The Impact of Cybercrime on Customer Trust in Bank Syariah Indonesia

Sriwahyuni Rustan[1], Ifayani Haanurat[2], Nurlina[3]*
[1,2,3]Universitas Muhammadiyah Makassar, Makasssar, Indonesia

ARTICLE INFORMATION

Received: July 24, 2025
Revised: January 24, 2026
Accepted: April 11, 2026
DOI : 10.57151/jeko.v5i1.1079

KEYWORDS

banking; cybercrime; customers; trust

CORRESPONDING AUTHOR

Name : Sriwahyuni Rustan
Address: Gowa, Indonesia
E-mail : swhynir02@gmail.com

A B S T R A C T

This study aims to analyze the influence of cybercrime on customer trust in Bank Syariah Indonesia (BSI). A quantitative approach was employed, using a survey method by distributing questionnaires to BSI customers who have used digital banking services. The research instrument was structured using a Likert scale and analyzed with the help of SPSS version 30.0. The results of the analysis indicate that cybercrime has a positive and significant effect on customer trust. This means that the higher the level of threat or experience related to cybercrime, the greater the impact on decreasing customer trust in the security and digital services provided by the bank. These findings also reveal that customers' perceptions of digital security greatly influence their confidence in conducting banking transactions. Therefore, banking institutions, particularly BSI, need to strengthen their cybersecurity systems, continuously educate customers about digital safety, and ensure transparency in handling security incidents to maintain and enhance customer trust. This research contributes to the existing literature on customer trust and highlights the importance of data protection in the era of banking digitalization.

INTRODUCTION

The advancement of internet technology has made a major contribution to driving innovation in the field of information and communication, including the banking sector. Globalization requires banks, both conventional and Islamic, to utilize digital technology to improve efficiency and service quality. The presence of technology has brought changes to various aspects of people's lives (Astiansyah & Damayanti, 2024). Technology creates convenience for humans in carrying out various activities. Digital transformation has become a primary necessity for Islamic banking to remain competitive in an increasingly competitive digital economy era. In Indonesia, the development of Islamic banking is supported by various regulations, such as Law No. 10 of 1998 concerning Banking and Law No. 21 of 2008 concerning Islamic Banking, as well as PBI No. 4/1/PBI/2002 (Nurul Muyasaroh, 2022). These regulations strengthen the position of Islamic banks as part of the national financial system that can compete on equal terms with conventional banks.

Although Indonesia is one of the countries with the largest Muslim population in the world and has shown progress in developing the Islamic financial system, Islamic accounting practices in Indonesia still face several fundamental challenges. Amid the rapid development of digital technology that brings convenience and efficiency to Islamic banking services, serious threats have also emerged in the form of cybercrime, which has the potential to disrupt customer data security and reduce trust in Islamic financial institutions (Saputri & Sihotang, 2023). Cybercrime refers to criminal acts that utilize computer networks and digital technology to gain illegal access to information systems, with the aim of stealing data, damaging systems, or obtaining financial benefits unlawfully (Butarbutar, 2023). In the banking context, such crimes can have significant impacts, ranging from the leakage of customers' personal data and disruption of financial transaction services to substantial material losses. Under these conditions, a sense of security becomes a fundamental factor in building and maintaining customer trust in financial institutions (Amalia, 2024). If digital security systems are perceived as weak, public trust in banking institutions can decline drastically.

The threat of cybercrime to the banking sector in Indonesia shows an increasing and concerning trend. Along with the development of digital technology, the complexity and sophistication of cybercrime methods have also increased, posing major challenges for financial institutions in safeguarding their security systems (Harahap et al., 2025). Various cases in recent years indicate the existence of security vulnerabilities that have not been fully addressed and have become a serious public concern. For example, a skimming case involving Bank Rakyat Indonesia (BRI) in 2016 recorded losses of approximately IDR 2.7 billion and involved at least 515 customers whose data

were stolen through information theft techniques from ATM cards at modified EDC machines (Cahyadi & Gorda, 2019).

