Cyber Security Awareness among Digital Banking users in Malaysia

Mohd Hafiz Bakar[1*], Siti Norbaya Yahaya[2] & Nurul Nadia Ramli[3]

[1]Faculty of Business & Management, Universiti Teknologi MARA, Cawangan Melaka Kampus Alor Gajah, KM 26, Jalan Lendu, 78000 Melaka, Malaysia.

[2,3] Faculty of Technology Management and Technopreneurship, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

DOI: https://dx.doi.org/10.47772/IJRISS.2025.910000038

Received: 29 September 2025; Accepted: 07 October 2025; Published: 03 November 2025

ABSTRACT

The purpose of this study is to assess the level of cyber security awareness among Malaysians who utilize the digital banking services. In addition to secondary data (such as journal articles, books, websites, and news articles), a survey questionnaire serves as the major data source for this study. A quantitative technique is also employed to collect information from a sample of 399 Malaysian digital banking users. Among Malaysians who utilize digital banking, knowledge of cyberattacks, laws and regulations, and multi-factor authentication are all significantly correlated with cybersecurity awareness. This study looks at the knowledge that users of digital banking should have about cyber security, including knowledge of laws and guidelines, multi-factor authentication (MFA), and cyber-attacks.

Keywords: Cyber security, digital banking, cyber-attacks, multi-factor authentication

INTRODUCTION

Due to the growing digitalization of financial services, improving cyber security in digital banking has become essential in Malaysia. The risk of cyber-attacks has considerably increased as more Malaysians conduct financial transactions online or via mobile devices. The Central Bank of Malaysia (Bank Negara Malaysia) has made many measures to enhance cyber security in digital banking in order to address these threats. Guidelines for the Management of Cyber Risk are one of these projects. Bank Negara Malaysia released guidelines in 2013 to help financial institutions manage cyber risk. These recommendations emphasized the significance of putting appropriate security measures in place to identify and stop cyber-attacks. In 2018, Bank Negara Malaysia published a cyber security framework that mandates the implementation of comprehensive cyber security programs for financial institutions that address governance, risk management, and incident management. In 2019, Bank Negara Malaysia introduced this platform. Financial institutions may proactively identify and mitigate cyber threats thanks to this platform's real-time cyber threat intelligence.

Customers can feel more secure while making financial transactions online or using mobile devices because financial institutions are now better able to detect and prevent cyber- attacks.

Payment with debit card online Customers may use the internet and cell phones to access all sorts of bank services 24 hours a day, and they can simply transact and manage their accounts from anywhere in the world (Dr. S. Nagaraju, 2022). However, despite how simple and straightforward banking-related activities are, cyber security is one area that needs to be given priority. The information and data banking is quite private. It is susceptible to online threats including hacking, data theft, and others. As the number of people using digital banking rises and its use spreads, this is becoming more and more the case. Cyber security threats are a growing concern for the digital banking industry in Malaysia. According to a survey conducted by the Malaysian computer Emergency Response Team (MyCERT), there was a 102% increase in reported cyber incidents in the banking and financial sector in Malaysia in 2019 compared to the previous year (Kuan, 2020). These incidents range from ransomware attacks to phishing scams and can result in financial losses for individuals and businesses alike. The Malaysian government has acknowledged the importance of cyber security in the financial sector and

has implemented various measures to improve it. The Central Bank of Malaysia has established guidelines for financial institutions to ensure the security of their systems and customer data (Bank Negara Malaysia, 2018). Additionally, the Malaysian Computer Emergency Response Team (MyCERT) provides cyber security training and support to financial institutions.

Despite these efforts, more needs to be done to improve cyber security in digital banking in Malaysia. To detect and mitigate cyber-attacks, financial institutions must invest in modern technologies such as artificial intelligence and machine learning. They should also regularly update their security systems and conduct regular vulnerability assessments to ensure that they are protected against the latest threats. Furthermore, customers need to be educated on the importance of cyber security and how to protect themselves from cyber threats. Financial institutions should provide regular security awareness training to their customers and ensure that their digital banking platforms are user-friendly and secure.

In conclusion, cyber security is a critical issue that needs to be addressed in the digital banking sector in Malaysia. Financial institutions and the government must work together to implement proactive measures to aware about cyber security and protect customers' data from cyber threats. Also, users of digital banking must aware how important cyber security in digital banking. The aim of this research is to study the cyber security awareness among digital banking users in Malaysia. The research objectives developed in this study based on the problem statement above as follow:

To identify cyber security awareness in digital banking.

To measure the level of cyber security awareness to digital banking.

To examine the most critical of cyber security awareness in digital banking.

Conceptual framework, theoretical review, and hypothesis development

Awareness of Cyber Attack

According to Amar Johri and Shailendra Kumar (2023), traditional banks become more exposed to cyber-attacks after cooperating with Fintech companies. In this era, nothing can save us from cyber-attacks, especially financially. Nida Tariq (2018) also said cybercrimes as a technological disease are spreading very speedily in the present era. Nothing is secure now and financial institutions are under great threat.

