

# The Influence of Financial Literacy on Customers' Ability to Avoid Phishing: A Case Study of Bank Syariah Indonesia Ahmad Yani Bone Branch Office

Edi Darnadi<sup>1</sup>, Muh. Hasbi Ash. Shiddiq<sup>2</sup>, Jumriani<sup>3</sup>

Institut Agama Islam Negeri Bone

Email: edidarnadisq@gmail.com, hasbi.m.as@iain-bone.ac.id, jumrianisafar@gmail.com

This study aims to determine the influence of financial literacy on customers' ability to avoid phishing attacks and the extent to which financial literacy influences customers' ability to avoid phishing attacks at Bank Syariah Indonesia's Ahmad Yani Bone Branch. This study used a quantitative approach, using a questionnaire as the data collection method. The sample consisted of 50 customers of Bank Syariah Indonesia's Ahmad Yani Bone Branch. The data were collected through validity testing, reliability testing, classical assumption testing, and hypothesis testing. The results show that financial literacy has a significant influence on customers' ability to avoid phishing attacks at Bank Syariah Indonesia's Ahmad Yani Bone Branch. This is indicated by the  $R^2$  value of 67.7%. This means that financial literacy is largely influenced by customers' ability to avoid phishing, while the remaining 32.3% is influenced by other factors. Therefore, the higher the financial literacy, the better the customer's ability to protect themselves from digital fraud.

**Keywords:** Financial Literacy, Customer Ability, Phishing Attacks

This is an open access  
article under the [CC BY-NC](#) license



## Corresponding Author:

Edi Darnadi  
Institut Agama Islam Negeri Bone  
edidarnadisq@gmail.com

## 1. Introduction

Knowledge, understanding, and the ability to manage finances independently are essential skills every individual must possess to analyze future financial risks. One way to implement this is through financial literacy. According to the Financial Services Authority (OJK), as cited by Choeruddin (2023), financial literacy is a series of activities to improve people's knowledge, skills, and confidence so they can manage their finances better and more optimally.

The importance of financial literacy is increasing as technological developments drive major transformations in the financial services sector. The presence of digital services such as mobile banking, internet banking, and digital wallets provides easy access for the public, but also presents new risks in the form of cybercrime. Data from the National Cyber and Crypto Agency (BSSN) shows that there were 16,882 cases of phishing emails in 2022. Furthermore, the financial sector is one of the sectors most frequently targeted by cyberattacks through various methods such as social engineering, OTP fraud, SIM swaps, and phishing. Simanjuntak (2023) explained that throughout 2021–2022, the National Agency for the Protection of State-Owned Enterprises (BPKN-RI) received 15 complaints related to phishing, with the main cases being debiting funds without customer consent, loss of funds from accounts, and fraudulent transactions.

This high level of threat is also reflected in data from the Financial Services Authority (OJK) and the Indonesia Anti-Scam Center (IASC). As of May 31, 2025, there were 135,397 reports of fraud in the financial sector, with total losses reaching IDR 2.6 trillion. A total of IDR 163.3 billion in funds were blocked, with 219,166 accounts reported and 49,316 accounts blocked. The most common methods identified included online shopping fraud, financial fraud, fraudulent activities involving impersonation of certain

parties, and investment fraud. Most of these cases involved phishing, a fraudulent technique aimed at obtaining personal data by impersonating a legitimate entity.

According to Yusuf (2022), phishing is the act of tricking someone into unknowingly providing important information through fake emails or websites that mimic official sites. Commonly stolen information includes account passwords, account numbers, and credit card details. Perpetrators use emails, banners, or pop-ups to direct victims to fake websites and exploit users' lack of discernment in recognizing a site's authenticity.

From an Islamic perspective, phishing is a prohibited act because it involves elements of fraud and the unlawful taking of another's property. This is emphasized in verse 188 of the Quran, Surah Al-Baqarah, which prohibits the unlawful taking of another's property. This verse demonstrates that all forms of manipulation and fraud, including digital phishing, contradict the Islamic principles of justice and honesty. The success of phishing is highly dependent on a person's low digital and financial literacy in recognizing the characteristics of suspicious messages or websites. Therefore, the public is urged to increase vigilance and uphold ethics and integrity in digital activities.

