Multidisciplinary Output Research For Actual and International Issue (MORFAI Journal) ISSN (e): 2808-6635
Volumes 5 No. 5 (2025)

ANALYSIS OF THE INFLUENCE OF THE PRINCIPLE OF CAUTION, TRANSACTION LITERACY, AND TECHNOLOGY LITERACY ON SOCIAL ENGINEERING PREVENTION IN FRAUD MODE IN THE NAME OF BANK BRI

Nina Amanda[1]*,Andri Soemitra [2], Isnaini Harahap[3]
Faculty of Islamic Economics and Business, Universitas Negeri Islam Sumatera Utara, Indonesia[1,2,3]
Corresponding E-mail: ninaamandaa28@gmail.com [1*], andrisoemitra@uinsu.ac.id [2], isnaini.harahap@uinsu.ac.id [3]

Received	: 21 April 2025	Published	: 29 June 2025
Revised	: 30 April 2025	DOI	: https://doi.org/10.54443/morfai.v5i5.3365
Accepted	: 28 May 2025	Link Publish	: https://radjapublika.com/index.php/MORFAI/article/view/3365

Abstract

Fraud using social engineering tactics impersonating Bank BRI continues to rise, targeting individuals with low transaction and technology literacy and who tend to neglect the principle of caution. This situation raises questions about the effectiveness of the principles of caution, transaction literacy, and technology literacy in efforts to prevent such fraud. This research aims to analyze the impact of the application of the principle of caution, transaction literacy, and technology literacy on preventing social engineering in fraudulent schemes impersonating Bank BRI, using an Islamic economic perspective. The study employs a quantitative method with a survey approach. The population in this study consists of Bank BRI customers in the city of Medan. The results of this study indicate that the principle of caution does not have a significant effect on preventing social engineering, while transaction literacy has a significant effect on preventing social engineering. and technology literacy also plays an important role in preventing social engineering.

Keywords: ***Precautionary Principles; Transaction Literacy; Technology Literacy; Social Engineering; BRI Bank***

INTRODUCTION

In the increasingly advanced digital era, the use of technology in the banking sector has seen a significant rise. This advancement provides various conveniences for customers in conducting financial transactions, such as fund transfers, bill payments, and various other banking services. However, behind these conveniences, there are security risks that must be watched out for, especially related to fraudulent schemes impersonating financial institutions like Bank BRI. One of the prevalent fraudulent schemes is social engineering. Social engineering is a method of psychological manipulation used by fraudsters to obtain sensitive information from victims, such as personal data or financial information, by pretending to be a trusted entity, like a bank. This type of fraud not only causes financial losses for customers but also damages the reputation of the financial institution that is used as a facade by the scammers. Social engineering cases can involve individuals from various age groups. In his presentation, Wani Sabu explained that millennial mothers aged 21-35 are a group that often becomes victims of social engineering. However, the success of social engineering efforts often depends on the level of technological literacy and the level of vigilance of potential victims. Therefore, it is important for all age groups to enhance their technological literacy and information security to protect themselves from potential threats.

The principle of prudence (prudent banking principle) is a rule or principle stating that banks, in carrying out their functions and business activities, must be prudent in order to protect the funds of the public entrusted to them, including in the allocation of funds derived from those collected funds. The principle of prudence in banking institutions is a principle that must be strictly adhered to by banking institutions. The provisions of Article 2 of Law Number 10 of 1998 concerning Banking state that the Indonesian banking system operates based on economic democracy while utilizing the principle of prudence. This indicates that the principle of prudence is one of the most important principles that must be implemented or carried out by banks in conducting their business activities. The implementation of the principle of prudence in all banking activities is one way to create a healthy banking environment. Therefore, the purpose of enforcing the principle of prudence is to ensure that banks are always in a healthy state. In other words, to always be in a liquid and solvent condition. The enforcement of the principle of

prudence is expected to keep the public's trust in banking high, so that people are willing and do not hesitate to deposit their funds in banks.

According to the provisions in OJK, financial literacy is defined as a series of activities aimed at acquiring and enhancing knowledge, skills, and confidence of users, customers, and people in general, so that they will be able to manage their finances more effectively and optimally. Furthermore, according to OJK, providing explanations and illustrations about the vision of financial literacy is an effort to create an Indonesian society with a high and good level of financial literacy so that people can choose, utilize, and use financial products and services to achieve and enhance their welfare. Meanwhile, the mission of financial literacy is to carry out education in the financial sector for the Indonesian society to manage finances smartly, improve access to information, and the use of financial products and services by developing infrastructure that supports financial literacy.

Quoting data from Oxford University, Wani mentioned that worldwide, 88 percent of banking cases in the digital era are social engineering. 'What about in Indonesia? It turns out that in Indonesia, 99 percent are social engineering,' he revealed. Often, social engineering fraudsters pretend to be from the bank to request the One Time Password (OTP). If the OTP code is provided, the scammer can access the victim's personal data. To address this issue, there are several approaches that can be taken. One of them is the application of the prudence principle in transactions. This principle emphasizes the importance of caution and vigilance in every financial activity, including maintaining the confidentiality of personal data and not easily trusting parties claiming to represent the bank without clear verification. In addition, transaction literacy and technology literacy also play an important role in preventing social engineering. Transaction literacy involves a good understanding of the procedures and security involved in conducting financial transactions, while technology literacy refers to individuals' ability to understand and use technology safely. Both of these literacies can enhance customers' awareness of fraud risks and ways to avoid them.

Financial literacy is the understanding of financial concepts aimed at achieving financial well-being. It highlights the importance of preparation in facing globalization, especially in the financial context. According to Hilgert and Holgart, knowledge about financial management and investment strategies has become increasingly important in today's globalization era. It can be concluded that the aspects of financial literacy according to OJK are that knowledge, skills, and confidence form a solid foundation for individuals in effectively managing their finances. By having adequate knowledge about various aspects of finance, skills in implementing that knowledge in decision-making, and confidence in their financial management, individuals can become more skilled and confident in managing their personal finances effectively.

