

Research Article

The Effect Of Digital Literacy, Financial Literacy, And Digital Security On Digital Financial Fraud Prevention Behavior (A Study of E-Wallet and Mobile Banking Users in Cikole District)

Hani Handayani: Muhammadiyah University of Sukabumi, **Indonesia**; Email: hanihndyani29@gmail.com

Sulaeman: Muhammadiyah University of Sukabumi, **Indonesia**; Email: sulaeman1342@ummi.ac.id

Irfan Sophan Himawan: Muhammadiyah University of Sukabumi, **Indonesia**; Email: irfan.sophan@ummi.ac.id

*Corresponding Author: hanihndyani29@gmail.com

DOI: <https://doi.org/10.61492/sadana.V1i2> | received: 06-15-2026; accepted: 06-15-2026; online: 06-30-2026

Abstract: The development of digital financial services, particularly e-wallets and mobile banking, has increased the convenience of public transactions, but has also increased the risk of digital financial fraud. This study aims to analyze the influence of digital literacy, financial literacy, and digital security on digital financial fraud prevention behavior among e-wallet and mobile banking users in Cikole District. The study used a quantitative approach with a survey method of 100 respondents selected using a purposive sampling technique. Data were collected through questionnaires and analyzed using multiple linear regression with the help of SPSS. The results show that digital literacy and financial literacy have a positive and significant effect on digital financial fraud prevention behavior. Financial literacy is the variable with the most dominant influence. Meanwhile, digital security does not have a significant effect partially on digital financial fraud prevention behavior. However, digital literacy, financial literacy, and digital security simultaneously have a significant effect on digital financial fraud prevention behavior. These findings indicate that improving digital literacy and financial literacy are important factors in strengthening the public's ability to recognize, avoid, and respond to various forms of digital financial fraud.

Keywords: Digital Literacy, Financial Literacy, Digital Security, Digital Financial Fraud Prevention Behavior

1. Introduction

The development of digital technology has significantly transformed the way people conduct financial activities. Digital transformation in the financial sector is marked by the increasing use of digital financial services such as e-wallets and mobile banking, which offer convenience, speed, and efficiency in various financial transactions. Today, people can make payments, transfer funds, purchase products, and even invest simply through digital devices connected to the internet. This situation demonstrates that digital financial services have become a vital part of modern economic life and are driving the acceleration of financial inclusion in various countries, including Indonesia (Bank Indonesia, 2024).

Indonesia is one of the countries with the fastest growth in digital financial transactions. Bank Indonesia (2024) reported that the value of electronic money transactions and digital banking services continues to increase year after year. This increase indicates a growing public acceptance of digital technology in financial activities. Furthermore, the development of fintech, e-commerce, and the digital payment ecosystem has also driven increased use of digital financial services by various groups (Financial Services Authority [OJK], 2024).

Despite its numerous benefits, the development of digital financial services has also been accompanied by an increasing risk of digital financial fraud. Various forms of cybercrime, such as phishing, social engineering, identity theft, misuse of one-time passwords (OTPs), malware, and fake links, are increasingly being used by criminals to gain access to users' financial data and assets. These

fraudulent methods are becoming increasingly complex as society's reliance on digital technology for financial activities increases (Bada et al., 2022).

This fact is supported by data from the Financial Services Authority (OJK) through the Indonesia Anti-Scam Center (IASC), which recorded 299,237 reports of digital financial fraud from November 2024 to October 2025, with an average of 874 cases per day. The total reported losses reached Rp 7 trillion.

Table 1. Data on Digital Financial Fraud Cases in Indonesia

Indicator	Period	Amount
Report to IASC OJK	Nov 2024–Oct 2025	299,237 reports
Average cases per day	2024–2025	874 cases
Total loss	2024–2025	Rp. 7 trillion
Reported account	2024–2025	487,378 accounts
Account blocked	2024–2025	93,344 accounts

Source: OJK & IASC, processed by the author (2026)

This phenomenon is reflected in the high number of digital financial fraud cases in Indonesia. Data from the Indonesia Anti-Scam Center (IASC), which is under the coordination of the Financial Services Authority (OJK), shows that from November 2024 to October 2025, there were hundreds of thousands of reports of digital financial fraud, resulting in losses to the public reaching trillions of rupiah. Furthermore, the National Cyber and Crypto Agency (BSSN) also reported that the financial sector has been a primary target of cyberattacks in Indonesia over the past few years (BSSN, 2024). This situation indicates that the increasing use of digital financial services has not been fully matched by the public's ability to protect themselves from various digital fraud threats.

One factor believed to play a role in encouraging behavior to prevent digital financial fraud is digital literacy. Digital literacy relates not only to the ability to use technological devices, but also to the ability to access, understand, evaluate, and utilize digital information critically and responsibly. Individuals with good digital literacy tend to be better able to recognize false information, identify suspicious activity, and understand the risks inherent in the digital environment (UNESCO, 2023). Therefore, digital literacy can be a form of initial protection against various forms of digital financial fraud.

In addition to digital literacy, financial literacy also plays a crucial role in shaping individual behavior in dealing with financial risks. Financial literacy reflects a person's level of knowledge, skills, confidence, and ability to make sound financial decisions. Individuals with high levels of financial literacy generally have a better understanding of the characteristics of financial products, investment risks, and the potential losses that may arise from various digital financial activities. Therefore, financial literacy can help people avoid various forms of fraud that exploit users' low financial literacy (OECD, 2023; Lusardi, 2023).