Utami et al. (2025) explained that low customer awareness of maintaining personal data confidentiality and a lack of digital financial literacy are the main factors contributing to increased vulnerability to social engineering-based digital crimes, including phishing. They also explained that the widespread use of digital banking services has increased the risk of phishing, while educational programs from banks and the Financial Services Authority (OJK) have not been optimally implemented due to limited human resources, low public interest, and the continued development of new crime methods.

Research by Sri Kusuma Lestari, Aniek Hindrayani, and Khresna Bayu Sangka shows that financial literacy and digital literacy have a positive and significant impact on the awareness of Solo Raya students in dealing with investment fraud. According to Lestari (2025), individuals with high levels of financial literacy tend to be more critical and cautious in making financial decisions because they are able to recognize risks and the characteristics of suspicious offers. Good digital literacy also helps individuals be more careful in accessing and evaluating information, thus preventing them from being easily influenced by financial behavioral biases.

These findings reinforce the importance of improving financial literacy as a preventative measure against social engineering-based crimes such as phishing. Therefore, this study is important to analyze the influence of financial literacy on customers' ability to detect and avoid phishing attacks. By focusing on banking customers who are vulnerable to phishing attacks, this study is expected to contribute to the development of literature on consumer protection and the security of digital financial transactions.

The objectives of this study are as follows: (1) to determine the influence of financial literacy on customers' ability to avoid phishing attacks; and (2) to determine the extent of financial literacy's influence on customers' ability to avoid phishing attacks at Bank Syariah Indonesia Ahmad Yani Bone Branch.

### **Hypothesis**

H0: There is no influence of financial literacy on customers' ability to avoid phishing attacks.

H1: There is an influence of financial literacy on customers' ability to avoid phishing attacks.

## **2. Method**

This study used a primary quantitative method with an associative quantitative approach to analyze the influence of financial literacy on customers' ability to avoid phishing. According to Silalahi (2010), primary quantitative research tests theories through variables measured numerically and analyzed statistically. Sugiyono (2025) explains that an associative approach is used to determine the relationships and influences

between variables. The study was conducted in Bone Regency from January to April 2026. The study population was customers of Bank Syariah Indonesia, Ahmad Yani Branch Office, Bone. According to Yuliardi (2017), a population is a generalized area with certain characteristics to be studied. The sample was determined using a purposive sampling technique with specific criteria and calculated using the Slovin formula, resulting in 50 respondents.

The data used was primary data obtained directly from customers of Bank Syariah Indonesia, Ahmad Yani Branch Office, Bone. Teguh (2001) states that primary data is data obtained from original sources, while Arikunto (2013) explains that the data source is the subject from which the data is obtained. The independent variable in this study is financial literacy (X), while the dependent variable is customers' ability to avoid phishing (Y). Financial literacy refers to the ability to understand and manage financial services (Choeruddin, 2023), while the ability to avoid phishing is the ability to recognize and prevent digital fraud (Tabrani, 2024).

Data collection was conducted through observation and questionnaires. Umar (2014) explains that observation is conducted through direct observation of the research subjects, while Mardalis (2008) states that questionnaires are used to obtain information from respondents through written questions. Assessments used a Likert scale of 1–5, as proposed by Prasetyo (2005). Data analysis was conducted through validity tests, reliability tests, normality tests, heteroscedasticity tests, t-tests, and the coefficient of determination (Adjusted R<sup>2</sup>). According to Ghozali (2013), validity and reliability tests are used to ensure the quality of research instruments, while Kuncoro (2011) explains that Adjusted R<sup>2</sup> is used to measure the influence of independent variables on the dependent variable.

### 3. Results and Discussion

#### Research Results

#### Descriptive Statistical Analysis

#### Financial Literacy (X)

**Table 1.** Financial Literacy Variables

|                     | Descriptive Statistics |         |         |       |                |
|---------------------|------------------------|---------|---------|-------|----------------|
|                     | N                      | Minimum | Maximum | Mean  | Std. Deviation |
| Financial Behavior  | 50                     | 2       | 5       | 4.16  | .766           |
| Demographic Factors | 50                     | 3       | 5       | 4.12  | .895           |
| Education Factors   | 50                     | 2       | 5       | 3.86  | .833           |
| Income Level        | 50                     | 2       | 5       | 3.90  | .863           |
| Total               | 50                     | 13      | 20      | 16.04 | 1.525          |
| Valid N (listwise)  | 50                     |         |         |       |                |

Based on the descriptive analysis, the financial behavior indicator obtained an average score of 4.16 with a standard deviation of 0.766. This value indicates that respondents have good financial behavior in managing, planning, and making financial decisions, and the level of response is relatively uniform. The demographic factor indicator had an average score of 4.12 with a standard deviation of 0.895, indicating that respondents' demographic characteristics contribute to financial literacy levels, although there was greater variation in responses.