Cybercrime issues in the banking sector initially developed as a global problem in line with the increasing use of digital technology in financial systems. The digitalization of banking services indeed provides convenience and efficiency, but at the same time opens opportunities for various forms of cybercrime, such as system hacking, data theft, phishing, and ransomware attacks. These threats do not occur in a single country, but have become shared risks faced by financial institutions worldwide. The development of this global issue is then reflected in the national context of Indonesia. The increasing use of digital banking services by the public has made the banking sector more vulnerable to cyberattacks. Several cases of data breaches and system disruptions that have occurred in Indonesian banks show that cybercrime has become a real problem rather than merely a theoretical threat. This condition also affects public perceptions of the security of digital banking services and their level of trust in banks.

Bank Syariah Indonesia (BSI), as the largest Islamic bank in Indonesia, faces similar challenges. BSI's dependence on digital services makes cybersecurity a crucial factor in maintaining customer trust. The digital service disruption experienced by BSI in 2023 illustrates how global cybercrime issues can have a direct impact on bank operations and customer perceptions. Although the bank stated that customer data and funds remained secure, the service disruption caused concern among customers and affected their sense of security when conducting transactions. In addition, the leakage of Bank Jatim customer data that was illegally traded on online forums with a value of IDR 3.5 billion in 2024 demonstrates the weakness of digital data protection systems and indicates that cybersecurity has not yet become a fully integrated priority in banking risk management (Duana et al., 2024). These cases serve as concrete evidence that cybercrime risks are not merely technical issues, but also have direct implications for public trust in banking institutions.

In 2023, Bank Syariah Indonesia (BSI), the largest Islamic financial institution in Indonesia, experienced a significant incident related to system hacking and alleged customer data theft. The incident began on May 8, when many users complained about being unable to access mobile banking services (Saputri & Sihotang, 2023). The disruption continued until May 11, triggering widespread concern and various speculations on social media and among the general public. After services returned to normal on May 15, claims emerged from a group of hackers who alleged that they had successfully breached BSI's internal systems and stolen sensitive customer data. Although BSI management, through Corporate Secretary Gunawan A. Hartoyo, stated that customer funds and data remained secure and that the bank would coordinate with authorities such as the Financial Services Authority and the National Cyber and Crypto Agency (Pohan et al., 2024), the incident left a significant trace of distrust among customers. This demonstrates that perceptions of digital security are crucial in shaping and maintaining customer loyalty toward Islamic banking services.

Although many studies have discussed customer trust in the context of digital banking services, there are still limited studies that specifically examine how cybercrime affects customer trust in Islamic banks, which have distinct characteristics and values compared to conventional banks. Islamic banks emphasize principles of justice, transparency, and trust as the foundation of the relationship between customers and the bank. However, when digital security, which serves as the foundation of trust, is compromised, these values are also put at risk. Therefore, this study is important to fill the existing literature gap and to provide empirical understanding of the real impact of cybercrime on customer trust in Islamic financial institutions such as BSI. The findings of this study are expected to serve as a reference for Islamic banking in designing digital security strategies that are not only technical in nature, but also consider customer perceptions and psychological aspects

.

METHOD

This study adopts a quantitative approach, which is a scientific method that emphasizes numerical and statistical data analysis to test previously formulated hypotheses. This approach is selected because it provides a systematic, objective, and measurable description of the relationship between the variables examined, namely Cybercrime and Customer Trust in Bank Syariah Indonesia (BSI). The data used in this study consist of two types, namely secondary data and primary data. Secondary data are obtained from various documents, journals, scientific articles, official reports, and other literature relevant to the research topic. Meanwhile, primary data are collected directly from respondents through the distribution of questionnaires as the main data collection instrument.

The population in this study comprises all customers of Bank Syariah Indonesia. However, due to the very large and undefined population size, the researcher selected a sample of 100 respondents. The determination of the sample size was carried out using the Slovin formula, which is appropriate for studies with large and inaccessible populations. The sampling technique used is non-probability sampling with an accidental sampling method, namely selecting respondents based on individuals who coincidentally meet the researcher and fulfill the predetermined criteria. The criteria for respondents in this study are active BSI customers who have used banking services for at least three to four years and conduct banking transactions at least three times per week. These criteria ensure that respondents have sufficient experience to provide relevant answers to the questionnaire items.