From the perspective of sharia economics, the principles of prudence, transaction literacy, and technology literacy are also in line with sharia values that emphasize justice, honesty, and protection of individual rights. Sharia economics regulates not only financial aspects but also prioritizes ethics and morals in every economic activity, including in preventing fraudulent actions that can be harmful. Therefore, this research aims to analyze the impact of the application of the principles of prudence, transaction literacy, and technology literacy on the prevention of social engineering in fraud schemes impersonating Bank BRI, using the perspective of sharia economics. It is hoped that the results of this research can contribute to improving the security of banking transactions and provide guidance for customers and financial institutions in avoiding increasingly sophisticated fraud schemes.

Research discussing Fraud Modus impersonating BRI Bank has been widely presented by previous researchers. Firstly, Kevin Tjendrawinata, et al. (2022). The title of the research: 'Social Engineering: Crisis In Humanity'. The research results indicate that Social Engineering is a technique of attack through social mechanisms or human interactions (persuasion, influence, and other interactions), aimed at controlling the actions of the victim, either consciously or unconsciously. Due to the nature of Social Engineering cases being the negligence of users, not all companies have compensation policies for losses. On the other hand, users/consumers feel disadvantaged due to the 'gaps' that can be exploited by fraudsters.

Secondly, Claudinar Tasya Salsabi, San Rudiyanto, (2024). Research title: "Implementation of Prevention and Resolution of Social Engineering Customer Service at Bank BRI ITN II Malang Unit." The research findings indicate that social engineering crimes pose a significant threat to banking businesses as they can lead to financial, reputational, and legal losses for both the bank and its customers through physical and psychological attacks. To prevent the impacts of social engineering on banking businesses, it is necessary to take anticipatory steps such as preventing password leaks, securing information access, verifying contacts, following procedures, reporting suspicious actions, managing emotions, providing ongoing training, and educating customers.

Third, Suherman, S. (2017). The title of the research is "The Effectiveness of Information Security in Facing Social Engineering Threats." The research findings indicate that through the proper implementation of Standard Operating Procedures, a sense of ownership, the use of official letters for requests, and sending emails to all employees regarding information security on a regular basis, the company can avoid social engineering threats. Thus, the effectiveness of information security in facing the dangers of social engineering can be realized. Banking information security can be well maintained both nationally and internationally.

The difference between my research and previous researchers is that this study combines three important elements, namely the principle of caution, transaction literacy, and technology literacy to provide a comprehensive analysis of social engineering prevention. Previous research tended to focus only on one or two elements. Additionally, this study uses an Islamic economic perspective that emphasizes ethical and moral values in banking transactions. This provides a more holistic framework compared to research that only uses a conventional perspective. Therefore, it is important to conduct an in-depth analysis of how these three factors affect an individual's ability to prevent and combat fraud impersonating Bank BRI. This understanding will help in formulating better strategies to protect the public and strengthen the banking security system in Indonesia.

LITERATURE REVIEW

I. Prudence Principle

The principle of prudence, also known as the 'prudence principle,' is one of the fundamental principles in banking, especially in Islamic banking. This principle aims to ensure that every transaction is conducted with caution and considers all potential risks that may arise. According to Hidayat (2020), the application of the prudence principle in Islamic banking not only protects the bank from financial risks but also maintains customer trust. This principle encompasses various aspects such as risk assessment, internal audits, and compliance with Islamic regulations.

In the context of Islamic economics, the principle of caution is emphasized through the application of Sharia rules that prohibit all forms of uncertainty (gharar) and deception (tadlis) in transactions. Related research indicates that the effective application of this principle can significantly reduce the level of fraud and enhance customer transaction security (Zaki, 2020). Fraud under the guise of banks (phishing and social engineering) is one form of threat that tests the application of the principle of caution in banking. Bank BRI, as one of the largest banks in Indonesia, often becomes a target of this fraud. Therefore, strengthening the principle of caution through customer education and internal supervision is key to mitigating this risk.

The following are the indicators of the Precautionary Principle according to Lilis Ekayani and Hardianto Djanggih 2023, namely:

1. The vulnerability of data theft crime, which is a condition that allows illegal access to data due to security weaknesses, lack of caution, and technological advancements that are not matched by adequate protection.
2. The communication media used can be in the form of traditional media, such as letters and telephones, as well as digital media, such as email, social media, and instant messaging applications, all of which play an important role in facilitating modern communication.
3. Clarity of Product and Service Information, namely the bank has the responsibility to provide complete information to customers regarding the products and services offered, complaint procedures, and the importance of protecting personal data.
4. Trust in Banking, namely that phishing crimes are not caused by the misuse of customers' personal data done without the bank's permission and respondents trust in the banking system that stores their personal data.
5. A Good Banking Security System, that the security system of Bank Rakyat Indonesia is not good yet, and some assess it as good even though improvements still need to be made to the security system.
6. Knowledge Factor, this factor is important because if there is a lack of understanding and knowledge among the public about the types of cybercrime, there will be more victims of such crimes.

II. Transaction Literacy

Transaction literacy refers to the understanding and ability of customers to conduct banking transactions safely and efficiently. This literacy includes knowledge about transaction procedures, risk identification, and fraud prevention measures. Rahmawati (2019) in her research found that good transaction literacy can enhance customer

awareness against fraud schemes, including understanding safe transaction procedures, types of digital fraud, and actions that need to be taken in response to signs of social engineering fraud.

Research by Fatimah (2021) states that a high level of transaction literacy is associated with a decrease in fraud cases in banking transactions. In the context of social engineering, customers with good transaction literacy are more able to recognize manipulation attempts by unauthorized parties, thus avoiding financial losses. Therefore, improving the transaction literacy of BRI Bank customers is an important effort in fraud prevention.

