Publikasi oleh: Yayasan Literasi Emas Nusantara
E-ISSN: 9999-9999 | P-ISSN: 9999-9999
Volume 0X Issue 0X, MM 202X
DOI : doi.org/reksy.v1i1.1

JURNAL RISET EKONOMI DAN KEUANGAN SYARIAH | REKSY

THE IMPACT OF CYBER CRIME ON THE INTEREST OF CUSTOMERS USING IT MOBILE BANKING BANK SYARIAH INDONESIA (BSI)

Tika Fajri Yanti[1], Wahyi Busyro[2], Putri Jamilah[3]
[1]Perbankan Syariah S1, Fakultas Studi Islam, Universitas Muhammadiyah Riau, tikafajriyanti1@gmail.com
[2]Perbankan Syariah S1, Fakultas Studi Islam, Universitas Muhammadiyah Riau, wahyi.busyro@umri.ac.id
[3]Perbankan Syariah S1, Fakultas Studi Islam, Universitas Muhammadiyah Riau, putrijamilah@umri.ac.id

Article Info:

Article history:

Received Date: 27/08/2024
Accepted Date: 19/09/2024
Published Date: 19/09/2024

Keywords:

Cybercrime
Customer Interest

ABSTRACT

Sharia banking is a banking system based on Islamic principles or Islamic law. Sharia banks operate based on the contents of the Qur'an and hadith. As a financial institution that operates based on sharia principles, sharia banks have also adopted digital banking services to provide ease and quick access for their customers. In creating banking technology such as mobile banking, it is important for banks to prioritize customers' privacy, specifically regarding the safety of customers' data. In some cases, hacker attacks can cause disruption to digital services in banks and Sharia banks are no exception to these attacks. The purpose of this study is to discover the effect of cybercrime on customers' interest using Bank Syariah Indonesia's mobile banking on the people of Pekanbaru city. Using quantitative research methods, the population in this study is the people of Pekanbaru city who use mobile banking of Bank Syariah Indonesia. The result of this study shows that cybercrime has a significant and positive effect on customer interest using mobile banking Bank Syariah Indonesia, which is indicated by a coefficient determination test (R2). Analysis shows that cybercrime has an effect of 49.0% on customer interest using mobile banking services at Bank Syariah Indonesia.

Corresponding Author:

Wahyi Busyro
Universitas Muhammadiyah Riau
wahyi.busyro@umri.ac.id

INTRODUCTION

Sharia banking is a banking system based on Islamic principles. Sharia banks carry out their operations based on the contents of the Qur'an and hadist (Busyro et al., 2020). In the growing digital era, many banks have adopted digital banking services to provide easy access and transactions to their customers. However, in some cases, hacker attacks can cause disruption to digital services in banks. Sharia banks are also vulnerable to cyber attacks by hackers that can disrupt their digital services. These disorders can include theft of customer information, disruption to the banking system or theft of unauthorized funds. Hacker attacks on sharia banks not only cause inconvenience to customers but also cause financial losses to banks (Ma'rifa, 2023).

Cybercrime is an act of crime that uses computer technology and internet networks to perform acts such as hacking, stealing, deceiving, spreading viruses and other digital criminal behaviors. Based on information obtained from comparitech.com , in 2021 there were 153 million new types of malware, of which 93.6% had the ability to change the original code, making it difficult to detect. In addition, more than 50% of computers that have been hit by hacking are likely to be hit again in the same year. Along with the development of computer and internet technology, there is also a way for criminals to steal corporate and individual data. There are several types of cybercrime including

Publikasi oleh: Yayasan Literasi Emas Nusantara
E-ISSN: 9999-9999 | P-ISSN: 9999-9999
Volume 0X Issue 0X, MM 202X
DOI : doi.org/reksy.v1i1.1

phishing, ransomware, carding, cracking, otp fraud, cyberbullying, content crime, and cyberbullying. (Chusna, 2023).