Data collection was conducted by distributing closed-ended questionnaires designed using a five-point Likert scale to measure respondents' attitudes, perceptions, and beliefs toward each statement item. This scale allows respondents to assess each statement using response options ranging from strongly disagree to strongly agree. The collected data were then analyzed using descriptive statistical techniques to describe respondent characteristics and data distribution, as well as inferential statistics to test hypotheses and examine relationships between variables. The analysis process was carried out using SPSS version 30, which facilitates validity testing, reliability testing, normality testing, heteroscedasticity testing, and simple linear regression analysis. Through these techniques, this study aims to objectively and measurably determine the extent to which cybercrime affects the level of customer trust in BSI.

The cybercrime variable in this study is measured using the following indicators:

1. Digital banking system security. Measures customer perceptions of BSI's ability to protect digital services from cyberattacks.
2. Personal data protection. Measures customer confidence that their personal and financial data are not easily accessed by unauthorized parties.
3. Risk of system hacking. Measures customer perceptions of the likelihood of hacking incidents in BSI's digital banking system.
4. Experience or information related to cybercrime. Measures the extent to which customers have experienced or are aware of cybercrime cases in banking services.
5. Digital transaction security. Measures customers' sense of security when conducting transactions through mobile banking and internet banking.
6. Phishing and digital fraud threats. Measures customer perceptions of fraud risks through messages, links, or other digital media.
7. Misuse of customer accounts. Measures customer concerns regarding unauthorized account usage.
8. Reliability of the bank's cybersecurity system. Measures customer perceptions of BSI's preparedness and capability in preventing cybercrime.
9. Impact of cybercrime on transaction convenience. Measures the influence of cybercrime threats on customer comfort when using digital services.

Customer Trust Variable Indicators

The customer trust variable in this study is measured using the following indicators :

1. eliability of banking services. Measures customer confidence that BSI provides stable and consistent services.
2. Transaction security. Measures the level of customer trust in the security of financial transactions at BSI.
3. Confidentiality of customer information. Measures confidence that personal and transaction data are kept confidential.
4. Bank integrity. Measures customer perceptions of BSI's honesty and responsibility in protecting customers.
5. Bank competence in managing digital risk. Measures BSI's ability to manage and handle cybercrime risks.
6. Information transparency. Measures the bank's openness in providing information related to security risks or service disruptions.
7. Sense of security in transactions. Measures customer comfort and sense of safety when using digital services.
8. Trust in the bank's digital system. Measures customer confidence in the reliability of the technology used by BSI.

9. Trust-based loyalty. Measures customers' tendency to continue using BSI services based on trust.

RESULT& DISCUSSION

Validity Test

The validity test is a process used to assess the extent to which a research instrument is able to measure what it is intended to measure (Saputri & Sihotang, 2023). The purpose of this test is to ensure that each item in the instrument is truly relevant and appropriate for measuring the intended variables. In this study, validity is tested by comparing the calculated r value with the r table value at a significance level of 0.05. If the calculated r value exceeds the r table value, the item is considered valid. Conversely, if the calculated r value is lower than the r table value, the item is considered invalid. The validity testing in this study is conducted on the items of the Cybercrime variable (X) and the Customer Trust variable (Y).

Table 1. Validity Test

Variable	Item	Calculated r Value	r Table Value	Description
(X) Cyber crime	X.1	0.596	0.196	Valid
	X.2	0.574	0.196	Valid
	X.3	0.567	0.196	Valid
	X.4	0.640	0.196	Valid
	X.5	0.634	0.196	Valid
	X.6	0.686	0.196	Valid
	X.7	0.515	0.196	Valid
	X.8	0.733	0.196	Valid
	X.9	0.490	0.196	Valid
(Y) Customer Trust	Y1	0.753	0.196	Valid
	Y2	0.730	0.196	Valid
	Y3	0.806	0.196	Valid
	Y4	0.774	0.196	Valid
	Y5	0.745	0.196	Valid
	Y6	0.711	0.196	Valid
	Y7	0.740	0.196	Valid
	Y8	0.764	0.196	Valid
	Y9	0.699	0.196	Valid

