, 7*(1), 70-78.
7. Mansumitrchai, S., & Chiu, C. (2012). Adoption of internet banking in UAE: Factors underlying adoption characteristics. *International Journal of Management and Marketing Research, 5*(1), 103-115
8. Mwiya, B., Chikumbi, F., Shikaputo, C., Kabala, E., Kaulung'ombe, B., & Siachinji, B. (2017). Examining factors influencing e-banking adoption: Evidence from bank customers in Zambia. *Scientific Research Publishing, 7*, 741-759.

9. Al-Smadi, M. O. (2012). Factors affecting adoption of electronic banking: An analysis of the perspectives of banks' customers. *International Journal of Business and Social Science, 3*(17), 294-309. Retrieved from https://pdfs.semanticscholar.org/0c15/fa76f5ba4390 d52bcc d8eb462484a404f576.pdf
10. Takele, Y., & Sira, Z. (2013). Analysis of factors influencing customers' intention to the adoption of e-banking service channels in Bahir Dar City: An integration of TAM, TPB, and PR. *European Scientific Journal, 9*(13), 402-417. doi:10.19044/esj.2013.v9n13p%p
11. Alkailani, M. (2016). Factors affecting the adoption of internet banking in Jordan: An extended TAM Model. *Journal of Marketing Development and Competitiveness, 10*(1), 39-52. Retrieved from http://www.na-businesspress.com/JMDC/AlKailaniM_Web10_1_.pdf
12. Shora, R. Y. & Kartono. (2020). Effectiveness of process-oriented guided inquiry learning with peer feedback on achieving students' mathematical reasoning capabilities. *International Journal of Instruction, 13*(3).
13. Hair, J. F., Page, M., & Brunsveld, N. (2019). Essentials of business research methods. Routledge.
14. Subedi, B. P. (2016). Using Likert type data in social science research: Confusion, issues, and challenges. *International Journal of Contemporary Applied Sciences,3*(2), 36-49.
15. Sarstedt, M., & Mooi, E. (2014). A concise guide to market research. Springer.
16. Safeena, R., Date, H., & Kammani, A. (2011). Internet Banking Adoption in an Emerging Economy: Indian Consumer's Perspective. *Int. Arab. J. e Technol., 2*, 56-64.
17. Tan, M., & Teo, T. (2000). Factors Influencing the Adoption of Internet Banking. *Journal of the Association for Information Systems, 1*(5), 1-42.
18. Akhlaq, M., & Shah, A. (2011). Internet Banking in Pakistan: Finding Complexities. *The Journal of Internet Banking and Commerce, 16*, 1-14.
19. Davis, F. (1986). A technology acceptance model for empirically testing new end-user information systems: Theory and results. Doctoral Dissertation, Sloan School of Management, Massachusetts Institute of Technology.
20. Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 319-340.
21. Subedi, B. P. (2016). Using Likert type data in social science research: Confusion, issues, and challenges. *International Journal of Contemporary Applied Sciences, 3*(2), 36-49.
22. Sarstedt, M., & Mooi, E. (2014). A concise guide to market research. Springer.

Appendix

Coefficients[a]

Model		Collinearity Statistics	
		Tolerance	VIF
1	PM	.505	1.980
	PUE	.551	1.815
	TPC	.885	1.130

a. Dependent Variable: SR, EU