According to Danur (2017), the increase in cyber cases is inseparable from the rapid progress of information technology. Indonesia is considered a country. This is related to the increase in internet users in line with the increased risk of information technology security attacks and the increase in cyberattacks in Indonesia. Cybercrime cases that occurred in Indonesia attacked various sectors, both government and private agencies, including the financial services sector, sourced from information from the State Cyber and Password Agency (BSSN), the financial sector ranked third after the government administration and energy scheme, as the sector that experienced the most internet anomalies. The internet anomalies that occurred, the majority of which came from ransomware attacks based on monitoring data in 2023, in which of the 160 million malware anomalies, 966,533 indicated ransomware. The E-government academy foundation has published a national cyber security index (NCSI) in 2023, where Indonesia's cyber security index chord is 63.64 on a scale of 100 or an increase of 24.6 points compared to the score in 2022 which was only 38.96. The score ranked Indonesia 49th out of 176 countries in 2023, a significant increase compared to 2022 which only ranked 83rd out of 160 countries. (OJK, 2022).

Act No. 27th of 2022 regarding personal data protection doesn't seem to be able to prevent cyber attacks and personal data leakage. This is evidenced by the proliferation of cyber attacks on various industrial sectors, both private companies and the government. Data from the Dani Sandi Negara Cyber Agency (BSSN) shows that in 2022, Indonesia experienced about 370 million cyber attacks. This data has increased quite dramatically from the previous year's 266 million cases (Prasetyo, 2023).

Table 1. Number of Cyber Attacks in Indonesia · Global Voices 2019-2022

Year	Number of Cyber Attacks
2019	290.381.283
2020	316.167.753
2021	266.741.784
2022	370.022.283

Source: Cyber and State Password Agency (BSSN)

The table above clearly illustrates the increase in cybercrime every year, as recorded by the State Cyber and Password Agency (BSSN), Indonesia received 370.02 million cyberattacks in 2022 and the number increased from the previous year which was 266.74 million attacks in Indonesia.

In May 2023, Bank Syariah Indonesia (BSI) became a victim of the Ransomware Lockbit 3.0 attack. This attack resulted in banking activities, especially the Bank Syariah Indonesia (BSI) application, being paralyzed for several days. In addition, the hacker group also claimed to leak 1.5 Terabytes (TB) of customer databases as well as employees of Bank Syariah Indonesia (BSI). The leaked data included names, full addresses, card numbers, phone numbers, PINs, and other document information. Although Bank Syariah Indonesia (BSI) services are now able to operate normally, this incident is certainly very detrimental to customers (Prasetyo, 2023).

Lockbit 3.0 hackers also provoke customers to no longer use Bank Syariah Indonesia (BSI) because the bank is unable to protect their personal information and savings. The public believes that Bank Syariah Indonesia (BSI) is unable to protect customers' personal data. In addition, this also indicates that cyber security in the banking sector is still weak. The growing number of hacking cases in the banking sector shows that the bank's cybersecurity system still has many loopholes. If this continues to be allowed, the community will certainly not trust financial institutions anymore (Prasetyo, 2023).

Bank Syariah Indonesia (BSI) customers in the city of Pekanbaru admitted that they were worried about notification of customer data suspected of being hacked by hackers. "As a customer, I am certainly worried about our data and transactions," said Didik, one of the customers of Bank Syariah Indonesia (BSI) in the city of Pekanbaru. He admitted that he was still afraid to make a transaction and even delayed to make a transaction (Susanti Unik, 2023)

A customer of Bank Syariah Indonesia (BSI) admitted that the money was lost amounting to IDR 378,251,749 which was uploaded through the twitter animation line. The customer has made a report of loss and complaints to Bank Syariah Indonesia (BSI) solo branch, the post was uploaded amid the shock of Bank Syariah Indonesia (BSI) service interrupted by a ransomware lockbit attack claiming to have stolen 1.5 Terabytes (TB) of customer data. However, the RCEO of Bank Syariah Indonesia (BSI) in the Semarang area, Ficko Hardowiseto, served as the complaint that the customer's loss of money was not due to the service interruption of Bank Syariah Indonesia (BSI)

Publikasi oleh: Yayasan Literasi Emas Nusantara
E-ISSN: 9999-9999 | P-ISSN: 9999-9999
Volume 0X Issue 0X, MM 202X
DOI : doi.org/reksy.v1i1.1

or the theft of data as claimed by lockbit. With this complaint, PT Bank Syariah Indonesia (BSI) said that the customer had a phishing attack in April 2023 and was not related to the systematic constraints that occurred at Bank Syariah Indonesia (BSI) (Hakim, 2023).