Source: Processed Data, 2025

Based on the results of the validity test presented in Table 1, all statement items used in the questionnaire for both research variables, namely Cybercrime (X) and Customer Trust (Y), show calculated r values (Corrected Item–Total Correlation) that are greater than the r table value of 0.296. For the Cybercrime variable, statement items numbered 1 to 9 meet the validity criteria, indicating that each item has a sufficiently strong correlation with the total score of the variable. A similar result is found for the Customer Trust variable, where all items from number 1 to 9 are declared valid because their calculated r values also exceed the predetermined r table value. It can therefore be concluded that all items for both research variables are valid, meaning they are capable of accurately measuring the intended aspects or constructs. High instrument validity is a crucial prerequisite in quantitative research, as it ensures that the collected data truly represent actual conditions in the field. The validity of this instrument also supports the accuracy of the analysis and the reliability of the conclusions drawn in this study, particularly in evaluating the impact of cybercrime on customer trust in Bank Syariah Indonesia (BSI).

Reliability Test

The reliability test is conducted to assess the extent to which the research instrument produces consistent data (Subhaktiyasa Gede Putu, 2024). In addition, item difficulty analysis aims to determine whether the questions presented are categorized as easy or difficult. Reliability is determined using Cronbach's Alpha value, where an instrument is considered reliable if the alpha value exceeds the minimum threshold of 0.60 at a significance level of 5%.

Table 2. Reliability test

Variable	ronbach's Alpha Value	Reliability Standard	Description
Cyber Crime (X)	0.778	0.60	Realibel
Kepercayaan Nasabah (Y)	0.899	0.60	Realibel

Source: Processed Data, 2025

Based on Table 2, the results of the reliability test for both variables, namely Cybercrime and Customer Trust, indicate that all questionnaire items have Cronbach's Alpha values exceeding 0.60. This value represents the minimum threshold commonly used to determine the reliability level of a research instrument. Therefore, it can be concluded that the instrument used in this study is reliable, meaning it is capable of producing consistent measurement results when applied under similar conditions. High instrument reliability is essential because it ensures that the variables under study are measured accurately, allowing the findings to be trusted and used as a basis for drawing valid scientific conclusions. This reliability also strengthens the overall integrity of the research methodology, particularly in examining the relationship between cybercrime and the level of customer trust in Bank Syariah Indonesia (BSI).

Normality Test

The normality test is used to determine whether the residual data in this study are normally distributed, which is one of the prerequisites in linear regression analysis (Nurajizah & Sari, 2023). Data normality is important to ensure that the results of the statistical analysis can be interpreted validly and without bias. The normality test is conducted using the Kolmogorov–Smirnov method, with the following decision criteria: if the significance value (Asymp. Sig. 2-tailed) is greater than 0.05, the residual data are considered to be normally distributed. Conversely, if the significance value is less than or equal to 0.05, the data are considered not normally distributed.

Table 3. Normality Test

One-Sample Kolmogorov-Smirnov Test

			Unstandardized Residual
N			100
Normal Parameters[a,b]	.0000000		.0000000
	4.41606513		3.75730430
Most Extreme Differences	.067		.087
	.053		.087
	-.067		-.077
Test Statistic			.067
Asymp. Sig. (2-tailed)[c]			.200[d]
Monte Carlo Sig. (2-tailed)[d]	.321		.060
	.309	Lower Bound	.054
		Upper Bound	.067

Source: Processed Data, 2025

Based on the data processing results presented in Table 3, the Kolmogorov–Smirnov test shows an Asymp. Sig. (2-tailed) value of 0.062. Since this significance value is greater than the 0.05 significance level (0.062 > 0.05), it can be concluded that the residual data in this study are normally

distributed. With the normality assumption fulfilled, the regression model used in this study can be considered appropriate for further analysis. The normality assumption is an important requirement in linear regression, as it ensures that the error terms are normally distributed, which in turn provides valid and unbiased estimation results. Therefore, the presence of normally distributed residuals supports the quality and accuracy of the model in examining the effect of cybercrime on customer trust in Bank Syariah Indonesia (BSI).