Awareness of Policies and Regulations

According to Juan Carlos Crisanto, et. Al (2017), Cyber-security regulations should require banks to develop effective control and response frameworks for cyber- risk. On the authority of Bank Negara Malaysia (BNM) (2020), the Bank endeavors to ensure the regulatory framework remains conducive for enablement of these innovations in a safe and sound manner that supports transformation of the financial ecosystem to meet future economic needs of the nation and promote sustainable and inclusive financial sector. According to David Smith (2020), cyber security regulations exist that encourage banks to share information regarding cyber threats among one another. The aim is to mitigate cyber-attacks and enhance overall cyber security in the banking industry.

Awareness of Multi-Factor Authentications

With the rise of digital banking and the increasing sophistication of cyberattacks, MFA has become an essential security measure for financial institutions to protect their customers' sensitive information and assets. Without MFA, customer accounts are vulnerable to hacking, identity theft, and other forms of fraud, which can lead to significant financial losses and reputational damage for both the institution and the individual. Therefore, MFA is an important step in digital banking to enhance the security of customer accounts and maintain trust in financial institutions. As stated by Amar Johri and et. al, (2022), users must realize that two-factor authentication is a measure used to defend client bank accounts againts online intrusions.

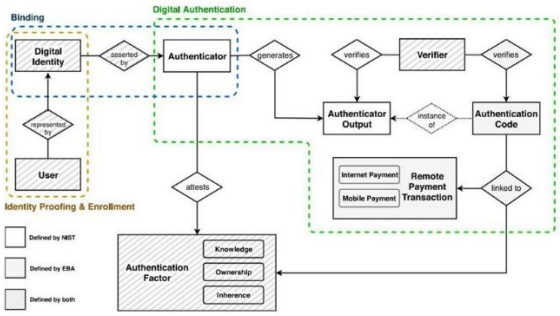

Fig.1 Theoretical framework developed by Federico Sinigagliaa, et. al (2020)

The conceptual framework proposed for this study aims to visually represent the various constructs and variables involved, and the connections between them. The independent variable includes three type of awareness: cyber-attack, policies and regulations, and multi-factor authentications. Through a diagram, the framework outlines the links between these independent variables and dependent variables under study.

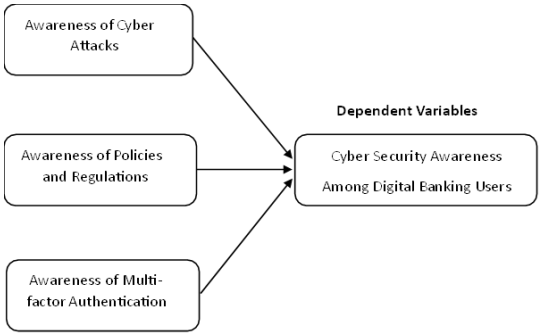

Fig.2 Conceptual Framework

RESEARCH METHODOLOGY

The choice of research technique is a critical decision in the research design process because it defines how relevant information for a study will be gathered; yet, the research design process comprises several connected considerations. It serves as a guide for the gathering, measuring, and interpretation of data. Because it gives the study direction and identifies what has to be done that may be valuable to the study, researchers believe that research design is crucial. This study's objective is cyber security awareness (independent variables) among digital banking users (dependent variables).

This investigation was carried out utilising quantitative methods. According to Oberiri Destiny Apuke (2017), quantitative research begins with the formulation of a problem, the development of a hypothesis or research question, the evaluation of related literature, and the quantitative analysis of data. The best way to gauge the link between the independent and dependent variables is through quantitative research. An independent variable (sometimes called an experimental or predictor variable) is a variable that is being manipulated in an experiment in order to observe the effect this has on a dependent variable (sometimes called an outcome variable). The dependent variable is simply that; a variable that is dependent on an independent variable(s). In order to answer the research question and to test research hypothesis, this study includes dependent variables consist of digital banking on users and three independent variables which are awareness of cyber-attacks, awareness of policies and regulations, and awareness of multi- factor authentication.

Data Collection

The research used both primary and secondary data. The original data were more reliable and provided a better degree of confidence in decision-making, with the trustworthy analysis having a direct link with the occurrences (Kassu Jilcha Sileyew, 2019). Primary data, according to Syed Muhammad Sajjad Kabir (2016), is knowledge obtained from personal experience. Primary data, which is more reliable, authentic, and impartial, has not yet

been disclosed. In contrast, secondary data is information acquired from a source that has already been published in some form or another. In any research, a review of literature is based on secondary data.

For the purpose of providing the questionnaire to respondents in this study, a self- administered survey approach is used. The questionnaire is divided into three pieces. Demographic data including gender, age, income, education and occupation, and etc. were expected to be gathered in Section A. Section B then asks users in Malaysia questions about cyber security awareness in digital banking using several Likert scale questions. In addition, section C includes additional questions about cyber security awareness are awareness of cyber-attacks, awareness of policies and regulations, and awareness of multi-factor authentication. The questions were designed to ascertain respondents' opinions on each component linked to cyber security awareness.