Of these cases, trust in cybersecurity is an influencing factor for customers' choice of mobile banking services influenced by security perception. According to Smith (2021), 60% of customers indicated that they would reconsider the use of mobile banking if they felt security measures were inadequate. This will show that cybercrime can negatively affect customers' interest in utilizing digital banking services.

As mobile device adoption and technological advances increase, mobile banking is expanding. Mobile banking offers customers flexibility and convenience, allowing them to carry out various banking activities at any time and from any location. However, in addition to the benefits provided by mobile banking, there is a growing concern about the impact of cybercrime behavior that targets customers' interests in utilizing this service can greatly affect customers' trust and confidence in mobile banking. A major consequence of this criminal behavior is the eroding of trust and assurance regarding system security, which significantly affects customers' willingness to use mobile banking services. Customers may be hesitant to use mobile banking if they consider it vulnerable to cyber attacks and violations (Aguayo & Ślusarczyk, 2020).

RESEARCH METHOD

In this study, researchers used quantitative research methods. This type of research focuses on the analysis of numerical data (numbers) processed through statistical techniques. Essentially, quantitative approaches are applied in inference research, particularly in hypothesis testing, and draw conclusions based on the probability of rejecting the zero hypothesis. Through quantitative methods, researchers can identify the significance of differences between groups or the importance of relationships between the variables studied. Overall, quantitative research usually involves large sample sizes (Azwar, 2015).

Characteristics and number of termin popularity in the sample. When dealing with a large population, researchers may not be able to study every speck due to constraints such as time, power, and funding. In such cases, researchers can utilize samples taken from the population. The insights gained from the sample allow for generalized conclusions across the population. Therefore, the samples collected must truly represent the residents (Sugiyono, 2021).

This study used a nonprobability sampling method using the Purposive sampling technique, namely the determination of samples with certain characteristics. Which means that not everyone can be sampled in this study. The sample criteria in this study are people in Pekanbaru city who use Indonesian sharia bank mobile banking. Since researchers did not know the number of populations of the study, Cochran's formula was used to determine the sample size of the study. From this formula, there are 100 respondents in this study: (Sugiyono, 2022).

The method of data collection in research activities aims to reveal the facts about the variables studied. The goal of knowing must be achieved by using efficient and accurate methods or methods. Therefore, the researchers used the following data collection methods in this study:

The questionnaire serves as a method of collecting data by providing respondents with a series of written questions or statements to respond to. This involves gathering information through various questions presented to participants in the questionnaire format (Sugiyono, 2017).

Table 2. Skor scale Likert

Alternative Answers	Score For Statement
Totally Agree (SS)	5
Agreed (S)	4
Neutral (N)	3
Disagree (TS)	2
Strongly Disagree (STS)	1

Source: Researcher's Process

Data analysis as described by Sugiyono (2018) is a step in the data processing journey conducted by researchers after the required data has been collected. Typically, statistical methods are used in data analysis techniques during research. Statistics consist of a set of tests that allow researchers to derive logical conclusions from processed data.

Publikasi oleh: Yayasan Literasi Emas Nusantara
E-ISSN: 9999-9999 | P-ISSN: 9999-9999
Volume 0X Issue 0X, MM 202X
DOI : doi.org/reksy.v1i1.1

Data analysis techniques in this study used SPSS version 25.

RESULTS AND FINDINGS

The purpose of this study is to find out how cybercrime affects customers' interest in using mobile banking offered by sharia banks in Indonesia. The subjects in this study consisted of residents of Pekanbaru city who used Bank Syariah Indonesia's mobile banking service. This study examined various characteristics of respondents, including age (18 years of age or older), gender, and occupation. The following is a general description of the respondents involved in the study:

Normality Test

The assessment of whether data follow a normal distribution is called a normality test. For the Kolmogorov-Smirnov test a significance value greater than 0.05 indicates normal distribution. There are various approaches to testing data normality, and the results may differ based on the method chosen. Researchers used the Kolmogorov-Smirnov and P-Plot tests to evaluate the normality of the data. The results of this normality test are shown in the chart below