Heteroscedasticity Test

The heteroscedasticity test aims to determine whether the variables have equal variance across the residuals from one observation to another (Saputri & Sihotang, 2023). If the significance value (Sig.) is greater than 0.05, heteroscedasticity does not occur. The following table presents the results of the heteroscedasticity test.

Tabele4. Heteroscedasticity Test

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.636	1.457		1.123	.264
	Cyber Crime	.058	.045	.131	1.310	.193

a. Dependent Variable: Abs_RES

Source: Processed Data, 2025

Based on the data processing results presented in Table 4, the significance value (Sig.) for the cybercrime variable is 0.193. This value is greater than the predetermined significance level of 0.05 (0.193 > 0.05), indicating that no heteroscedasticity is present in the regression model used. Thus, the distribution of residuals or errors in the regression model is homogeneous or constant across all values of the independent variable. The absence of heteroscedasticity suggests that the regression model satisfies one of the important classical assumptions in regression analysis, thereby supporting the validity and reliability of the regression parameter estimates. Therefore, the regression analysis results can be considered reliable in describing the relationship between cybercrime and the level of customer trust in Bank Syariah Indonesia (BSI).

Simple Linear Regression Analysis

Simple linear regression analysis is used in this study to determine the extent to which the independent variable, namely Cybercrime, affects the dependent variable, namely Customer Trust in Bank Syariah Indonesia (Putri Amalia & Hastriana, 2022). This analysis aims to measure the strength of the relationship between the two variables and to predict the value of the dependent variable based on changes in the independent variable. By using one independent variable and one dependent variable, this model provides a clear description of a simple yet significant causal relationship. Simple linear regression also indicates the direction of the relationship, whether positive or negative, as well as the level of significance of the effect of cybercrime on customer trust.

Table 5. Simple Linear Regression Analysis

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	26.616	2.445		10.886	<.001
	Cyber Crime	.350	.075	.427	4.672	<.001

a. Dependent Variable: Kepercayaan Nasabah

Source: Processed Data, 2025

Based on the SPSS output in Table 5, the simple linear regression model can be formulated as follows:

$Y = a + bX$

$Y = 26.616 + 0.350X.$

The results of the simple linear regression analysis indicate that the constant (intercept) value (a) is 26.616. This means that when the independent variable, namely cybercrime, is in a constant condition or does not change (value of zero), the value of the dependent variable, customer trust, remains at 26.616. In other words, customer trust in Bank Syariah Indonesia (BSI) still exists at a

certain level even without the influence of cybercrime. The regression coefficient or slope value (b) of 0.350 indicates a positive direction of the relationship between cybercrime and customer trust.

This means that every one-unit increase in the cybercrime variable is followed by an increase of 0.350 in the customer trust value. This interpretation confirms that increased attention to cybercrime aspects, including awareness, understanding, and prevention and mitigation efforts, can enhance customers' sense of security when conducting digital transactions, thereby increasing their level of trust in Islamic banking institutions. These findings highlight the importance of professional and sustainable cybersecurity risk management by banks, as well as adequate customer education to build awareness and vigilance against potential cybercrime threats within the digital banking ecosystem.

T-Test (Partial Test)

The t-test is conducted to examine the extent to which the independent variable influences the dependent variable in this study (Ismulyaty et al., 2022). The following table presents the results of the t-test.

Table 6. t-Test

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	26.616	2.445		10.886	<.001
	Cyber Crime	.350	.075	.427	4.672	<.001
a. Dependent Variable: Kepercayaan Nasabah						

Source: Processed Data, 2025

Based on the data analysis results presented in Table 6, a significance value of 0.001 is obtained, which is far below the predetermined significance level of 0.05. In addition, the calculated t value of 4.672 is greater than the t table value of 1.661. These two indicators provide strong statistical evidence that there is a significant relationship between the independent variable, Cybercrime (X), and the dependent variable, Customer Trust (Y). Therefore, the null hypothesis (H_0), which states that cybercrime has no effect on customer trust, is rejected, while the alternative hypothesis (H_a), which states that cybercrime has a significant effect, is accepted. These results indicate that cybercrime has a real impact on the level of customer trust in Bank Syariah Indonesia (BSI). This means that the higher the intensity or presence of cybercrime threats, the greater the likelihood that customer trust will be affected, either directly or indirectly. The findings emphasize the importance of data protection, digital transaction security, as well as bank transparency and responsiveness in addressing cybersecurity issues as crucial elements in building and maintaining customer trust in the current digital era.