To clarify, probability sampling (or representative sampling) is most typically connected with survey research methodologies in which you must draw statistical inferences about a population from your sample in order to answer your research question(s) and accomplish your objectives. Non-probability sampling (or non-random sampling) offers a variety of sample selection procedures, the majority of which incorporate an element of subjective assessment.

The technique is random sampling because the researcher employs probability sampling. This method of choosing sample size assumes that each sample has an equal and independent chance of being chosen from the population under study. The survey's intended users are Malaysians who utilize digital banking. According to the researcher, Malaysia has 32.5 million people. Robert V. Krejcie and Daryle W. Morgan (1970) stated that the sample size is 384 when the population is greater than 1 000 000. 384 individuals are so chosen to complete surveys and serve as a source of data and evaluation.

Malaysia state is the primary focus of the investigation. The rationale for selecting this country is that Malaysia is quickly expanding its use of digital banking. According to Ong Ching Chuan (2019), the year 2020 would be an exciting year for Malaysian banking. Bank Negara Malaysia (BNM) has issued rules that allow technology companies and other non-financial entities to compete directly with traditional banks. Successful digital banks often identify a market gap with adequate size and growth and develop a business strategy that caters to the needs of that target group.

DATA ANALYSIS AND RESULTS

The purpose of pilot study is to test the feasibility of the questionnaire whether respondents can understand the questions. In this study, the researcher select 40 respondents which are 10% of total respondents. Cronbach's alpha is used to measure the consistency of data where the value not less than 0.7 represent that the questionnaire has consistent reliability.

Awareness of Cyber Security

Table 1: Reliability Statistics

Cronbach's Alpha	N of Items
.741	4

Awareness of Policies and Regulations

Table 2: Reliability Statistics

Cronbach's Alpha	N of Items
.773	5

Awareness of Multi-Factor Authentications

Table 3: Reliability Statistics

Cronbach's Alpha	N of Items
.787	5

Cyber Security Awareness

Table 4: Reliability Statistics

Cronbach's Alpha	N of Items
.702	4

Reliability Analysis

Table 5: Reliability Statistics

Cronbach's Alpha	N of Items
.877	18

Descriptive Analysis

Awareness of Cyber Attack

The response of 399 respondents on independent variable, awareness of cyber security that focusing on awareness can reduce cybercrime. The item CA1 states that users of digital banking believe focusing on awareness can reduce cybercrime. From the result, there are 66.9% respondents strongly agree on the statement, 30.3% of respondents agree on the statement and 2.5% expressed neutral. However, there are 0.3% of respondents disagree on the statement.

The item CA2 describe users aware about all kinds of threats. Based on the result obtained, there has 30.6% strongly agree on the statement and majority of respondents (41.9%) agree on the statement. There are 18.8% of respondents claims that they are neutral but 6.5% of respondents disagree and 2.3% strongly disagree on the statement.

Next, item CA3 explain that respondents should concerned about the possibility of cyber attacks affecting digital banking transaction. From the table, majority of respondents (58.1%) strongly agree to concerned about the possibility of cyber attacks affecting digital banking transactions and 30.3% agree on the statement followed by 11.5% of respondents are neutral on the statement. There has no respondents not concerned about the possibility of cyber attacks affecting digital banking transaction.

Besides, item CA4 states that respondents would like to reports suspicious email or activity related to digital banking transactions to bank. There are 44.9% of respondents strongly agree and 46.1% of respondents agree on the statement followed by 8% of respondents claim that they feel neutral on the statement. On the other side, there are 0.8% of respondents disagree and 0.3% strongly disagree on the statement.

Awareness of Policies and Regulations

The responses of 399 respondents on awareness of policies and regulations. Items PR1 states that users need to be aware of government regulations concerning digital banking. There are 51.6% respondents strongly agree

followed by 46.6% respondents agree with the statement. 1.5% respondents claims that they are neutral on the statement. However, only 0.3% of respondents disagree and no respondents strongly disagree with the statement.

The item PR2 describe respondents think current regulations in digital banking protect customers. There are 45.1% respondents strongly agree and 50.4% respondents agree on the statement. The table also shows that there are 3.5% respondents are neutral on the statement. On the other hand, there are 1% respondents disagree and no respondent strongly disagree.

Next, the item PR3 state that respondents should aware of the privacy policies of the digital banking institution we use. Based on the table, 45.9% respondents strongly agree on the statement and 44.6% respondents agree on the statement. However, there are respondents who have different opinions where 9.3% respondents are neutral while 0.3% respondents disagree with the statement and no one strongly disagree with the statement.

The fourth statement, PR4 states that respondents believe that digital banking institutions adequately protect personal data. There are 43.6% respondents strongly agree and 31.6% respondents agree on the statement. However, there are respondents who have different opinions where 22.1% are neutral while 1.8% respondents disagree with the statement and 1% respondents are strongly disagree with statement PR4.