The following are the Transaction Literacy indicators according to Mitchell, Lusardi, and Arif:

1. Basic Financial Knowledge, Knowledge about finance includes personal financial knowledge, which is how to manage income and expenses, as well as understanding basic financial concepts.
2. Capability, capability can be defined as when a person has a high level of literacy, they are able to make good financial decisions.
3. Attitude, in personal financial management, attitude means the ability to know cash sources, pay obligations, knowledge about opening accounts at sharia financial institutions, applying for financing, and making personal financial plans for the future.
4. Confidence, not everyone is able to increase self-confidence when planning for long-term needs.

III. Technology Literacy

Technology literacy has become an important component in the era of banking digitalization. Customers are required to have a good understanding of the technology used in banking services, such as mobile banking and internet banking. In the context of preventing social engineering, technology literacy refers to the ability of customers to understand and use technology safely. This includes knowledge about the importance of two-factor authentication, the utilization of encryption, and the avoidance of fake websites and applications.

In the context of banking, technology literacy includes understanding cybersecurity, using digital banking applications, and identifying signs of online fraud. Susilo (2021) found that strategies to enhance technology literacy can significantly reduce the risk of banking fraud in the digital era. Kurniawan (2020) emphasizes the importance of implementing advanced technologies such as automated fraud detection systems and multi-factor authentication in preventing banking fraud. However, this study does not highlight the role of customer technology literacy in fraud prevention.

Here are the indicators of Technology Literacy according to the Ministry of Communication and Informatics (2021), namely:

1. Digital literacy, the ability of society to know, understand, and utilize ICT hardware and software, and the use of digital operating systems in daily life.
2. Digital Ethics, the ability of society to provide examples, be aware, make self-adjustments, rationalize, make considerations, and develop digital ethics governance in everyday life.
3. Digital Security, the ability of every individual to recognize, model, apply, analyze, consider, and enhance awareness of digital security and personal data protection in everyday life.
4. Digital Culture, the ability of every individual to read, habituate, decode, examine, and build national insights, the values of Pancasila and Bhinneka Tunggal Ika in everyday life, as well as the digitalization of culture by utilizing ICT.

IV. Prevention of Social Engineering

Social engineering is a psychological manipulation technique used by criminals to obtain confidential information from victims. Fraud that employs this modus operandi often takes advantage of customers' trust in banking institutions by pretending to be legitimate bank representatives, as in cases impersonating Bank BRI. Putri's (2018) research identifies various social engineering techniques used in banking fraud, such as phishing, pretexting, and baiting. Educating customers about these techniques is crucial to raise awareness and prevent fraud. Wardhana (2017) highlights that financial literacy education can help customers recognize the signs of social engineering fraud. However, this study does not examine in depth the role of technology literacy and the principle of caution in this context.

In the perspective of Islamic economics, such crimes not only violate positive law but also breach the principles of Sharia that emphasize honesty, transparency, and the prohibition against all forms of deception. Social engineering poses a serious threat to Islamic banking because its impacts are not only financial but also damaging to the reputation and trust of customers in Islamic financial institutions.

The following are the indicators of Social Engineering Prevention according to Tri Hastuti, Yusa Djuyandi, and Wawan Budi Darmawan 2021, which are:

1. Reciprocation, a situation or relationship in which two people or groups agree to do something similar for each other, to allow each other to have equal rights, etc.
2. Consistency, being consistent is behavior that is steady and unchanged. The way to be consistent is to do what should be done, such as being obedient and compliant with regulations or procedures.
3. Social Validation, the purpose of validation is to demonstrate that the system of a procedure remains in accordance with its specifications and that the system meets expectations.
4. Liking, preferences in general can be described in various forms including: fondness, respect, friendship, and trust related to their curiosity about something/material in Social Engineering.
5. Authority, authority is a power held by an individual or group to exercise that power according to the authority granted, and the authority should not be exercised beyond the power obtained.
6. Scarcity in social engineering is a technique used to make the victim feel that they must complete an action within a short period of time.

V. Prevention of Fraud in the Perspective of Sharia Economic

In Islamic economics, fraud prevention is part of the obligation to conduct transactions that align with the principles of justice and honesty. The principle of maqasid shari'ah, which aims to protect property (hifz al-mal), is highly relevant in this context. Islamic banks are expected not only to provide safe and transparent services but also to protect customers from crimes that could financially harm them. Islamic economics emphasizes ethical and moral principles in financial transactions, such as justice, transparency, and compliance with shari'ah law. Hidayat (2020) in his research shows that the implementation of shari'ah principles in banking can enhance customer trust and reduce the risk of fraud. Islamic economics also prioritizes social responsibility and protection of customer rights.

In the context of Islamic economics, the prevention of fraud through social engineering must also pay attention to sharia values such as:

1. Justice (al-'adl): The transaction process must be fair and not harm any party, including banks and customers.
2. Transparency (ash-shidq): Every transaction must be transparent, without any lies or manipulation that could lead to fraud.
3. Trustworthiness: The banking parties must maintain customer trust by protecting data and confidential information from abuse.
4. Social responsibility (maslahah): The banking system must ensure the protection of social interests, by educating customers and the community about the dangers of fraud and prevention efforts.

These principles affirm that deceit, no matter how small, has adverse consequences both in this world and the hereafter. Research in Islamic economics also shows that Islamic principles can be applied to reduce banking fraud through strengthening business ethics and consumer protection.

Quranic verse:
Allah forbids all forms of deception in His words:

وَلَا تَأْكُلُوٓا۟ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ وَتُدْلُوا۟ بِهَآ إِلَى ٱلْحُكَّامِ لِتَأْكُلُوا۟ فَرِيقًا مِّنْ أَمْوَٰلِ ٱلنَّاسِ بِٱلْإِثْمِ وَأَنتُمْ تَعْلَمُونَ ﴿١٨٨﴾

"And do not consume one another's wealth unjustly or send it [in bribery] to the rulers in order that [they might aid] you [to] consume a portion of the wealth of the people in sin, while you know [it is unlawful]." (Quran, Al-Baqarah: 188).
This verse explains that taking the wealth of others through illegitimate means, including fraud, is a prohibited action in Islam.
Hadits:
The Prophet Muhammad (peace be upon him) also warned his followers about the dangers of deception in transactions: The Prophet said: 'Whoever deceives us is not one of us' (Hadith narrated by Muslim, Ibn Majah, and Ahmad).