The education factor indicator obtained an average score of 3.86 with a standard deviation of 0.833. These results indicate that education influences financial literacy, but some respondents still have suboptimal financial understanding. Meanwhile, the income level indicator had an average score of 3.90 with a standard

deviation of 0.863, indicating that income plays a role in shaping financial literacy, with respondents with higher incomes tending to have better financial understanding and management.

Overall, the financial literacy variable had an average score of 16.04 with a standard deviation of 1.525. This value indicates that the financial literacy level of Bank Syariah Indonesia Ahmad Yani Bone Branch customers is in the good category. Therefore, the majority of respondents have sufficient understanding and skills in managing their finances and understand various aspects of the financial services they use.

### Customer Ability to Avoid Phishing (Y)

**Table 2.** Variable: Customer Ability to Avoid Phishing (Y)

| Descriptive Statistics         |    |         |         |       |                |
|--------------------------------|----|---------|---------|-------|----------------|
|                                | N  | Minimum | Maximum | Mean  | Std. Deviation |
| Digital Security Awareness     | 50 | 2       | 5       | 3.84  | .912           |
| Phishing Identification Skills | 50 | 2       | 5       | 3.90  | .931           |
| Preventive Measures            | 50 | 3       | 5       | 4.04  | .947           |
| Total                          | 50 | 8       | 15      | 11.78 | 2.207          |
| Valid N (listwise)             | 50 |         |         |       |                |

For the digital security awareness indicator, the minimum score was 2 and the maximum score was 5, with a mean of 3.84 and a standard deviation of 0.912. This mean score indicates that respondents' awareness of the importance of digital security is in the fairly good category. Respondents generally understood the importance of protecting personal data, but there was still considerable variation in responses, as indicated by the standard deviation.

Furthermore, for the ability to identify phishing, the minimum score was 2 and the maximum score was 5, with a mean of 3.90 and a standard deviation of 0.931. This indicates that respondents are quite capable of recognizing the characteristics of phishing attacks, such as suspicious messages, fake links, or other digital fraud attempts. However, the relatively high variation in responses indicates that not all respondents have the same ability to identify these threats.

For the preventive measures indicator, the minimum score was 3 and the maximum score was 5, with a mean of 4.04 and a standard deviation of 0.947. A higher mean score compared to other indicators indicates that respondents tend to have taken good preventative measures, such as not sharing personal information carelessly, being careful when accessing links, and verifying information received.

Overall, the variable regarding customer ability to avoid phishing has a minimum total score of 8 and a maximum of 15, with a mean score of 11.78 and a standard deviation of 2.207. This total mean score indicates that customer ability is in the fairly high or good category in dealing with and avoiding phishing risks.

### Validity Test

#### Variable X

**Table 3.** Validity Test for Financial Literacy Variable

|    | R count | Sign | R table | Description |
|----|---------|------|---------|-------------|
| X1 | 0,414   | >    | 0,278   | Valid       |
| X2 | 0,385   | >    | 0,278   | Valid       |
| X3 | 0,502   | >    | 0,278   | Valid       |
| X4 | 0,515   | >    | 0,278   | Valid       |

For X1, the calculated  $r$  value was 0.414, which is greater than the table  $r$  (0.278), so item X1 was declared valid. This indicates that the item accurately measures financial literacy.

Furthermore, for X2, the calculated  $r$  value was 0.385, also greater than the table  $r$  (0.278), so item X2 was declared valid. This means that this item has a fairly strong relationship with the measured variable. For X3, the calculated  $r$  value was 0.502, which was also greater than the table  $r$  (0.278), so item X3 was declared valid. This value indicates that item X3 has a good correlation in measuring financial literacy variables.