Item PR5 declare that respondents believe that regulations are necessary in digital banking. The results show that 51.4% respondents are strongly agree that regulations are necessary in digital banking and 46.9% respondents agree with the statement. Nevertheless, 1.5% respondents are neutral while 0.3% respondents disagree with the statement and no one strongly disagree with the statement.

Awareness of Multi-factor Authentications (MFA)

The result of awareness of multi-factor authentications among users of digital banking. The item MF1 point out respondents believe MFA so effective preventing unauthorized access to transactions. There are 46.1% respondents strongly agree and 34.6% respondents agree with the statement. In addition, 18.8% respondents are neutral with the statement. However, there are 0.5% respondents disagree and no respondents strongly disagree with the statement.

Item MF2 highlight on whether respondents use the same password across multiple online accounts, including bank account will expose to cyber attacks. Most of the respondents (50.4%) strongly agree on the statement and 37.6% agree that use the same password across multiple online accounts, including bank account will expose to cyber attack. There are 7.3% respondents neutral with the statement. However, there are 2.5% respondents disagree on the statement and 2.3% respondents strongly disagree.

Item MF3 states that respondents enabled MFA for digital banking account. There are 37.1% respondents strongly agree that user need to enabled MFA for digital banking account and 51.9% respondents agree with item MF3. Furthermore, 9.5% respondents feel neutral on the statement. Conversely, there are 1% respondents disagree on the statement and 0.5% respondents strongly disagree with the statement.

Next, item T4 mention that respondents think that it is not difficult for me to set up and use MFA for digital banking transactions. 34.6% respondents strongly agree on the statement and 42.1% respondents agree on the statement. There are 21.6% respondents are neutral on the statement. 1% respondents disagree that MFA is not difficult to set up for digital banking while 0.8% respondents strongly disagree on the statement.

Lastly, item MF5 states that respondents should change MFA settings or update authentication methods frequently. There are 32.3% respondents strongly agree and 43.1% respondents agree on the statement. 21.1% respondents are neutral on the statement. However, 1.5% respondents are disagree that MFA settings or update my authentication methods frequently should to change and 2% respondents strongly disagree with the statement.

Awareness of Cyber Security

Descriptive statistics results of the dependent variable, awareness of cyber security. Item CS1 describe that respondents received any suspicious emails or messages asking for personal or banking information. There are 5.3% respondents strongly agree that they always received any suspicious emails or messages asking for personal or banking information and 6.3% respondents agree with the statement. Aside, there 19% respondents feel neutral with item CS1. However, 31.6% respondents disagree and 37.8% respondents strongly disagree on the statement.

Item CS2 point out that respondents frequently check account activity and statements for any unusual transactions or activity. There are 22.6% respondents who are strongly agree and strongly disagree on the statement. However, 8.3% respondents agree and 15.5% respondents feel neutral with item CS2. Majority of the respondents disagree on the statement, which is 31.1% respondents.

Item CS3 highlight that respondents have received any cyber security training or education from bank or other trusted sources to stay away and safe online. There are 10.3% respondents strongly agree with the statement and 8.8% respondents agree. In addition, 20.6% respondents are neutral on the statement. There are 27.6% respondents who disagree and 32.8% respondents strongly disagree that they received any cyber security training or education from bank or other trusted sources to stay away and safe online. Next, CS4 states that respondents will checked on a suspicious link or attachment in an email or message, or downloaded an app from an untrusted source. There are 2.3% respondents strongly agree and 2% respondents agree on the statement. However, 12.8% respondents feel neutral on the statement followed by 24.3% respondents disagree with the statement. Majority of respondents strongly disagree (58.6%) with the statement.

Respondent's Profile

Table 6: Gender

	Frequency	**Percent**	**Cumulative percent**
Female	226	56.6	56.6
Male	173	43.4	100
Total	399	100	

Table shows the frequency and percentage of respondents' demographic of gender. There are total 399 respondents and among the respondents, male respondents consist of 173 which is are 43.4**%** while female respondents consist of 226 which are 56.6% as shown in the figure.

Table 7: Age

	Frequency	**Percent**	**Cumulative percent**
18-23 years old	174	43.6	43.6
24-29 years old	88	22.1	65.7
30-35 years old	51	12.8	78.4
36-41 years old	42	10.5	89.0
42-47 years old	25	6.3	95.2
48-53 years old	7	1.8	97.0

54-59 years old	10	2.5	99.5
60 years old and above	2	0.5	100
Total	399	100	

Table shows the data of the range on the age of respondents. Among 399 respondents, there are 174 respondents (4.3%) in aged between 18 to 23 years old which is the highest age group among the respondents. The respondents who are aged between 24 to 29 years old consist of 88 respondents (22.1%). Besides, the range from 30 to 35 years old has 51 respondents (12.8%). There are 42 respondents who aged between 36 to 41 years old (10.5%). The respondents in range age 42 to 47 years old is 25 respondents (6.3%). However, respondents who are aged between 48 to 53 years old is 7 respondents only (1.8%). In range aged 54 to 59 years old, there has 10 respondents (2.5%). The rest are only 2 respondents (0.5%), which is who are aged 60 years old and above.