The Prophet also issued a warning for those who are oppressive with his saying: 'Oppression will turn into darkness on the Day of Judgment' (Hadith narrated by Bukhari and Muslim).

METHOD

This study uses a quantitative method with a survey approach. According to Sugiyono (2020), quantitative research is a research method based on the philosophy of positivism, used to examine a specific population or sample and collect data using research tools, analyze quantitative or statistical data with the aim of testing hypotheses.

The population in this study is customers of Bank BRI who have experienced or are aware of social engineering fraud schemes in Medan City. In this research, the researcher distributed questionnaires online via Google Forms to all Bank BRI customers in Medan City. The use of this online questionnaire aims to be more efficient and effective in collecting the required data.

Since the population in this study cannot be precisely determined, the researcher employed sample measurement using the Lemeshow formula, which can be used to calculate the sample size when the total population cannot be accurately known (Rofiudin et al., 2022):

$$n = \frac{Z^2 .\ P\ .\ (1 - P)}{d^2}$$

$$n = \frac{1{,}96^2 .\ 0{,}5\ (1 - 0{,}5)}{0{,}1^2}$$

$$n = \frac{3{,}8416\ .\ 0{,}5\ .\ 0{,}5}{0{,}1^2}$$

$$n = \frac{0{,}9604}{0{,}1^2}$$

$$n = 96{,}04 = 97$$

Explanation:
n = Sample size
Z = Z score at 95% confidence = 1.96
P = Maximum estimate = 50% = 0.5
d = Error margin = 10% = 0.1

Based on the calculations above, the result of the data is 96.4, which is a fraction, and according to (Sugiyono, 2017). Calculations that yield a fraction (with a decimal) should be rounded so that the total in this study is 100 respondents. This study uses a non-probability sampling technique where the research does not provide the same or equal opportunity for every member of the population to be selected as a sample.

RESULTS AND DISCUSSION

A. Characteristics of Respondents

The characteristics of the respondents aim to provide a clear picture of the profile of respondents involved in this research. By explaining the characteristics of the respondents who are samples, we can understand the extent to which their profiles are relevant and contribute to the results of this research. The elaboration of the respondents' identities allows researchers to identify the relationship between the respondents' backgrounds and the research findings, thereby providing a deeper context for the analysis conducted.

Table 1 | Characteristics of Respondents

No.	Description	Total	Percentage

1.	Age - Under 20 Years - 20-30 Years - 31-40 Years - Over 40 Years	 4 79 13 4	 4% 79% 13% 4%
2.	Gender - Female - Male	 59 43	 59% 43%
3.	Work - Students - Housewife - CEO/CFO/Businessperson - Civil Servants - Others	 57 3 11 9 20	 57% 3% 11% 9% 20%
4.	Experience Using Banking Services (Year) - Under 1 Years - 1-5 Years - Over 5 Years	 20 53 27	 20% 53% 27%

Source: 2024 Research Questionnaire

From the data, it can be seen that the demographic distribution of respondents is detailed in four main categories, which include age, gender, occupation, and experience in using banking services, providing an in-depth view of the backgrounds of the subjects involved.

Age: The age composition of respondents is predominantly in the 20-30 year group, with a proportion reaching 79%, indicating that the younger generation is more involved in this study. Meanwhile, the age groups below 20 years and above 40 years are both only represented by 4% of the total respondents, showing minimal participation from both age groups. The age group of 31-40 years has a better representation at 13%, but still significantly lower compared to the dominant age group.

Gender: The majority of respondents in this survey are female, with a percentage of 59%, while male participation is at 43%. This disparity may reflect differing tendencies or habits of participation in surveys between genders or perhaps survey subjects that are more relevant or interesting to women.

Occupation: Most respondents are students, accounting for about 57% of the total sample, consistent with the dominance of the younger age group. A small number of respondents come from professional backgrounds such as CEOs/CFOs/Businesspersons, making up 11%, and Civil Servants (PNS) at 9%. Housewives represent only 3% of the sample, while the remaining 20% fall under the 'Other' category, indicating a variety of occupations that are not explicitly categorized.

Banking Service Experience: Respondents' experiences using banking services are divided into three groups; 20% have less than one year of experience, indicating a new involvement in banking services. Respondents with experience between 1 to 5 years constitute the largest group, covering 53%, while 27% of respondents have more than 5 years of experience, indicating a significant depth of banking experience among some participants.

A. Validity and Reliability Test

To test the validity and reliability, the author used analysis with the SPSS 26 computer application, the following are the results of the tests:

1. Validity Test

According to Sugiyono (2018: 455), the validity test is the degree of accuracy between the actual data occurring in the object that can be reported by the researcher. Testing validity means examining the extent of the consistency or truth of an instrument as a measuring tool for research variables. If the instrument is correct (valid), then the measurement results are likely to be true.

Table 2 | Results of Validity Test

Variable	Question Item	Rcount	Rtable	Explanation
Precautionary Principle (X1)	X1.1	0,802	0,197	Valid
	X1.2	0,734	0,197	Valid
	X1.3	0,603	0,197	Valid
	X1.4	0,663	0,197	Valid
	X1.5	0,612	0,197	Valid
	X1.6	0,764	0,197	Valid
	X1.7	0,667	0,197	Valid
Transaction Literacy (X2)	X2.1	0,749	0,197	Valid
	X2.2	0,813	0,197	Valid
	X2.3	0,792	0,197	Valid
	X2.4	0,796	0,197	Valid
	X2.5	0,841	0,197	Valid
	X2.6	0,819	0,197	Valid
	X2.7	0,778	0,197	Valid
Technology Literacy (X3)	X3.1	0,857	0,197	Valid
	X3.2	0,806	0,197	Valid
	X3.3	0,848	0,197	Valid
	X3.4	0,871	0,197	Valid
	X3.5	0,855	0,197	Valid
	X3.6	0,802	0,197	Valid
	X3.7	0,884	0,197	Valid

Based on the table above, the correlation values (Pearson Correlation) in the Rhitung column obtained for each statement have Rhitung > Rtabel, so it can be said that all statements for the variables of Precautionary Principle, Transaction Literacy, Technology Literacy, and Social Engineering Prevention are valid.