Table 3. Normality Test Result

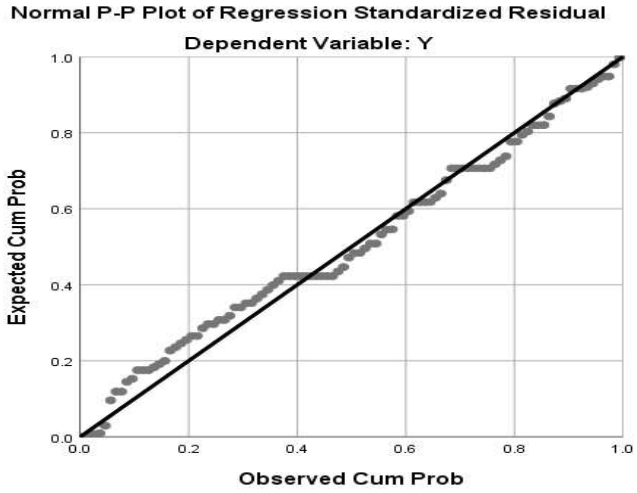
One-Sample Kolmogorov-Smirnov Test		
		Unstandardized Residual
N		100
Normal Parameters[a,b]	Mean	.0000000
	Std. Deviation	3.22794011
Most Extreme Differences	Absolute	.074
	Positive	.053
	Negative	-.074
Test Statistic		.074
Asymp. Sig. (2-tailed)		.197[c]
a. Test distributioni is Normal.		
b. Calculated from data.		
c. Lilliefors Significance Correction.		

Source: Data processed by researchers

Based on the findings presented in table 3, the Kolmogorov-Smirnov test produced a significance value (Asymp. 4). Sig) was 0.197, exceeding 0.05. The results led to the conclusion that the data used in this study followed a normal distribution.

With normal data distribution, researchers can proceed to the further analysis stage with a higher level of confidence in the results i obtained. Data normality also facilitates interpretation of analysis results, as many statistical modes are assumed to work optimally on normally distributed data. In addition, the normal distribution of data allows the use of parametric tests that have higher statistical strength than non-parametric tests.

Publikasi oleh: Yayasan Literasi Emas Nusantara
E-ISSN: 9999-9999 | P-ISSN: 9999-9999
Volume 0X Issue 0X, MM 202X
DOI : doi.org/reksy.v1i1.1



Graph 1. P-Plot Normality Results
Source: Data processed by researchers

Based on Graph 1 above, the normality test results from P-Plot show that the data points are clustered around a diagonal line, thus showing that the data follow a normal distribution. A spread close to this diagonal line indicates that the assumption of normality is satisfied, so statistical analysis requiring normal distributed data can be performed with higher validity.

Heteroskedasticity Test

The purpose of the heteroskedasticity test is to assess whether there are differences in residual variance between different observations in a regression model. A regression model is considered effective if the residual variance across all observations remains stable, a condition called homoscedasticity. Conversely, if the variance of the residue varies between observations, then it is called heteroskedasticity.

Table 4. Results of Heterocedsticity Test With the Glejser Test Coeffisien

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.834	1.552		1.826	.071
	Cyber Crime a. Dependent Variabel : RES2	-.014	.048	-.029	-.290	.772

Source: Data processed by researchers

Based on the results shown in table 4 which presented the findings of the heteroskedasticity test conducted using the Glejser method, the significance value of the independent variable (X) was 0.772. This number far exceeds the standard significance threshold of 0.05". Therefore, it can be concluded that this model does not indicate any heteroskedasticity related problems. It means that the residual variant remains constant for all free variable values, which is one of the important assumptions in classical linear regression analysis.

Publikasi oleh: Yayasan Literasi Emas Nusantara
E-ISSN: 9999-9999 | P-ISSN: 9999-9999
Volume 0X Issue 0X, MM 202X
DOI : doi.org/reksy.v1i1.1