Table 8: Occupation

	Frequency	**Percent**	**Cumulative percent**
Employed	156	39.1	39.1
Retire	6	1.5	40.6
Student	193	48.4	89
Unemployed	42	10.5	99.5
Others	2	0.5	100
Total	399	100	

Table demonstrates occupation of respondents. Among the respondents, 156 employed (39.1%), while 2 respondents (0.5%) are others, the lowest group of occupation of respondents. There are total 6 respondents (1.5%) are retire while 193 39.1, 39% 0.5, -1% 1.5, 2% 48.4, 48% 10.5, 11% Occupation Employed Others Retire Student Unemployed50 respondents (48.4%) are students, which is the highest group of respondents' occupation. The rest is an unemployed, there 42 respondents (10.5%).

Descriptive Statistics

Table 9: Descriptive Statistics

Independent Variable	**N**	**Minimum**	**Maximum**	**Mean**	**Standard Deviation**
Awareness of Cyber Attacks	399	3.00	5.00	4.34	0.44
Awareness of Policies and Regulations	399	2.80	5.00	4.38	0.38
Awareness of Multi-factor Authentications	399	2.00	5.00	4.19	0.53

The descriptive statistics of each independent variable (awareness of cyber-attacks, awareness of policies and regulations, awareness of multi-factor authentications). Based on the table, all the independent variables have almost similar value of mean. Awareness of policies and regulations has the highest mean at 4.38 subsequently followed by awareness of cyber-attacks at 4.34 and awareness of multi-factor authentication has lowest mean at

4.19. From the table obtained, it can be clearly seen that majority of the respondents rated agree on the questionnaire that the independent variables aware among digital banking users.

In contrast, standard deviation specifies how the data spread from the mean. From the study, awareness of multi-factor authentications has the highest standard deviation at 0.53 followed by awareness of cyber-attacks at 0.44 while the lowest standard deviation is awareness of policies and regulations at 0.38. The standard deviation value indicate that the data are not deviate from the mean.

Pearson's Correlation Analysis

The relationship between awareness of cyber-attacks, awareness of policies and regulations, awareness of multi-factor authentications with awareness of cyber security among digital banking user through Pearson's Correlation Analysis. Pearson's Correlation Analysis measures the strength of linear relationship between the independent variables and dependent variable. Pearson's Correlation Coefficient value ranges from +1 to -1. The positive value represents positive correlation between the variables while negative value represents negative correlation between the variables. The zero value of coefficient indicate that there is no association between the variables. The value of Pearson's Correlation Coefficient is denoted by r.

The table indicates significant correlations ranging from 0.714 to 0.489. Among the three independent variables, knowledge of cyber-attack has the highest coefficient value of 0.714. The value reflects a significant positive relationship between knowledge of cyber assault and awareness of cyber security. The p-values for all variables are less than 0.01 at the significance level, and two asterisks at the two-tailed test indicate that there is a statistically significant link.

Next, awareness of policies and regulations has the second highest correlation coefficient value, r at 0.600. It indicates that has strong positive correlation with awareness of cyber security. Furthermore, the R-value of awareness of multi-factor authentications is 0.489 which is clearly shows strong positive relationship between awareness of multi-factor authentications and awareness of cyber security.

Therefore, there is significant relationship between independent variables which consist of awareness of cyber-attacks, awareness of policies and regulations, awareness of multi-factor authentications and dependent variable which is awareness of cyber security. Thus, the researcher conducts further analysis on the independent variables with multiple linear regression analysis.

Multiple Linear Regression

The model summary from usage of multiple linear regression analysis where the results show the value of R is 0.856 which indicate all the three independent variables are highly correlated. The coefficient of determination, R square is at 0.731 indicate that 73.1% of total variation in awareness of cyber security among digital banking user can be explained by the independent variables (awareness of cyber-attack, awareness of policies and regulations, and awareness of multi-factor authentications). The value of R Square is lower than 0.5 which is considered a good value because there is high variance towards awareness of cyber security as the independent variables in regression model. However, there is 26.9% remain unexplained in the variation. Hence, there are other significant reasons of cyber security awareness among digital banking user not included for this research.

The significance value, p-value is 0.000 which is less than the alpha value, 0.05 is statistically significant. The F-value is 358.143 is significant because when the F-value is higher, alternative hypotheses are well fit in the model and accepted. Therefore, the significance of overall model is $F(3,395) = 3858.143$, $p < 0.05$. It shows that overall multiple regression model is significant at 5% level of significant. Each independent variable in the research has contribution in awareness of cyber security among digital banking user. Awareness of cyber attack is the strongest predictor variable where $\beta = 0.442$, $t(399) = 19.533$, $p < 0.05$. The unstandardized beta, β also has the highest value compared to other independent variables. It can be clearly seen that awareness of cyber attack has the highest influence of positive relationship with cyber security awareness among digital banking user.