Coefficient of Determination (R^2)

The coefficient of determination (R^2) is a value that describes the proportion or percentage of the total variation in the dependent variable (Y) that can be explained by the independent variable (X)

Table 7. Coefficient of Determination (R^2)

Model Summary[b]				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.427[a]	.182	.174	4.439

Source: Processed Data, 2025

Based on the data processing results in Table 7, the R Square value is 0.182, indicating that the Cybercrime variable contributes 18.2% to the variation in Customer Trust. Thus, it can be concluded that the effect of cybercrime on customer trust is real but not dominant. Meanwhile, the remaining 81.8% is explained by other variables not examined in this study, such as service quality, system security, bank reputation, and other external factors.

Cybercrime is a serious threat to internet users, including those in the banking sector. Based on the survey results and data analysis, this study finds that cybercrime has a positive and significant effect on customer trust (Hayatin Nupus et al., 2025). The findings also reveal that, partially, the cybercrime variable has a significant influence on the level of customer trust in Bank Syariah Indonesia (BSI). This is evidenced by the t-test results, which show a significance value of 0.001, lower than the 0.05 significance level, and a calculated t value of 4.672, which is higher than the t table value of 1.661. Accordingly, the null hypothesis (H_0), which states that cybercrime has no effect

on customer trust, is rejected, while the alternative hypothesis (H_a) is accepted. These results statistically demonstrate that the presence and threat of cybercrime have a real impact on customers' perceptions, attitudes, and levels of trust in the security of digital-based Islamic banking services.

The findings also indicate that aspects such as customers' level of knowledge about cybercrime risks, personal or social experiences related to such incidents, and the extent to which personal data protection is guaranteed by the bank are important factors in shaping customer trust. Trust is not built solely through promotions or friendly services, but also through a sense of security that arises from systemic protection against potential cyber threats (Hayatin Nupus et al., 2025). In this context, efforts to prevent and control cybercrime through continuous updates of digital security systems, digital literacy education for customers, and transparency in handling security incidents become strategic steps. These efforts not only enhance customers' sense of security in conducting digital transactions, but also strengthen their loyalty to Islamic banking institutions.

This study further reveals that customers' level of knowledge regarding cybercrime plays a significant role in forming and influencing their trust in digital banking services. When customers have limited understanding or are unaware of various forms and modes of cybercrime, they tend to be more vulnerable and less vigilant in protecting their personal information. This condition can ultimately reduce their sense of security and create anxiety when conducting online financial transactions. Customer trust is a key component in supporting the sustainability and operational stability of a banking institution, as it reflects confidence in the bank's ability to provide security, comfort, and reliability in every service offered. As the reliability of the bank's cybersecurity system increases, customer trust in the institution also increases. In the context of this study, the respondents are customers of Bank Syariah Indonesia (BSI), which had previously experienced or was indirectly affected by a ransomware attack that disrupted part of its digital services. This experience psychologically and emotionally influenced customers' perceptions of the bank's information system security and shaped their level of trust going forward.

The study also shows that customers' personal experiences, either directly or through information obtained from their social environment regarding cybercrime incidents, have a considerable influence on their trust in digital banking services. Customers who have had negative experiences or possess sufficient knowledge about incidents such as account hacking, personal data theft, or system disruptions due to cyberattacks tend to be more skeptical and less confident in the bank's digital systems to protect their information and transactions. This lack of trust can lead to discomfort, excessive concern, and even fear of fully using electronic banking services. In some cases, it may cause customers to withdraw from digital banking usage and prefer conventional transaction methods that are perceived as safer (Safitri & Fasa, 2024). Therefore, it is crucial for banking institutions not only to enhance cybersecurity systems, but also to provide education and transparent information to customers so that they can understand and respond appropriately to cybercrime threats, thereby maintaining and increasing trust in banking institutions.