Tabel 3 | Test Data Validity (Y)

Variable	Question Item	Rcount	Rtable	Explanation
Prevention of Social Engineering (Y)	Y.1	0,818	0,197	Valid
	Y.2	0,831	0,197	Valid
	Y.3	0,828	0,197	Valid
	Y.4	0,849	0,197	Valid
	Y.5	0,823	0,197	Valid
	Y.6	0,589	0,197	Valid
	Y.7	0,701	0,197	Valid

Based on the table above, the correlation value (Pearson Correlation) in the Rhitung column obtained for each statement shows that Rhitung > Rtabel, so it can be said that all statements for the Social Engineering Prevention variable are valid.

2. Reliability Test

Table 4 | Reliability Test

Variable	Cronbach's Alpha	Syarat Cronbach's alpha	Result

Precautionary	0,808	0,6	Reliabel
PrinciplesTransaction	0,904	0,6	Reliabel
LiteracyTechnology	0,933	0,6	Reliabel
SocialEngineering Prevention	0,892	0,6	Reliabel

Source: Primary data processed by SPSS 26

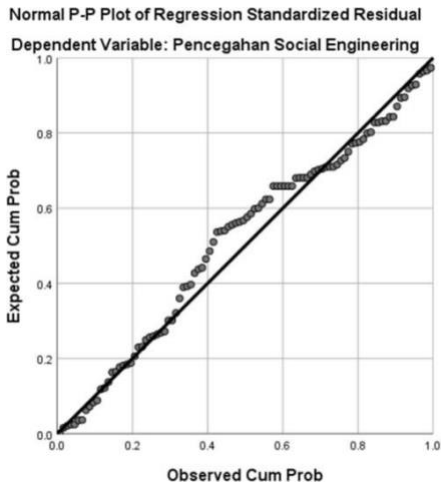
Table 4 shows that the variable of the Precautionary Principle has a Cronbach's alpha value of 0.808, the Transaction Literacy variable has a Cronbach's alpha value of 0.904, the Technology Literacy variable has a Cronbach's alpha value of 0.933, and the Social Prevention variable has a Cronbach's alpha value of 0.892. They are reliable and suitable to be used as research data.

B. B. Classical Assumption Testing

1. Normality Test

Normality test is conducted to determine whether the sample data is taken from a normally distributed population. This test is generally performed to verify whether the data involved in the research has a normal distribution.

Pictures 1 | P-P Normality Test Plot



Source: Data SPSS 26, 2024

Based on the data visualization, it is clear that the data plot forms a straight line pattern moving from the lower left to the upper right. This indicates that the linearity assumption in the regression model has been met. Good linearity shows a consistent relationship between the independent and dependent variables, allowing the results of the regression analysis to provide valid and accurate interpretations. Meeting this assumption is crucial in ensuring the reliability of predictions and the conclusions drawn by the model.

2. Multicollinearity Test

Table 5 | Multicollinearity Test

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.	Collinearity Statistics Tolerance	Collinearity Statistics VIF
1	(Constant)	.059	1.652		.036	.972		
	Precautionary Principle	.137	.083	.123	1.655	.101	.428	2.337
	Transaction Literacy	.420	.100	.443	4.204	.000	.214	4.684
	Technology Literacy	.325	.094	.365	3.479	.001	.216	4.638

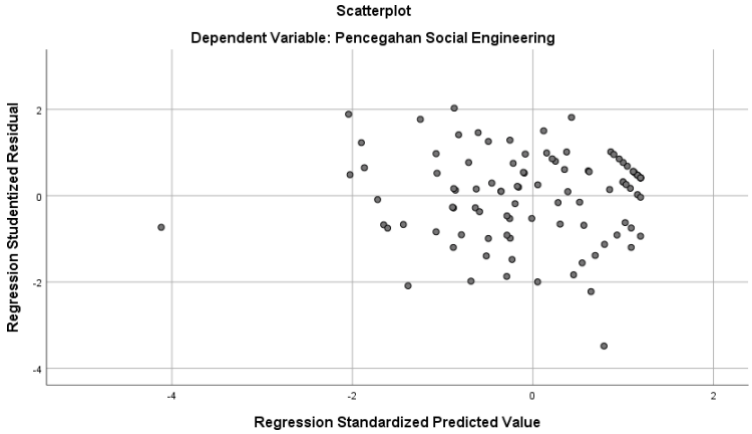
a. Dependent Variable: Prevention of Social Engineering

Based on the table of multicollinearity test results above, it can be seen that the variable of the Precautionary Principle has a Tolerance value of 0.428 > 0.1 and a VIF value of 2.337 < 10, the transaction literacy variable has a Tolerance value of 0.214 > 0.1 and a VIF value of 4.684 < 10, and the technology literacy variable has a Tolerance value of 0.216 > 0.1 and a VIF value of 4.638 < 10. Therefore, it can be concluded that there is no multicollinearity in this study.

3. Heteroscedasticity Test

Heteroscedasticity testing is conducted on regression models to test whether there is a disparity in the variance of residuals from one observation to another (Juliandi et al., 2014). Heteroscedasticity tests are conducted to examine whether there is a disparity in variance or residuals between one observation and another. Heteroscedasticity tests are performed to determine whether there is a discomfort of variance of the residuals in one observation compared to another in a regression model.

Pictures 2 | Heteroscedasticity Test



Source: Data SPSS 26, 2024

From the scatterplot above, it can be seen that the data points are randomly scattered around the number 0, both above and below the horizontal axis. There is no pattern indicating that the data is spreading wider or narrower, nor is there a specific wave pattern formed. Therefore, it can be concluded that this model does not experience heteroscedasticity problems. Meeting this requirement is very important in multiple linear regression, because the absence of heteroscedasticity indicates that the residual variance is constant, making the regression results more reliable and its interpretation more valid.