Next, awareness of policies and regulations has subsequent stronger predictor where $\beta = 0.299$, $t(399) = 11.157$, $p = < 0.05$. The unstandardized beta, β of awareness of policies and regulations is the second highest positive value among the variables. From the result, awareness of policies and regulations is the second highest awareness in cyber security awareness among digital banking users. Then, awareness of multi-factor authentications is the lower predictor variable where $\beta = 0.202$, $t(399) = 11.133$. The unstandardized beta, β of awareness of multi-factor authentications is the lowest positive among the variables. From the result, awareness of multi-factor authentications has lowest positive value of all independent variables and is the third awareness in cyber security awareness among digital banking users. Based on the result, each of the independent variable has different level of contribution towards dependent variable and provide significant prediction towards cyber security awareness among digital banking users. The relationship between dependent variable and independent variables can be determined by the multiple regression equation.

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_i X_i$$

Y : Dependent variable

β_0 : Intercept

β_i : Slope for X_i

X : Independent variable

Figure 3: Equation of Multiple Regression Analysis

CONCLUSION AND RECOMMENDATION

In previous chapter, the study had achieved the research objectives which are to identify the cyber security awareness in digital banking, to measure the level of cyber security awareness of digital banking, and to examine the most critical cyber security awareness in digital banking. The finding of this research is to have deeper understanding about critical cyber security awareness in digital banking as there is increase in cyber-attack victims among digital banking user in Malaysia. From the research, there are only three types of awareness are being studied but the researcher believed that there are still other type of awareness that can influence user of digital banking to aware on issues of cyber security.

The study had achieved the research objectives through literature review, Pearson's Correlation Coefficient's analysis and Multiple Linear Regression analysis and test the hypothesis on the relationships on independent variables (awareness of cyber-attack, awareness of policies and regulations, and awareness of multi-factor authentications) aware about cyber security. In summary, awareness of cyber-attack, policies and regulations, and multi-factor authentications among digital banking user is the most significant awareness for cyber security awareness among digital banking users. The critical cyber security awareness in digital banking is crucial to have in depth understanding on issues of cyber security among digital banking users to be aware about cyber security. For user, they can increase awareness of their security in digital banking to avoid cybercrime in digital banking. As the cybercrime rises, Bank Negara Malaysia (BNM) has made many measures to enhance cyber security in digital banking to address these threats. Also, Bank Negara Malaysia (BNM) periodically holds awareness programs to inform the public and financial institutions about the value of cyber security and how to defend themselves from cyber-attacks.

For future research, this study proposed only consists of three independent variables (awareness of cyber-attacks, awareness of policies and regulations, and awareness of multi-factor authentications). However, the researcher believed that there is other cyber security awareness that can avoid from cybercrime in digital banking. The future researchers may do qualitative research on digital banking studies to gain deeper insights on digital banking user. Future researchers can increase the sample size of study to have generalization on digital banking user. Based on the study of Amar Johri and Shailendra Kumar (2023), awareness of phishing attacks is one of

the cyber security awareness among digital banking users. Therefore, it will be an awareness of cyber security among digital banking users. Amar Johri and Shailendra Kumar (2023) also states that awareness of hacking which includes cyber security awareness among digital banking. There, awareness of hacking can be used in future research on digital banking studies.

REFERENCES

1. Alt, R., Beck, R., & Smits, M. T. (2018). Fintech and the transformation of the financial industry. Electronic Markets, 28(3), 235–243. https://doi.org/10.1007/s12525-018-0310-9
2. Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022). Cyber security threats on Digital Banking. 2022 1st International Conference on AI in Cybersecurity (ICAIC). https://doi.org/10.1109/icaic53980.2022.9896966
3. Ammirato, S., Sofo, F., Felicetti, A. M., & Raso, C. (2019). A methodology to support the adoption of IOT innovation and its application to the Italian Bank branch security context. European Journal of Innovation Management, 22(1), 146–174. https://doi.org/10.1108/ejim-03-2018-0058
4. Balbaa, M. E., Eshov, M. P., & Ismailova, N. (2022). The impacts of Russian ukrainian war on the global economy in the frame of digital banking networks and cyber attacks. Proceedings of the 6th International Conference on Future Networks & Distributed Systems. https://doi.org/10.1145/3584202.3584223
5. Bapat, D. (2021). Exploring the relationship between lifestyle, digital financial element and Digital Financial Services experience. International Journal of Bank Marketing, 40(2), 297–320. https://doi.org/10.1108/ijbm-12-2020-0575
6. Barroso, M., & Laborda, J. (2022). Digital transformation and the emergence of the Fintech sector: Systematic Literature Review. Digital Business, 2(2), 100028. https://doi.org/10.1016/j.digbus.2022.100028
7. Belke, A., & Beretta, E. (2020). From cash to central bank digital currencies and cryptocurrencies: A balancing act between modernity and monetary stability. Journal of Economic Studies, 47(4), 911–938. https://doi.org/10.1108/jes-07-2019-0311
8. Buja, A. G. (2021). Cyber Security Featuresfor National E-Learning policy. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(5), 1729–1735. https://doi.org/10.17762/turcomat.v12i5.2169
9. Chandra sekhar, & Kumar, M. (2023). An overview of cyber security in digital banking sector. East Asian Journal of Multidisciplinary Research, 2(1), 43–52. https://doi.org/10.55927/eajmr.v2i1.1671
10. Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., & Cai, Z. (2022). A survey on blockchain systems: Attacks, defenses, and Privacy Preservation. High-Confidence Computing, 2(2), 100048. https://doi.org/10.1016/j.hcc.2021.100048
11. Financial sector blueprint 2022-2026 – Bank Negara Malaysia. (n.d.-i). https://www.bnm.gov.my/publications/fsb3
12. Formosa, P., Wilson, M., & Richards, D. (2021). A Principlist Framework for cybersecurity ethics. Computers & amp; Security, 109 102382. https://doi.org/10.1016/j.cose.2021.102382
13. Ghelani, D., Hua, T. K., & Koduru, S. K. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. https://doi.org/10.22541/au.166385206.63311335/v1
14. Gogolin, F., Lim, I., & Vallascas, F. (2021). Cyberattacks on small banks and the impact on local banking markets. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3823296
15. Gola, C., & Roselli, A. (2009). The UK Banking System and Its Regulatory and Supervisory Framework. https://doi.org/10.1057/9780230235779
16. Gulyás, O., & Kiss, G. (2023). Impact of cyber-attacks on the Financial Institutions. Procedia Computer Science, 219, 84–90. https://doi.org/10.1016/j.procs.2023.01.267
17. Guma, A. (n.d.). Development of a Secure Multi-Factor Authentication Algorithm for Mobile Money Applications. https://doi.org/10.58694/1782
18. Jebarajakirthy, C., & Shankar, A. (2021). Impact of online convenience on mobile banking adoption intention: A moderated mediation approach. Journal of Retailing and Consumer Services, 58, 102323. https://doi.org/10.1016/j.jretconser.2020.102323