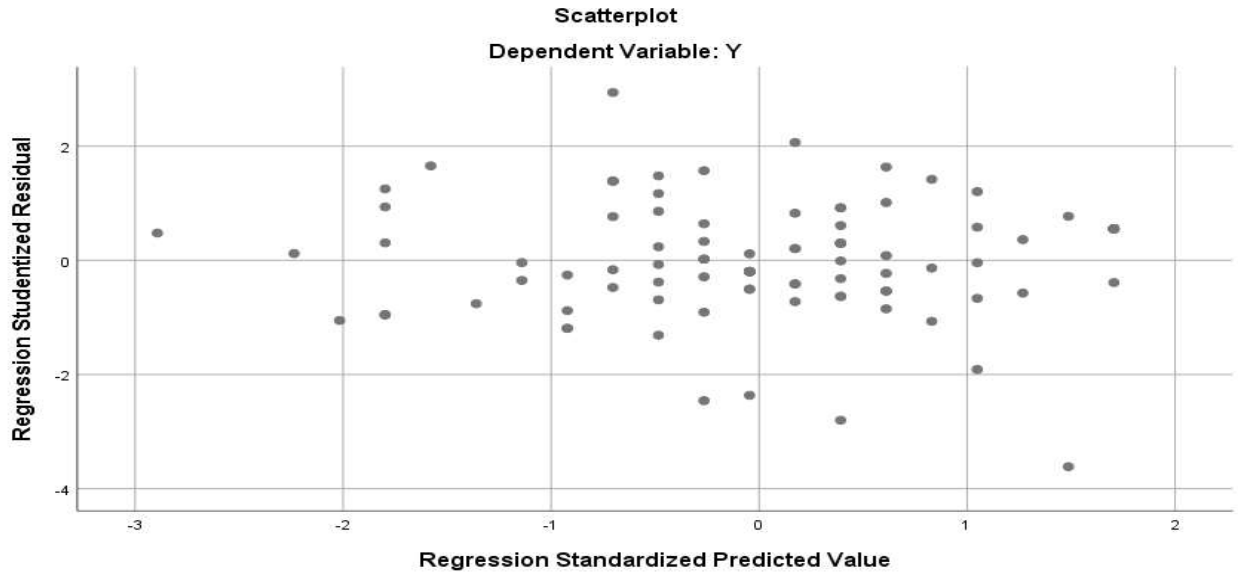


Chart 4. Heterocedsticity Test Results (Scatterplot)
Source: Data Processed by Researchers

Based on graph 1 the results of the Heteroskedasticity Test illustrated with Scatterplot show scattered points either above or below, or around zero. Moreover, the alignment of these points indicates that they are not just clustered at the top or bottom. These observations indicate the presence of heteroskedasticity symptoms..

Simple Regression Test

The purpose of the simple regression test is to assess the extent of the effect of the independent variable (X) on the dependent variable (Y). Therefore, a simple linear regression test is performed, and the results of the test are shown below

Table 5. Simple Regression Test Results Coeffisients

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	10.211	2.323		4.396	.000
	Cyber Crime a. Dependent variables: customer interest	.701	.071	.704	9.813	.000

Source: Data Processed by Researchers

Table 5 shows the regression coefficient values. The Constants value in the Unstandardized Coefficient column is 10.211 asccompanied by a regression direction coefficient value of 0.701. Therefore, the equation can be expressed as follows:

$$Y = a + bX + e$$
$$Y = 10.211 + 0.701 + e$$

Publikasi oleh: Yayasan Literasi Emas Nusantara
E-ISSN: 9999-9999 | P-ISSN: 9999-9999
Volume 0X Issue 0X, MM 202X
DOI : doi.org/reksy.v1i1.1

The equation presented can be understood as follows:

A constant value of 10.211 indicates that when the Cyber Crime variable remains constant then the customer interest variable (Y) will show a positive value of 0.701.

The regression coefficient of the Customer Interest variable (Y) is 0.701. This shows that an increase in customer interest of 1 unit results in an increase in customer interest rate in utilizing mobile banking of 0.701 or 70.1%. This shows that cybercrime variables have a positive effect on customers' interest in the use of sharia mobile banking.

Partial Significance Test Results (Test)

This test is performed to evaluate simple linear regression individually. The goal is to determine the significance of the independent variable (X) and its partial influence on the dependent variable (Y).

Table 6. Test Results (Partial) Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	10.211	2.323		4.396	.000
	Cyber Crime	.701	.071	.704	9.813	.000

Source: Data Processed by Researchers, 2024
a. Dependent Variable: Customer Interest

Based on the available tables, it is clear that cybercrime variables (X) have an effect on customer interest (Y). The count value is 9.813 which means the count exceeds the table t by 1.984 and the significance value is 0.0000 which is less than 0.05. Therefore, H0 was rejected while Ha was accepted, meaning that the cyber crime variable (X) had a significant and positive influence on the user interest variable (Y).