C. Analysis of Multiple Linear Regression

Multiple linear regression analysis is conducted with the aim of determining the extent of the influence of independent variables on the dependent variable. The multiple regression analysis in this study was performed using SPSS 26. The results of the multiple regression analysis regarding the Influence of the Application of the Precautionary Principle, Transaction Literacy, and Technology Literacy on the Prevention of Social Engineering in scams purporting to be from Bank BRI.

Coefficients[a]					
	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
Model	B	Std. Error	Beta		

1	(Constant)	.059	1.652		.036	.972
	Precautionary Principle	.137	.083	.123	1.655	.101
	Transaction Literacy	.420	.100	.443	4.204	.000
	Technology Literacy	.325	.094	.365	3.479	.001

a. Dependent Variable: Prevention of Social Engineering

Thus, the regression results above can be organized into the following regression equation:

$Y = \alpha + \beta1X1 + \beta2X2 + \beta3X3 + e$

$Y = 0{,}059 + 0{,}137X1 + 0{,}420X2 + 0{,}325X3$

The multiple regression equation above means:

1. The constant value of 0.059 represents the state when the Social Engineering Prevention variable is not influenced by the principles of caution, transaction literacy, and technology literacy. This means that if these independent variables have no influence, the Social Engineering Prevention variable does not change, with a score of 0.059.
2. The regression coefficient value of the Principle of Caution (X1) is 0.137, indicating that the principle of caution variable has a positive effect on Social Engineering Prevention, meaning that for each increase of 1 unit in the principle of caution variable, Social Engineering Prevention will increase by 0.137 units, assuming that other variables remain constant.
3. The value of the regression coefficient for transaction literacy (X2) is 0.420, indicating that the variable of transaction literacy has a positive effect on Social Engineering Prevention, meaning that for every increase of 1 unit in the transaction literacy variable, it will increase Social Engineering Prevention by 0.420 units, assuming that other variables remain constant.
4. The value of the regression coefficient for technology literacy (X3) is 0.325, indicating that the variable of technology literacy has a positive effect on Social Engineering Prevention, meaning that for every increase of 1 unit in the technology literacy variable, it will increase Social Engineering Prevention by 0.325 units, assuming that other variables remain constant.

Partial Test (Uji t)

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	T	Sig.
1	(Constant)	.059	1.652		.036	.972
	Precautionary Principle	.137	.083	.123	1.655	.101
	Transaction Literacy	.420	.100	.443	4.204	.000
	Technology Literacy	.325	.094	.365	3.479	.001

a. Dependent Variable: Prevention of Social Engineering

Based on the analysis results above, the following explanations can be obtained:

1. The Carefulness Principle variable obtained a t-count value of 1.655 and a significance value of 0.101, which is greater than 0.05 ($p > 0.05$), thus it can be concluded that the carelessness principle does not influence Social Engineering Prevention.
2. The Transaction Literacy variable obtained a t-count value of 4.204 and a significance value of 0.000, which is less than 0.05 ($p < 0.05$), thus it can be concluded that transaction literacy has a significant effect on Social Engineering Prevention.
3. The Technology Literacy variable obtained a t-count value of 3.479 and a significance value of 0.001, which is less than 0.05 ($p < 0.05$), thus it can be concluded that technology literacy has a significant effect on Social Engineering Prevention.

Uji F (Simultaneous Test)

ANOVA[a]

Model	Sum of Squares	df	Mean Square	F	Sig.

1	Regression	1648.181	3	549.394	108.751	.000[b]
	Residual	484.979	96	5.052		
	Total	2133.160	99			

a. Dependent Variable: Prevention of Social Engineering
b. Predictors: (Constant), Technology Literacy, Precautionary Principle, Transaction Literacy

Based on the results of the simultaneous test above, it can be concluded that the calculated F value obtained is 108.751 and the significance value obtained is 0.000 < 0.05 (p < 0.05), thus it can be concluded that the principle of caution, transaction literacy, and technology literacy together have a significant effect on Social Engineering Prevention.

Uji Koefisien Determinasi (R2)

The coefficient of determination (R2) test is conducted to see how well the model explains the variation of the dependent variable. The value of the coefficient of determination ranges from 0 to 1.

The calculated value of the coefficient of determination can be seen below.

Model Mmary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.879[a]	.773	.766	2.248

a. Predictors: (Constant),), Technology Literacy, Precautionary Principle, Transaction Literacy

Based on the data, a coefficient of determination or R-Square (R2) value of 0.773 was obtained, which means that the contribution of the variables of the precautionary principle, transaction literacy, and technology literacy to the Prevention of Social Engineering is 77.3%. The remaining variation of 22.7% in the Prevention of Social Engineering is influenced by other variables that were not included in this study.

Discussion

A. The Influence of the Precautionary Principle on the Prevention of Social Engineering

In the analysis of the variable of the Precautionary Principle against the prevention of Social Engineering, a calculated t value of 1.655 was obtained with a significance value of 0.101. Since this significance value is greater than 0.05 (p > 0.05), it can be concluded that the Precautionary Principle does not have a significant effect on the prevention of Social Engineering. This result indicates that although the Precautionary Principle is an important concept in maintaining information security, its application in the context of preventing Social Engineering-based fraud has not yet provided optimal impact. One of the main reasons is the lack of understanding and awareness among customers regarding the importance of consistently applying security principles.

For example, in statement item X1.6, which inquires about understanding the risks of cybercrime such as phishing and social engineering, the low average response score indicates that many customers do not yet understand the risks associated with these crimes. In other words, although the bank has provided security guidelines, there remains a gap in customers' understanding of the application of the precautionary principle in daily activities. This underscores the need for more effective education from banks to raise customer awareness about the importance of maintaining personal information security to avoid the threats of Social Engineering fraud.