19. Johri, A., & Kumar, S. (2023a). Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of Banking Digital Transformation. Human Behavior and Emerging Technologies, 2023, 1–10. https://doi.org/10.1155/2023/2103442
20. Kasri, R. A., Indrastomo, B. S., Hendranastiti, N. D., & Prasetyo, M. B. (2022). Digital payment and banking stability in emerging economy with dual banking system. Heliyon, 8(11). https://doi.org/10.1016/j.heliyon.2022.e11198
21. Kulu, E., Opoku, A., Gbolonyo, E., & Tayi Kodwo, M. A. (2022). Mobile money transactions and Banking Sector Performance in Ghana. Heliyon, 8(10). https://doi.org/10.1016/j.heliyon.2022.e10761
22. Loaba, S. (2022). The impact of mobile banking services on saving behavior in West Africa.Global Finance Journal, 53, 100620. https://doi.org/10.1016/j.gfj.2021.100620
23. Ly, B., & Ly, R. (2022). Internet banking adoption under technology acceptance model— evidence from Cambodian users. Computers in Human Behavior Reports, 7, 100224. https://doi.org/10.1016/j.chbr.2022.100224
24. Mai, P. T., & Tick, A. (2021). Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. Acta Polytechnica Hungarica, 18(8), 67–89. https://doi.org/10.12700/aph.18.8.2021.8.4
25. Mawudor, B. G., Kim, M.-H., & Park, M.-G. (2015). Continuous monitoring methods as a mechanism for detection and mitigation of growing threats in banking security system. 2015 4th International Conference on Interactive Digital Media (ICIDM). https://doi.org/10.1109/idm.2015.7516317
26. Mbama, C. I., & Ezepue, P. O. (2018). Digital Banking, customer experience and Bank Financial Performance. International Journal of Bank Marketing, 36(2), 230–255. https://doi.org/10.1108/ijbm-11-2016-0181
27. Md Haris Uddin Sharif, & Mehmood Ali Mohammed. (2022). A literature review of financial losses statistics for Cyber Security and future trend. World Journal of Advanced Research and Reviews, 15(1), 138–156. https://doi.org/10.30574/wjarr.2022.15.1.0573
28. Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from Seven nations. Computers & Security, 120, 102820. https://doi.org/10.1016/j.cose.2022.102820
29. Murthy, N., & Gopalkrishnan, S. (2022). Does openness increase vulnerability to digital frauds? observing social media digital footprints to analyse risk and legal factors for Banks International Journal of Law and Management, 64(4), 368–387. https://doi.org/10.1108/ijlma-04-2022-0081
30. Nie, J. (2008). Mobile Banking Information Security and Protection Methods. 2008 International Conference on Computer Science and Software Engineering. https://doi.org/10.1109/csse.2008.1422
31. Nurse, J. R. C. (2021, February 28). Cybersecurity awareness. arXiv.org. https://arxiv.org/abs/2103.00474
32. Othman, R., Aris, N. A., Mardziyah, A., Zainan, N., & Amin, N. M. (2015). Fraud detection and prevention methods in the Malaysian Public Sector: Accountants' and internal auditors' perceptions. Procedia Economics and Finance, 28, 59–67. https://doi.org/10.1016/s2212-5671(15)01082-5
33. Palmié, M., Wincent, J., Parida, V., & Caglar, U. (2020). The evolution of the Financial Technology Ecosystem: An introduction and agenda for future research on disruptive innovations in ecosystems. Technological Forecasting and Social Change, 151, 119779. https://doi.org/10.1016/j.techfore.2019.119779
34. Patel, R., Migliavacca, M., & Oriani, M. E. (2022). Blockchain in banking and finance: A bibliometric review. Research in International Business and Finance, 62, 101718. https://doi.org/10.1016/j.ribaf.2022.101718
35. Prakash, R., Anoop, V. S., & Asharaf, S. (2022). Blockchain technology for cybersecurity: A text mining literature analysis. International Journal of Information Management Data Insights, 2(2), 100112. https://doi.org/10.1016/j.jjimei.2022.100112
36. Puente, F., Sandoval, J. D., Hernandez, P., & Molina, C. J. (2005). Improving online banking security with hardware devices. Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology. https://doi.org/10.1109/ccst.2005.1594874
37. Rastogi, S., Panse, C., Sharma, A., & Bhimavarapu, V. M. (2021). Unified payment interface (UPI): A Digital Innovation and its impact on financial inclusion and Economic Development. Universal Journal of Accounting and Finance, 9(3), 518–530. https://doi.org/10.13189/ujaf.2021.090326