Furthermore, the results emphasize that the protection of customers' personal data plays an important role in building trust in Bank Syariah Indonesia (BSI). When customers are confident that their personal and financial information is properly managed and secured, they feel more comfortable and trust the banking institution more. Optimal data protection not only increases transaction security, but also encourages long-term customer loyalty. This finding is consistent with the study by Febriana and Indrarini (2024), which concludes that the higher the level of cybersecurity in the Islamic banking industry, the higher the level of customer trust in Islamic banks. Therefore, it is essential for banking institutions, particularly Islamic banks, to continuously develop and strengthen their digital security infrastructure as an effort to maintain stability and customer trust in the era of digital transformation.

CONCLUSION

Based on the results of the data analysis in this study, it can be concluded that cybercrime has a positive and significant effect on the level of customer trust at Bank Syariah Indonesia (BSI). This finding indicates that the higher the intensity of perceived or known cybercrime threats, the lower the level of customer trust in digital banking services. This condition is in line with growing public concern over incidents such as account hacking, personal data theft, and fraud through digital banking applications. These incidents directly create a sense of insecurity in conducting transactions, especially when customers have personal experiences or know others who have been affected by similar cases. Although the bank has implemented various efforts to strengthen its digital security systems, these

measures have not fully restored customer confidence, particularly when they are not accompanied by transparent communication and continuous education regarding digital security.

Several limitations of this study should be considered for future research. First, this study focuses only on one independent variable, namely cybercrime, as the main factor influencing customer trust. In reality, customer trust in financial institutions can also be influenced by other factors such as service quality, system reliability, customer experience, institutional reputation, and the level of digital literacy and awareness among customers. Second, the scope of this study is limited to customers of Bank Syariah Indonesia at one sub-branch office in Makassar. Therefore, the results cannot be directly generalized to all Islamic banks in Indonesia, let alone to conventional banks with different service characteristics. Third, the quantitative approach used, particularly through closed-ended questionnaires, is not sufficient to capture complex psychological and emotional dimensions, such as fear, digital trauma, or subjective perceptions of cybercrime risk. Therefore, future studies using qualitative or mixed-method approaches are recommended to provide a more comprehensive and in-depth understanding of this issue.

REFERENCES

Amalia. (2024). Pengaruh Cyber Crime Terhadap Tingkat Kepercayaan Masyarakat Dalam Bertransaksi Di Bank Syariah Kota Pekanbaru. *Jurnal Islamika*, *7*(01), 75–90. https://doi.org/10.37859/jsi.v7i01.7713

Astiansyah, S. A., & Damayanti, S. D. (2024). Analisis Preferensi Penggunaan Quick Response Code Indonesian Standard (QRIS) Pada Generasi Z. *Jurnal Ekonomi Dan Bisnis*, *3*(2), 96–101. https://doi.org/10.57151/jeko.v3i2.389

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Jurnal Hukum & Pembangunan*, *2*(2). https://doi.org/10.21143/telj.vol2.no2.1043

Cahyadi, I. K. P., & Gorda, A. A. . N. S. R. (2019). Perlindungan Hukum Terhadap Nasabah dari Ancaman Perbankan Skimming Melalui Layanan Electronic Banking (Studi Kasus Di Bank Rakyat Indonesia Kantor Wilayah Denpasar). *Jurnal Analisis Hukum*, *2*(2), 116–128. http://journal.undiknas.ac.id/index.php/JAH/article/view/2208

Duana, G. R., Masyar, A., & Wulandari, C. (2024). TINJAUAN TEORI KRIMINOLOGI DALAM KEJAHATAN SIBER (KASUS KEBOCORAN DATA NASABAH) Overview of Criminological Theory in Cyber Crime (Customer Data Leakage Cases). *Jurnal Prioris*, *11*(2), 161–174. https://doi.org/10.25105/prio.v11i2.18959