Unlike the results obtained in the study conducted by Saputra, R., & Wijaya, L. (2018), this research reveals that the principle of caution does not have a significant and negative impact on the prevention of social engineering.

B. The Influence of Transaction Literacy on the Prevention of Social Engineering

In the analysis of the Transaction Literacy variable against the prevention of Social Engineering, a t-value of 4.204 was obtained with a significance value of 0.000. Since this significance value is much smaller than 0.05 ($p < 0.05$), it can be concluded that Transaction Literacy has a significant influence on the prevention of Social Engineering. This result indicates that the higher the transaction literacy possessed by customers, the greater their ability to recognize and avoid various forms of Social Engineering-based fraud. Transaction literacy includes customers' understanding of how to transact securely, the ability to identify suspicious transactions, and vigilance against fraud patterns.

In item statement X2.5, which asks whether customers are able to recognize signs of suspicious transactions or potential fraud, a strong response from customers indicates that good knowledge in financial transactions plays an important role in protecting them from fraud threats. Customers with good transaction literacy are more likely to understand the existing risks and be more vigilant against manipulation attempts by irresponsible parties.

Thus, these results emphasize the importance of improving Transaction Literacy among customers as a strategic step in preventing Social Engineering. Banks and financial institutions need to continuously provide comprehensive education to customers about the importance of understanding the correct transaction procedures and recognizing signs of fraud, in order to minimize risks that could harm customers. In line with the research of Rahman, F., & Suharto, B. (2021), this study shows that Transaction Literacy has a significant and positive effect on the prevention of Social Engineering, as understanding the existing risks will help customers avoid attempts at fraud.

C. The Influence of Technology Literacy on the Prevention of Social Engineering

In the analysis of the Technology Literacy variable against Social Engineering prevention, a t-value of 3.479 was obtained with a significance value of 0.001. Because this significance value is less than 0.05 ($p < 0.05$), it can be concluded that Technology Literacy has a significant effect on Social Engineering Prevention. This result shows that customers' understanding of technology, especially regarding cyber threats and Social Engineering techniques, plays an important role in protecting them from scams that often use digital means. Technology literacy includes customers' ability to recognize threats that arise through technology platforms such as email, banking applications, and social media, as well as an understanding of how to effectively protect personal data.

In the statement item X3.3, which inquires about the importance of maintaining digital security, especially in protecting personal data during online transactions, significant results indicate that customers with good technological literacy are more prepared to face such threats. Knowledge of how to use technology safely, recognize cyber threats, and avoid scams impersonating banks is essential in prevention efforts.

Thus, the results of this study emphasize that the improvement of Technology Literacy is crucial in facing Social Engineering. Customers who are more technologically literate tend to be more vigilant and capable of protecting themselves from various types of digital fraud. Banks need to continue investing in education related to digital security and technology literacy to help customers deal with the evolving complex cyber threats. In line with the research by Putri, D. A., & Ramadhan, F. (2020), this study reveals that Technology Literacy has a significant impact on the Prevention of Social Engineering, as customers who are more knowledgeable about technology, especially cyber threats such as phishing and malware, tend to be more capable of detecting and avoiding social engineering-based fraud attempts.

CONCLUSION

After conducting data analysis, the researcher draws the following conclusions:

1. The Precautionary Principle Does Not Have a Significant Impact
   Based on testing results, the precautionary principle has no significant impact on the prevention of Social Engineering. This is due to the customers' lack of understanding of the importance of following the security guidelines provided by the bank, especially in protecting personal information from fraud threats.
2. Transaction Literacy Has a Significant Impact

Research shows that transaction literacy has a significant impact on the Prevention of Social Engineering. Customers who understand the signs of suspicious transactions and have better awareness of how to transact safely are more capable of protecting themselves from potential fraud.

3. Technology Literacy Has a Significant Impact
   Technology literacy also plays an important role in Preventing Social Engineering. Knowledge about cyber threats and manipulation techniques such as Social Engineering helps customers recognize and avoid scams that claim to be from the bank. This understanding of technology becomes an important tool in protecting customers from various digital threats.

Overall, the results of this study emphasize the importance of enhancing Transaction and Technology Literacy as a preventive step in combating Social Engineering, while the Principle of Caution needs to be reinforced with more in-depth education for customers so that they better understand the importance of safeguarding personal information.

REFERENCES

Arifin, Z. (2018). Penerapan Teknologi Blockchain dalam Mencegah Penipuan Perbankan. Jurnal Teknologi Finansial, 6(2), 270–285.

Aulia, R. (2021). Modus Penipuan Mengatasnamakan Bank: Tantangan dan Solusi. Jurnal Keamanan Siber, 5(2), 150–165.

Fadhila, R. (2019). Implementasi Sistem Keamanan Informasi di Bank untuk Mencegah Social Engineering. Jurnal Sistem Informasi, 14(2), 250–265.

Fatimah, L. (2021). Pengaruh Literasi Transaksi terhadap Pencegahan Penipuan Perbankan".

Firdaus, M. (2018). Peran Edukasi dan Literasi dalam Mencegah Penipuan Perbankan di Indonesia. Jurnal Edukasi Masyarakat, 7(2), 45–60.

Fitriana, L. (2020). Strategi Bank dalam Menghadapi Penipuan melalui Social Engineering. Jurnal Manajemen Risiko Keuangan, 5(4), 330–345.

Hamzah, M. (2017). Pengaruh Literasi Teknologi terhadap Keamanan Transaksi Perbankan di Era Digital. Jurnal Manajemen Teknologi, 12(4), 410–425.

Hanum, F., Jannah, N., & Soemitra, A. (2024). Analysis of the Influence of Price, Service Quality and Customer Experience on Customer Loyalty.

Hasanah, U. (2019). Penerapan Prinsip Hati-hati dalam Transaksi Perbankan Syariah: Tinjauan Literatur. Jurnal Ekonomi dan Hukum Islam, 14(2), 112–128.