Coefficient of Determination Test (R2)

The Determination Coefficient Test (R2) shows the magnitude of the relationship between an independent variable, namely cybercrime (X) and a bound variable, User Interest (Y), reflecting how much influence a free variable has on the bound variable.

Table 7. Results of Coefficient of Determinasi (R2) testing Summary Model

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.704[a]	.496	.490	3.244

Source: Data Processed by Researchers, 2024
a. Predictors: (Constant), Cyber Crime

According to table 4.10, the adjusted R-squared value for the coefficient of determination (R2) is 0.490 or equivalent to 49.0%. This shows that the independent variable, cyber crime (X), has an effect of 49.0% on the dependent variable, namely the interest of customers using mobile banking from Bank Syariah Indonesia. At the same time, the remaining 51.0% had an impact on various factors that were not discussed in this study.

DISCUSSION

A test of the coefficient of determination (R2) showed that cyber crime affects customers' interest in using sharia bank mobile banking services with a yield of 0.490 or 49.0%. This shows that cybercrime has a significant impact on customers' interest in Bank Syariah Indonesia's mobile banking service, which accounts for nearly half of all the factors that affect it. In contrast, the remaining 51.0% was due to other variables not examined in this study, including transaction security, ease of use, customer service, and various external influences.

This finding shows a correlation in which the increase in Cyber Crime crimes leads to a decrease in customer interest in mobile banking services. This trend may stem from increasing customer concerns about the security of digital transactions. Consequently, sharia banks must prioritize security features in their mobile banking offerings to maintain and increase customer involvement with these services. An important strategy for mitigating the adverse effects of cybercrime is to improve transaction security measures and improve customer service to effectively address virtual crime problems.

Publikasi oleh: Yayasan Literasi Emas Nusantara
E-ISSN: 9999-9999 | P-ISSN: 9999-9999
Volume 0X Issue 0X, MM 202X
DOI : doi.org/reksy.v1i1.1

The findings of this study were supported by previous studies conducted by Nadia Tulfitri (2023). This study seeks to examine how security affects the interest of mobile banking users in Islamic banks among STIES Banda Aceh students. The results showed that security had a positive and significant impact on mobile banking users. Based on the determination coefficient test, R2 obtained a value of 0.345 which showed that the safety variable (X) was able to contribute 34.5% of the relationship with the user interest variable (Y), while the remaining 57.5% was associated with other variables. an influencing factor

The research findings are further supported by research conducted by Lutfhi Hazanatin Zahro (2023). This investigation aims to assess how the use of mobile banking and customer protection is related to cybercrime in Surakarta city. The results showed that the mobile banking user variable showed t = 1.194, smaller than t table = 0.17, at a significance level of 0.036, which is below 0.05. Therefore, H0 was rejected and H1 was accepted, meaning that the hypothesis test results showed a significant effect on mobile banking users' variables on crime.

The research conducted by Dinda Adhelia Ashifa with the title Affecting Accessibility, Brand Equity, and Cyber Crimester has applied the user's confidence in producing E-banking. Bank Syariah Indonesia (KCP) is a subsidiary of Bank Syariah Indonesia. Cape Coral. Based on the research results, there were positive and significant results between the accessibility and cybercrime of partial bank-product customer trust. However, for variable brand equity, there is no partial significant influence. Simultaneously, the variables of accessibility, brand equity and cybercrime are positive and significant. Accessibility, Brandequity and cybercrime have suggested with Islamic economic principles and are now contributing together in increasing customer confidence in producing E-banking.

Research conducted by Rika Nur Erfiana (2023). With the title The Influence of Cyber Crime and E-banking on the Satisfaction of Customers of Bank Syariah Indonesia. Case studies on the students of the grand solos. Based on the research results, there are results that cybercrime and e-banking have an effect on customer satisfaction of Indonesian Islamic bank users with a T-test result of 5,126 with a table of 1.94, meaning t-count > t-table. Significant value of 0.01 thus significant value < 0.05. According to the provisions, the H0 result was rejected by H1 is accepted, meaning that the cyber crime variable (X) affects the customer satisfaction variable (Y).