Similarly, for X4, the calculated  $r$  value was 0.515, which is greater than the table  $r$  (0.278), so item X4 was declared valid. This value is the highest among the other items, so it can be said that item X4 has the strongest contribution in measuring financial literacy variables. Overall, because all calculated  $r$  values (X1–X4) are greater than the table  $r$ , all statement items in the financial literacy variable are declared valid and suitable for use as research instruments. This indicates that the instrument used is able to accurately measure the concept of financial literacy and can be reliably used for further analysis.

#### Variable Y

**Table 3.** Validity Test of the Variable: Customer Ability to Avoid Phishing

|    | R count | Sign | R table | Description |
|----|---------|------|---------|-------------|
| Y1 | 0,723   | >    | 0,278   | Valid       |
| Y2 | 0,724   | >    | 0,278   | Valid       |
| Y3 | 0,923   | >    | 0,278   | Valid       |

For Y1, the calculated  $r$  value was 0.723, which is greater than the table  $r$  (0.278), so item Y1 is declared valid. This value indicates that the item has a strong correlation in measuring customer ability to deal with phishing threats. Furthermore, for Y2, the calculated  $r$  value of 0.724 is also greater than the table  $r$  (0.278), so item Y2 is declared valid. This indicates that item Y2 has a high degree of correlation with the measured variable.

For Y3, the calculated  $r$  value was 0.923, the highest value among all items and significantly exceeds the table  $r$  (0.278), so item Y3 is declared valid. This value indicates that item Y3 has a very strong contribution in measuring the variable of customer ability to avoid phishing.

Because all calculated  $r$  values (Y1, Y2, and Y3) are greater than the table  $r$ , all items in the variable of customer ability to avoid phishing are declared valid and suitable for use as research instruments. Thus, the instrument used in this study met the validity criteria and can be used for further analysis, such as reliability testing and analyzing the influence of financial literacy variables on customers' ability to avoid phishing.

#### Reliability Test

**Table 4.** Reliability Test

| Variable                           | Cronbach's Alpha | Description |
|------------------------------------|------------------|-------------|
| Financial Literacy                 | 0,788            | Reliable    |
| Customer Ability to Avoid Phishing | 0,701            | Reliable    |

For the financial literacy variable, a Cronbach's Alpha value of 0.788 was obtained. This value indicates that the instrument used has a high level of internal consistency. This means that each statement item in this variable consistently measures the same concept, making it reliable for use in research. Furthermore, for the variable regarding customer ability to avoid phishing, a Cronbach's Alpha value of 0.701 was obtained. This value is also greater than the minimum threshold, so this variable is considered reliable. This indicates that the items in this variable have sufficient consistency in measuring customer ability to deal with phishing risks.

Overall, both variables have Cronbach's Alpha values above 0.60, so it can be concluded that all research instruments are reliable and suitable for further analysis, such as regression testing or hypothesis testing. Therefore, the data obtained are credible due to their high level of reliability.

### Classical Assumption Test

#### Normality Test

Table 5. Normality Test

| One-Sample Kolmogorov-Smirnov Test       |                         |                         |
|------------------------------------------|-------------------------|-------------------------|
|                                          |                         | Unstandardized Residual |
| N                                        |                         | 50                      |
| Normal Parameters <sup>a,b</sup>         | Mean                    | .0000000                |
|                                          | Std. Deviation          | 2.20633475              |
| Most Extreme Differences                 | Absolute                | .184                    |
|                                          | Positive                | .184                    |
|                                          | Negative                | -.136                   |
| Test Statistic                           |                         | .184                    |
| Asymp. Sig. (2-tailed) <sup>c</sup>      |                         | .205                    |
| Monte Carlo Sig. (2-tailed) <sup>d</sup> | Sig.                    | .270                    |
|                                          | 99% Confidence Interval |                         |
|                                          | Lower Bound             | .260                    |
|                                          | Upper Bound             | .271                    |

a. Test distribution is Normal.

b. Calculated from data.

c. Lilliefors Significance Correction.

d. Lilliefors' method based on 10000 Monte Carlo samples with starting seed 2000000.

Based on the test results, it was found that the sample size (N) was 50 respondents. In the normal parameters section, the mean residual value was 0.0000000, indicating that the residual average was close to zero. This is an ideal condition in regression analysis, as good residuals should have a mean of zero. Meanwhile, the standard deviation value of 2.20633475 indicates a spread of residual data around the mean, but still within reasonable limits.