Febriana, V. C., & Indrarini, R. (2024). Pengaruh Cyber Crime Dan Cyber Security Terhadap Tingkat Kepercayaan Nasabah Bank Syariah Dalam Menggunakan Layanan M-Banking Di Wilayah Surabaya. *Jurnal Ekonomika Dan Bisnis Islam*, *7*(3), 161–174. https://journal.unesa.ac.id/index.php/jei

Harahap, S. S., Halkis, M., & Sutanto, R. (2025). Advanced Persistent Threat (APT) sebagai Ancaman Perang Siber Asimetris Terhadap Pemerintah Indonesia. *Innovative: Journal Of Social …*, *5*, 4465–4485. http://j-innovative.org/index.php/Innovative/article/view/19091%0Ahttps://j-innovative.org/index.php/Innovative/article/download/19091/13149

Hayatin Nupus, Ayu Kartini, & Lidia Desiana. (2025). Pengaruh Cyber Crime dan Persepsi Keamanan Terhadap Tingkat Kepercayaan Pengguna Produk E-banking (Survei Pada Pengguna E-banking Bank Syariah di Indonesia). *Jurnal Semesta Ilmu Manajemen Dan Ekonomi*, *1*(3), 102–116. https://doi.org/10.71417/j-sime.v1i3.202

Ismulyaty, S., Nurmaini, & Roni, M. (2022). Pengaruh Kualitas Layanan Dan Kepuasan Pengguna Internet Banking Terhadap Loyalitas Nasabah Bank Syariah Indonesia (Bsi Kalirejo). *NISBAH: Jurnal Perbanka Syariah*, *8*(1), 66–75. https://doi.org/10.30997/jn.v8i1.6117

Nurajizah, N., & Sari, R. M. (2023). Pengaruh Kemudahan Dan Kualitas Informasi Terhadap Minat Mahasiswa Dalam Penggunaan Layanan M-Banking Pada Bank Syariah. *Jurnal Al-Fatih Global Mulia*, *5*(1), 57–70. https://doi.org/10.59729/alfatih.v5i1.61

Nurul Muyasaroh. (2022). Eksistensi Bank Syariah dalam Persfektif Undang-Undang No.21 Tahun 2008 Tentang Perbankan Syariah. *Syarikat: Jurnal Rumpun Ekonomi Syariah*, *5*(2), 12–31. https://doi.org/10.25299/syarikat.2022.vol5(2).10657

Pohan, R. N. A., Rokan, M. K., & Syarvina, W. (2024). Faktor-Faktor Yang Mempengaruhi Penggunaan Mobile Banking Pada Layanan BSI Mobile Dengan Menggunakan Model Unified Theory Of Acceptance And Use Of Technology (UTAUT). *Jurnal Manajemen Akuntansi (JUMSI)*, *4*(3), 732–740. https://doi.org/10.36987/jumsi.v4i3.4025

Putri Amalia, & Hastriana, A. Z. (2022). Pengaruh Kemanfaatan, Kemudahan Keamanan, dan Fitur M-Banking terhadap Kepuasan Nasabah dalam Bertransaksi pada Bank Syariah Indonesia (Studi Kasus BSI KCP Sumenep). *Alkasb: Journal of Islamic Economics*, *1*(1), 70–89. https://doi.org/10.59005/alkasb.v1i1.163

Safitri, C., & Fasa, M. I. (2024). Strategi Digital Marketing Dalam Meningkatkan Aksesibilitas Layanan Bank Syariah Di Era 4.0. *JICN: Jurnal Intelek Dan Cendikiawan Nusantara*, *1(5)*(November), 7096–7110. https://jicnusantara.com/index.php/jicn

Saputri, M., & Sihotang, M. K. (2023). Pengaruh pembiayaan dan pendampingan usaha terhadap kesejahteraan nasabah pada bank wakaf mikro pesantren mawaridussalam. *Al Urwatul Wutsqa: Kajian Pendidikan Islam*, *6*(November), 530–541. https://journal.unismuh.ac.id/index.php/alurwatul/article/viewFile/7757/4690

Subhaktiyasa Gede Putu. (2024). Evaluasi Validitas dan Reliabilitas Instrumen PenelitianKuantitatif: Sebuah Studi Pustaka. *Journal of Education Research*, *5*(4), 5599–5609.