Hidayat, T. (2020). Prinsip Hati-hati dalam Transaksi Perbankan Syariah: Studi Kasus Bank Syariah XYZ. Jurnal Ekonomi Syariah, 12(2), 234–250.

Judijanto, L., Fajariana, D. E., Harsono, I., & Sutanto, H. (2024). Eksplorasi Penelitian Etika Bisnis dan Tanggung Jawab Sosial Perusahaan dengan Pendekatan Bibliometrik. Sanskara Manajemen Dan Bisnis, 02.

Kurniawan, A. (2020). Peran Teknologi dalam Pencegahan Penipuan Perbankan: Studi Kasus pada Bank BUMN di Indonesia. Jurnal Teknologi Perbankan, 8(2), 190–205.

Kusuma, D. (2021). Analisis Penggunaan Media Sosial dalam Modus Penipuan Perbankan. Jurnal Media Digital dan Keamanan, 4(1), 110–125.

Laturette, K., Widianingsih, L. P., & Subandi, L. (n.d.). Literasi Keuangan Pada Generasi Z. J. Pendidik. Akunt, 9(1), 131–139.

Lubis, N. S., & Nasution, M. I. P. (2023). Perkembangan Teknologi Informasi dan Dampaknya pada Masyarakat. Kohesi: Jurnal Sains Dan Teknologi, 1(12), 41–50.

Munawaroh. (2018). Penerapan Nilai Islam Pada Bank Syariah dan Pengaruhnya Terhadap Loyalitas Nasabah Masyarakat Medan. Uin, 162.

Muti, S., Hasibuan, A., Soemitra, A., & Nasution, S. A. (2024). Analysis of Socioeconomic and Situational Factors, Winning Probability, and Perception of Convenience on Online Gambling Addiction Among Gen Z.

Nasution, M. I. P. (2008). Urgensi Keamanan pada Sistem Informasi. IQRA': Jurnal Perpustakaan dan Informasi, 2(2), 41–53.

Nurhayati, D. (2018). Pengaruh Literasi Keuangan terhadap Keputusan Keuangan Nasabah di Bank Syari'ah. Jurnal Ekonomi Islam, 10(1), 54–70.

Puspitasari, E. (2019). Analisis Kerentanan Nasabah terhadap Penipuan Social Engineering di Bank Konvensional. Jurnal Kriminologi, 13(2), 75–92.

Putri, L. M. (2018). Analisis Social Engineering dalam Modus Penipuan Perbankan: Studi pada Nasabah Bank Konvensional di Jakarta. Jurnal Manajemen Risiko, 10(1), 45–60.

Rahmani, N. A. B. (2016). Metode Penelitian Ekonomi. Febi Uinsu Press.

Rahmawati, S. (2019). Pengaruh Literasi Keuangan dan Literasi Teknologi terhadap Pencegahan Penipuan Perbankan di Indonesia. Jurnal Keuangan dan Perbankan, 23(4), 567–580.

Rahmawati, T. (2022). Peran Literasi Teknologi dalam Meningkatkan Keamanan Perbankan Digital". Jurnal Teknologi dan Keuangan.

S., D. A. Y., N., A. I. L., & N, M. L. I. (2023). Pengaruh Kualitas Layanan, Kepercayaan, Dan Kepuasan Terhadap Loyalitas Nasabah : Studi Kasus Bank Sumut Syariah KCP Lubuk Pakam. Journal of Islamic Economics and Finance, 1(4), 153–173.

S., Y. A., & N, M. I. P. (2023). Meningkatkan Literasi Perbankan Syari'ah dengan Mengembangkan Aplikasi Edukasi Berbasis Android. Sci-tech Journal, 2(1).

Sjahdeini, S. R. (1993). Kebebasan Berkontrak dan Perlindungan yang Seimbang Bagi Para Pihak Dalam Perjanjian Kredit Bank di Indonesia, Institut Bankir Indonesia.

Soemitra, A. (2010). Bank dan Lembaga Keuangan Syariah. Kencana Prenada Media Group.

Soemitra, A. (2022). Perlindungan Konsumen terhadap Kebocoran Data pada Jasa Keuangan di Indonesia. Juripol (Jurnal Institusi Politeknik Ganesha Medan, 5(1), 288–303.

Sugiyono. (2014). Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif, dan R&D. Alfabeta.

Susilo, D. (2021). Strategi Peningkatan Literasi Keuangan dalam Mencegah Penipuan Perbankan pada Era Digital. Jurnal Edukasi Keuangan, 15(3), 301–315.

Syahputra, H. (2021). Penerapan Prinsip-Prinsip Syari'ah dalam Pencegahan Penipuan Perbankan. Jurnal Hukum Islam, 9(3), 210–225.

Tambunan, R. T., & Padli Nasution, M. I. (2022). Tantangan dan Strategi Perbankan Dalam Menghadapi Perkembangan Transformasi Digitalisasi di Era 4.0. Sci-Tech Journal, 2(2), 148–156.

Usman, R. (2001). Apsek-aspek Hukum Perbankan di Indonesia. PT.Gramedia Pustaka Utama.

Vionita, C., Sintia, D., & Muhammadiyah Bengkulu, U. (2024). PENTINGNYA ETIKA PROFESI DAN BISNIS DALAM UPAYA KEMAJUAN PERUSAHAAN.

Wardhana, R. (2017). Efektivitas Pendidikan Literasi Keuangan dalam Mencegah Penipuan Perbankan. Jurnal Pendidikan Ekonomi, 11(1), 78–90.

Wijaya, F. (2020). Analisis Pencegahan Penipuan Perbankan melalui Teknologi Keamanan Informasi. Jurnal Teknologi Informasi, 9(3), 340–355.

Yulia, R. A. (2023). Etika Dalam Perusahaan Sebagai Hasil Dari Prinsip Tata Kelola Perusahaan Yang Baik.

Zaki, H. (2020). Prinsip Hati-hati dalam Perbankan Syariah: Sebuah Pendekatan untuk Mengatasi Risiko Penipuan". Jurnal Ekonomi Syariah.