Furthermore, in the most extreme differences section, the absolute value was 0.184, the positive value was 0.184, and the negative value was -0.136. This value indicates the maximum difference between the cumulative distribution of the data and the theoretical normal distribution. The smaller the difference, the closer the distribution is to normal.

The resulting test statistic value was 0.184. However, the most important factor in the Kolmogorov-Smirnov normality test is the significance value (Sig.). Based on the table, the Asymp. Sig. value was obtained. (2-tailed) was 0.205. Furthermore, the Monte Carlo Sig. (2-tailed) value was 0.270, with a 99% confidence interval ranging from 0.260 to 0.271. Both significance values are greater than the significance level used in this study, which is 0.05.

Therefore, because the significance values (0.205 and 0.270) are  $>0.05$ , it can be concluded that the residual data in this study is normally distributed. This means there is no violation of the normality assumption, and the regression model used in this study is suitable for proceeding to the next stage of analysis.

The results of this normality test indicate that the research data regarding the effect of financial literacy on customers' ability to avoid phishing has met one of the classic assumptions in regression analysis. This provides a strong basis for valid and scientific interpretation of the hypothesis testing results.

The Influence of Financial Literacy on Customers' Ability to Avoid Phishing: A Case Study of Bank Syariah Indonesia  
Ahmad Yani Bone Branch Office. Edi Darnadi et.al

## Heteroscedasticity Test

**Table 6.** Heteroscedasticity Test

|       |            | Coefficients <sup>a</sup>   |            |                           |       |
|-------|------------|-----------------------------|------------|---------------------------|-------|
| Model |            | Unstandardized Coefficients |            | Standardized Coefficients | t     |
|       |            | B                           | Std. Error | Beta                      | Sig.  |
| 1     | (Constant) | 1.948                       | 1.487      |                           | 1.310 |
|       | Total      | .001                        | .092       | .001                      | .008  |

a. Dependent Variable: abs\_res

Based on the test results in the coefficients table, it is known that the independent variable used is total financial literacy. The test results show a regression coefficient (B) of 0.001 with a significance value (Sig.) of 0.994. Furthermore, the calculated t-value is very small, at 0.008. This significance value is much higher than the significance level used in the study, which is 0.05. According to Glejser (1969), if the significance value (Sig.) of an independent variable is greater than 0.05, there are no symptoms of heteroscedasticity. Conversely, if the significance value is less than 0.05, there are indications of heteroscedasticity in the model.

Based on these results, because the significance value of 0.994 is greater than 0.05, it can be concluded that there are no symptoms of heteroscedasticity in this research's regression model. Meanwhile, the significance value at the constant of 0.196 is also greater than 0.05, further confirming that the regression model does not experience heteroscedasticity. This indicates that the residual variance is constant and is not affected by changes in the value of the independent variable.

Therefore, it can be concluded that the regression model in this study on the effect of financial literacy on customers' ability to avoid phishing has met the assumption of homoscedasticity. This means that the regression model used is adequate and can proceed to the next stage of analysis, such as linear regression and hypothesis testing.

## Hypothesis Testing

### t-Test

**Table 7.** t-Test

|       |                   | Coefficients <sup>a</sup>   |            |                           |       |
|-------|-------------------|-----------------------------|------------|---------------------------|-------|
| Model |                   | Unstandardized Coefficients |            | Standardized Coefficients | t     |
|       |                   | B                           | Std. Error | Beta                      | Sig.  |
| 1     | (Constant)        | 11.436                      | 3.365      |                           | 3.399 |
|       | Literasi Keuangan | .021                        | .209       | .015                      | 3.103 |

a. Dependent Variable: Total

Based on the analysis results in the coefficients table, the regression coefficient (B) for the financial literacy variable was 0.021, with a calculated t-value of 3.103 and a significance value (Sig.) of 0.019. The positive regression coefficient indicates that financial literacy has a direct relationship with customers' ability to avoid phishing. This means that the higher a person's level of financial literacy, the greater their ability to recognize and avoid various forms of digital fraud, including phishing.