38. Rodrigues, A. R., Ferreira, F. A. F., Teixeira, F. J. C. S. N., & Zopounidis, C. (2022). Artificial Intelligence, Digital Transformation and cybersecurity in the banking sector: A multi- stakeholder cognition-driven framework. Research in International Business and Finance, 60, 101616. https://doi.org/10.1016/j.ribaf.2022.101616
39. Sanusi, Z. M., Rameli, M. N., & Isa, Y. M. (2015). Fraud schemes in the banking institutions: Prevention measures to avoid severe financial loss. Procedia Economics and Finance, 28, 107–113. https://doi.org/10.1016/s2212-5671(15)01088-6
40. Saripan, H., & Hamin, Z. (2011). The application of the digital signature law in securing internet banking: Some preliminary evidence from Malaysia. Procedia Computer Science, 3, 248–253. https://doi.org/10.1016/j.procs.2010.12.042
41. Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking Information Resource Cybersecurity System Modeling. Journal of Open Innovation: Technology, Market, and Complexity, 8(2), 80. https://doi.org/10.3390/joitmc8020080
42. Sileyew, K. J. (2019, August 7). Research design and methodology. IntechOpen. https://www.intechopen.com/chapters/68505
43. Sinigaglia, F., Carbone, R., Costa, G., & Zannone, N. (2020). A survey on multi-factor authentication for online banking in the wild. Computers & Security, 95, 101745. https://doi.org/10.1016/j.cose.2020.101745
44. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039
45. TN, N., & Shailendra Kulkarni, M. (2022). Zero click attacks – a new cyber threat for the E- banking sector. Journal of Financial Crime. https://doi.org/10.1108/jfc-06-2022-0140
46. Vinod Ramchandra, M., Kumar, K., Sarkar, A., Kr. Mukherjee, S., & Agarwal, K. (2022). Assessment of the impact of blockchain technology in the banking industry. Materials Today: Proceedings, 56, 2221–2226. https://doi.org/10.1016/j.matpr.2021.11.554
47. Wahid, S. D., Buja, A. G., Jono, M. N., & Aziz, A. A. (2021). Assessing the influential factors of cybersecurity awareness in Malaysia during the pandemic outbreak: A structural equation modeling. International Journal of Advanced Technology and Engineering Exploration, 8(74), 73–81. https://doi.org/10.19101/ijatee.2020.s1762116
48. Widyadhana, A. N., Handayani, P. W., & Larasati, P. D. (2022). Influence of technological, social, and individual factors on security and privacy take-up of Digital Banking. 2022 International Conference on Information Management and Technology (ICIMTech). https://doi.org/10.1109/icimtech55957.2022.9915231
49. Williamson, J., & Curran, K. (2023, April 28). The role of multi-factor authentication for Modern Day Security. Semiconductor Science and Information Devices. https://journals.bilpubgroup.com/index.php/ssid/article/view/3152
50. Wodo, W., Blaskiewicz, P., Stygar, D., & Kuzma, N. (2021). Evaluating the security of electronic and mobile banking. Computer Fraud & Security, 2021(10), 8–14. https://doi.org/10.1016/s1361-3723(21)00107-x
51. Yildirim, N., & Varol, A. (2019). A research on security vulnerabilities in online and Mobile Banking Systems. 2019 7th International Symposium on Digital Forensics and Security (ISDFS). https://doi.org/10.1109/isdfs.2019.8757495
52. Zahiroh, M. Y. (2020). Cybersecurity awareness and digital skills on readiness for change in digital banking. Li Falah: Jurnal Studi Ekonomi Dan Bisnis Islam, 5(2), 53. https://doi.org/10.31332/lifalah.v5i2.2271