CONCLUSION

Based on the results and discussions of the research presented on the information, it was concluded that cyber crime was positive and significant for the interest of Pekanbaru city community customers in holding mobile banking bank syariah indonesia. "If cyber crime continues to increase, it is likely that customer interest in mobile banking will decrease. Therefore, it is important for bank syariah indonesia to increase the security of their banking motival to close customer trust and encourage wider use. To organize this challenge and improve the sub-district with mobile banking bank syariah indonesia, efforts must focus on customer education, improving services, and implementing strategic steps.

SUGGESTIONS

Based on the findings of this study there are several suggestions and from the following: With the conclusion of this study, there are results that cybercrime has a positive and significant influence on customers' interest using Indonesian sharia bank mobile banking. Makassar researchers knock on Bank sharia Indonesia are more supportive of customer data because it is one of the factors that affects customers' interest in developing Indonesia's mobile banking sharia bank. Customers are advised to be more careful in conducting digital transactions for customers. Make sure to always update the mobile banking application to the latest version and use the password Strong for the sake of customer security and personal data. For academics, with this research suggestions for the essence of educators and the ability to Cultivate to Develop a Deeper Curriculum on Cybercrime and Its Implications in the Sector

REFERENCES

Afriani, S., Trisna Yanti, R., & Economics at Dehasen University Bengkulu, F. Entrepreneurial Interest in Women in Bengkulu City.*08*(01), 1–14.

Ahdiat Adi. (2023). Digital Banking Transactions in Indonesia Grow 158% in the Last 5 Years. In *Https://Databoks.Katadata.Co.Id/Datapublish/2023/07/05/Transaksi-Digital-Banking-Di-Indonesia-Tumbuh-158-Dalam-5-Tahun-Terakhir*.

Anonim. (2021). Mobile Banking: Understanding, Function, Features, Advantages and Disadvantages.In *Cardlez*. https://cardlez.com/mobile-banking/

Aprianto, I. G. L. A. (2022). Literature Review: UTAUT Model Technology Acceptance CONSTELLATION: Convergence of Technology and Information Systems, *2*(1), 138–144. https://doi.org/10.24002/konstelasi.v2i1.5377

Ashifa, D. A. (2023). The Effect of Accessibility, Brand Equity, and Cyber Crime on E-Banking Product Users' Trust Levels.*Angewandte Chemie International Edition, 6(11), 951–952.*, *2*.

Azwar, S. (2015). *Metode Penelitian*.

bankbsi.co.id. (2021). About We - Corporate Information | Sharia Bank of Indonesia. - It's Https://Bankbsi.Co.Id. https://www.bankbsi.co.id/company-information/tentang-kami

Busyro, W., Jamilah, P., & Septianingsih, R. (2020). The Effect of Services on Community Decisions in Selecting Sharia Bank Services in Rokan Hulu Regency. *Jurnal ISLAMIKA*, *3*(1), 197–202.

Chusna, F. (2023). What's Cyber Crime? Definition, Type, and Case Examples. In Linknet enterprise. Disdukcapil, 2023. (2023). Data Agregat Kependudukan Kota Sukabumi. *Disdukcapil Kota Sukabumi 2023*, *2*.

Erfiana, R. N. (2023). The Effect of Cyber Crime and E-Banking on the Satisfaction of Customers of Bank Sharia Indonesia (Study Case of Solo Raya Students). *Journal of Engineering Research*.

Fadhlurrahman, I. (2024). Riau's popuslation reaches 6.86 million people, 16% of them are in Pekanbaru City by the end of 2023. In Databoks.

Fitri, J. (2021). The Influence of Internet Banking and Cyber Crime on Customers' Trust in Sharia Banking (Study on Independent Sharia Bank Tapan Tuan). September *2016*, 1–6.

Gunawan, H. (2020). Cybercrime Crime in the perspective of Fikih Jinayah. Journal of El-Qanuniy: Journal of the Sciences of Paganism and Social Affairs, 6(1), 96–110. https://doi.org/10.24952/el-qanuniy.v6i1.2473

Haditya, F. (2020). The Effect of Cyber Crime on the Loyalty of E-Banking Product Customers (Study Case of Sharia Bank Customers in Indonesia).1–23.