The significance value of 0.019 is lower than the significance level used in this study, which is 0.05 ( $0.019 < 0.05$ ). Furthermore, the calculated t-value of 3.103 also indicates a fairly strong effect. Therefore, based on the hypothesis testing criteria, it can be concluded that financial literacy significantly influences customers' ability to avoid phishing. Regarding the hypotheses proposed in this study, namely:

- 1) H<sub>0</sub>: There is no effect of financial literacy on customers' ability to avoid phishing.

2) H1: There is an effect of financial literacy on customers' ability to avoid phishing.

Therefore, based on the results of the t-test, H0 is rejected and H1 is accepted. This is because the significance value is less than 0.05, indicating a statistically significant effect between financial literacy and customers' ability to avoid phishing. Substantively, the results of this study indicate that financial literacy plays a crucial role in increasing individual awareness and ability to deal with the risks of digital crime. Customers with good financial understanding tend to be more critical, cautious, and able to identify indications of fraud, such as suspicious messages, requests for personal data, or fake links often used in phishing practices.

The results of this t-test not only strengthen the research hypothesis but also provide practical implications: improving financial literacy needs to be continuously pursued, both through formal education and outreach by financial institutions, to minimize the risk of digital crime among the public.

### Coefficient of Determination (R<sup>2</sup>) Test

**Table 8.** Coefficient of Determination (R<sup>2</sup>) Test

| Model Summary                    |                   |          |                   |                            |
|----------------------------------|-------------------|----------|-------------------|----------------------------|
| Model                            | R                 | R Square | Adjusted R Square | Std. Error of the Estimate |
| 1                                | .615 <sup>a</sup> | .677     | .621              | 2.229                      |
| a. Predictors: (Constant), Total |                   |          |                   |                            |

Based on the analysis results in the Model Summary table, an R value of 0.615 was obtained. This value indicates a fairly strong relationship between financial literacy and customers' ability to avoid phishing. This relationship is positive, meaning that the higher the financial literacy, the higher the customer's ability to avoid phishing. Furthermore, the R Square (R<sup>2</sup>) value was 0.677. This indicates that 67.7% of the variation in customers' ability to avoid phishing can be explained by financial literacy. In other words, financial literacy makes a significant contribution to influencing customers' ability to deal with phishing risks.

Meanwhile, the Adjusted R Square value of 0.621 indicates that, after adjusting for the number of variables and the research sample, the financial literacy variable's ability to explain the dependent variable was 62.1%. This value provides a more accurate picture of the model's strength in the population. The remaining 32.3% (100% - 67.7%) is influenced by factors outside the research model, such as technological knowledge, experience using digital services, individual vigilance, environmental factors, and digital security education, which were not examined in this study.

Furthermore, the Std. Error of the Estimate value of 2.229 indicates a high level of prediction error in the regression model. This value is relatively small, indicating that the model has a fairly good level of accuracy in predicting the dependent variable. Thus, it can be concluded that financial literacy contributes significantly to explaining customers' ability to avoid phishing. This result also supports the findings of the previous t-test, which showed that financial literacy significantly impacts the dependent variable.

## Discussion

### The Effect of Financial Literacy on Customers' Ability to Avoid Phishing

Financial literacy has a positive and significant influence on customers' ability to avoid phishing. Financial literacy is not only related to the ability to manage finances but also encompasses an understanding of financial risks and digital crime. Customers with good financial literacy tend to have a better understanding of the safe use of financial products and services, are able to recognize the risks of digital transactions, and are more alert to requests for personal data, suspicious links, and messages impersonating official institutions.

The results of the study indicate that financial literacy significantly influences customers' ability to avoid phishing. This is evidenced by a t-test, which yielded a significance value below 0.05 and a positive regression coefficient. Furthermore, the coefficient of determination ( $R^2$ ) test results indicate that financial literacy explains a significant portion of the variation in customers' ability to avoid phishing. In other words, the higher a person's level of financial literacy, the better their ability to protect themselves from the threat of digital fraud.

These findings are supported by the 2022 OJK National Survey on Financial Literacy and Inclusion, which showed that people with higher levels of financial literacy tend to be more able to use financial services safely, avoid illegal financial practices, and have greater trust in formal financial institutions. This research also aligns with the findings of Sheng et al. (2022), who stated that digital financial knowledge forms a "cognitive shield" that allows individuals to better resist the psychological pressure often used in phishing schemes. Jampala et al. (2022) also emphasized that the ability to verify information is an important indicator of mature digital literacy, enabling individuals to more carefully validate information through official channels before making transactions or providing personal data.

Customers with high financial literacy are generally more critical, less likely to trust information with uncertain veracity, and more thorough in checking information sources. Financial literacy is also related to digital awareness, including the ability to recognize phishing characteristics such as the use of informal language, urgency to act immediately, and suspicious links. Therefore, financial literacy plays a crucial role in fostering vigilance and preventive behavior against digital crime. This study confirms that financial institutions need to continuously improve financial literacy through education, outreach, and training to enhance customer transaction security and reduce the risk of becoming a victim of phishing in the digital age.

### **The Impact of Financial Literacy on Customers' Ability to Avoid Phishing at Bank Syariah Indonesia's Ahmad Yani Bone Branch**

The impact of financial literacy on customers' ability to avoid phishing at Bank Syariah Indonesia's Ahmad Yani Bone Branch is strong and significant. The analysis shows a coefficient of determination ( $R^2$ ) of 0.677, meaning that 67.7% of customers' ability to avoid phishing can be explained by their level of financial literacy. This finding indicates that financial literacy is a key factor in enhancing customers' ability to recognize and avoid various forms of digital fraud.

Meanwhile, 32.3% of customer ability was influenced by factors outside the study, such as digital literacy, experience using digital banking services, individual vigilance, social environment, and cybersecurity education received. The t-test results also showed a significance value of 0.019 ( $<0.05$ ), confirming that the influence of financial literacy on the ability to avoid phishing was statistically significant. Furthermore, the positive regression coefficient indicates that the higher a customer's financial literacy, the greater their ability to recognize and avoid phishing schemes.

This finding is supported by research by Diana (2025), which states that digital financial literacy plays a crucial role in improving an individual's ability to recognize and avoid online fraud, including phishing. Individuals who understand financial products, transaction security, and personal data protection tend to be more alert to fake links and suspicious data requests. These results emphasize that financial literacy not only functions in financial management but also as a means of protecting oneself from the risks of digital crime.

In practice, customers with good financial literacy are better able to identify phishing attacks, maintain the confidentiality of their PINs, OTPs, and passwords, and exercise greater caution in digital transactions.

Therefore, banking institutions need to continuously improve education and outreach regarding financial literacy and digital transaction security. With a contribution of 67.7%, financial literacy can be concluded as a key factor in building customer resilience against phishing and is a crucial component of consumer protection strategies in the banking sector.

#### 4. Conclusion

Based on the results of research on the Influence of Financial Literacy on Customers' Ability to Avoid Phishing at Bank Syariah Indonesia's Ahmad Yani Bone Branch, several conclusions were drawn:

- a. Financial literacy has a positive and significant effect on customers' ability to avoid phishing. The higher the level of financial literacy, the better the customer's ability to recognize, be aware of, and prevent various forms of digital fraud. Therefore, financial literacy is a crucial factor in improving customer security and protection in digital transactions.
- b. Financial literacy has a significant and significant effect on customers' ability to avoid phishing at Bank Syariah Indonesia's Ahmad Yani Bone Branch. This is indicated by the  $R^2$  value of 67.7%, indicating that customers' ability to avoid phishing is largely influenced by their level of financial literacy, while the remaining 32.3% is influenced by other factors. Therefore, the higher the level of financial literacy, the better the customer's ability to protect themselves from digital fraud.

#### 5. Reference

- Abdullah, K. (2013). *Tahapan dan langkah-langkah penelitian*. Lukman Al Hakim Press.
- Arikunto, S. (2013). *Prosedur penelitian*. Rineka Cipta.
- Bank Indonesia. (2017). *Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang penyelenggaraan teknologi finansial*. Bank Indonesia.
- Bank Indonesia. (2018). *Booklet financial technology*. Bank Indonesia.
- Choeruddin, A., et al. (2023). *Literasi keuangan*. PT Global Eksekutif Teknologi.
- Diana. (2025). Literasi keuangan digital dan kemampuan menghindari penipuan online. *Jurnal Literasi Keuangan Digital*.
- Fakultas Ekonomi dan Bisnis Islam IAIN Bone. (2020). *Pedoman penulisan karya tulis ilmiah*. IAIN Bone.
- Fitrah, M., & Luthfiah. (2018). *Metodologi penelitian: Penelitian kualitatif, tindakan kelas & studi kasus*. CV Jejak.
- Ghozali, I. (2013). *Aplikasi analisis multivariate dengan program IBM SPSS 23*. Universitas Diponegoro.
- Jampala, R. C., et al. (2022). Digital financial literacy and cybersecurity awareness: A study on bank customers. *International Journal of Professional Business Review*.
- Kementerian Agama RI. (2019). *Al-Qur'an dan terjemahnya*. Badan Litbang dan Diklat Kementerian Agama RI.
- Lestari, S. K., Hindrayani, A., & Sangka, K. B. (2025). Pengaruh literasi keuangan dan literasi digital terhadap kesadaran penipuan investasi pada mahasiswa. *E-Jurnal Ekonomi dan Bisnis Universitas Udayana*, 14(4), 490–501.
- Muftiadi, A., Agustina, T. P. M., & Evi, M. (2022). Studi kasus keamanan jaringan komputer: Analisis ancaman phishing terhadap layanan online banking. *Hexatech: Jurnal Ilmiah Teknik*, 1(2), 61.
- Otoritas Jasa Keuangan. (2019). *Indeks literasi dan inklusi keuangan Indonesia*. Otoritas Jasa Keuangan.
- Otoritas Jasa Keuangan. (2020). *Strategi nasional literasi keuangan Indonesia (SNLKI) 2021–2025*. Otoritas Jasa Keuangan.
- Otoritas Jasa Keuangan. (2021). *Roadmap pengembangan dan penguatan fintech 2021–2025*. Otoritas Jasa Keuangan.

- Otoritas Jasa Keuangan. (2025). *Strategi nasional literasi keuangan Indonesia (SNLKI) 2021–2025*. Otoritas Jasa Keuangan.
- Prasetyo, J., & Jannah. (2005). *Metode penelitian kuantitatif*. Raja Grafindo Persada.
- Putra, I. K. O. K., et al. (2022). Tindakan kejahatan pada dunia digital dalam bentuk phishing. *Cybersecurity dan Forensik Digital*, 4(2), 78.
- Rahmiyanti, S., Fahrurnisa, V., Ridwan, M., et al. (2024). Penyuluhan interaktif literasi keuangan guna mencegah jebakan pinjaman online ilegal. *Jurnal Pengabdian UNDIKMA*, 5(3), 456–463.
- Sheng, S., et al. (2022). Why they fall for phishing: An analysis of consumer vulnerability and protection. *Journal of Cybersecurity and Privacy*.
- Silalahi, U. (2010). *Metode penelitian sosial*. PT Refika Aditama.
- Sugiyono. (2014). *Statistika untuk penelitian*. IKAPI.
- Sugiyono. (2025). *Metode penelitian kuantitatif, kualitatif dan R&D*. Alfabeta.
- Syahdeni, S. R. (2009). *Kejahatan & tindak pidana komputer*. Pustaka Utama Grafit.
- Tabrani, S., et al. (2024). Kejahatan phishing ditinjau dari perspektif hukum dan kejahatan siber. *Civilia: Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan*, 3(1), 4.
- Teguh, M. (2001). *Metodologi penelitian*. PT Raja Grafindo Persada.
- Umar, H. (2014). *Metode penelitian untuk skripsi dan tesis*. Raja Grafindo Persada.
- Winarni, S. E. (2021). *Literasi keuangan dan inklusi keuangan di Indonesia*. Rajawali Pers.
- Yuliardi, R., & Nuraeni, Z. (2017). *Statistika penelitian plus tutorial SPSS*. Innosain.
- Yusuf, M. D., Addermi, & Lim, J. (2022). Kejahatan phishing dalam dunia cyber crime dan sistem hukum di Indonesia. *Jurnal Pendidikan dan Konseling*, 4(5), 8019–8020.
- Winda Nuraeni, et al. (2025). Analisis literasi keuangan dan perencanaan keuangan generasi Z di Kabupaten Bekasi terhadap risiko penipuan keuangan. *YUME: Journal of Management*, 8(1), 216–230.