Another equally important factor is digital security. Digital security relates to an individual's ability to protect personal data, digital accounts, and online activities from various cyber threats. Using strong passwords, multi-factor authentication, regular application updates, and being careful when accessing digital links are all part of digital security practices that can minimize the risk of digital financial fraud (Kominfo, 2023). The higher an individual's awareness of digital security, the more likely they are to take preventative measures against various technology-based fraud threats.

Theoretically, this research is based on Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB). Protection Motivation Theory explains that individuals will be motivated to take protective action when they are aware of a threat and believe that the preventive action taken can reduce the risk faced (Maddux & Rogers, 1983). Meanwhile, the Theory of Planned Behavior explains that individual behavior is influenced by attitudes, intentions, and perceived control over certain behaviors (Ajzen, 1991). In the context of this research, digital literacy, financial literacy, and digital security can be factors that strengthen an individual's ability to carry out digital financial fraud prevention behaviors.

Previous research has shown that digital and financial literacy are related to various digital financial behaviors, such as the use of financial technology, awareness of illegal investments, and the use of mobile banking (Umar & Dalimunthe, 2024; Widiyati & Erliana, 2024; Lestari et al., 2025). However, most research still focuses on technology adoption behavior, the use of digital financial services, or awareness of fraudulent investments. Research specifically examining digital financial fraud prevention behavior as a dependent variable is still relatively limited. Furthermore, research that integrates digital literacy, financial literacy, and digital security into a single research model is still rare, especially in the context of the general public using e-wallets and mobile banking.

Based on these phenomena and research gaps, this study offers novelty through the development of an integrative model that examines the influence of digital literacy, financial literacy, and digital security on digital financial fraud prevention behavior among e-wallet and mobile banking users in Cikole District. Unlike previous studies, which predominantly focused on student respondents or users of specific technologies, this study focuses on the general public, who have more heterogeneous characteristics in terms of age, education, digital experience, and financial behavior. Therefore, this study is expected to provide theoretical contributions to the development of literature on digital financial behavior and provide practical implications for regulators, financial institutions, and digital service providers in improving consumer protection against the risk of digital financial fraud.

2. Literature Review and Hypothesis Development

Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) is a behavioral theory that explains how individuals respond to threats and develop protective behaviors against the risks they face. This theory was first introduced by Rogers and later developed further by Maddux and Rogers (1983). PMT explains that an individual's motivation to take protective action is influenced by two main cognitive processes: threat appraisal and coping appraisal (Maddux & Rogers, 1983).

In the context of digital finance, PMT is widely used to explain cybersecurity behaviors, digital privacy protection, and online fraud prevention practices. Individuals who are aware of the high risks of data theft, phishing, and misuse of digital financial accounts will be motivated to implement better protective measures if they have sufficient skills and knowledge to address these threats (Ifinedo, 2021; Tsai et al., 2021).

Recent research shows that digital literacy, cybersecurity awareness, and the ability to understand digital transaction risks are strongly associated with the formation of protective behaviors among digital financial service users (Alghamdi et al., 2023). Therefore, PMT serves as a relevant theoretical basis for explaining digital financial fraud prevention behaviors among e-wallet and mobile banking users.

Theory of Planned Behavior (TPB)

The Theory of Planned Behavior (TPB) developed by Ajzen (1991) explains that individual behavior is influenced by behavioral intention which is formed through three main components, namely attitude toward behavior, subjective norm, and perceived behavioral control.

According to the TPB, individuals are more likely to engage in a behavior if they have a positive attitude toward it, receive social support from their environment, and feel they have sufficient ability to carry it out (Ajzen, 1991). In the context of digital technology, the TPB has been widely used to explain technology use behavior, information security, digital transactions, and personal data protection (Yasa et al., 2023).

In this study, digital literacy, financial literacy, and digital security are considered factors that can increase an individual's perceived behavioral control. The greater a person's understanding of digital technology and financial risks, the greater their confidence in their ability to avoid various forms of digital fraud. Thus, individuals will be more motivated to adopt digital financial fraud prevention behaviors (Alharbi & Sohaib, 2021).

Digital Literacy

Digital literacy is an individual's ability to access, understand, evaluate, create, and utilize information through digital technology effectively, critically, and responsibly (UNESCO, 2023). Digital literacy encompasses not only the technical ability to operate digital devices but also critical thinking skills, digital security, digital communication, and the ability to identify valid information in the digital environment (European Commission, 2022).

According to UNESCO (2023), digital literacy is a fundamental competency in the era of digital transformation because individuals are required to be able to filter information, identify cyber threats, and make informed decisions in an increasingly complex digital environment. Meanwhile, the Ministry of Communication and Information Technology (2023) explains that digital literacy in Indonesia still faces challenges, particularly in the areas of digital security and digital culture.

In the digital financial sector, digital literacy plays a crucial role in helping users recognize fraudulent methods such as phishing, fake websites, malware, social engineering, and OTP misuse. Individuals with strong digital literacy skills tend to be more alert to various forms of digital threats than those with low levels of digital literacy (Umar & Dalimunthe, 2024).

Research conducted by Harliani and Kurniawan (2025) shows that digital literacy skills contribute to improving individuals' ability to recognize and avoid various forms of online fraud. Similar findings were also reported by Lestari et al. (2025), who found that digital literacy positively impacted the ability to detect fraudulent investments and misleading financial information.

Financial Literacy

Financial literacy is a combination of knowledge, skills, attitudes, and behaviors that enable individuals to make effective financial decisions to improve their financial well-being (OECD, 2023). The Financial Services Authority (OJK) (2024) defines financial literacy as the knowledge, beliefs, and skills that influence the quality of decision-making and financial management.

Financial literacy is a crucial factor in the digital era, as more and more financial products and services become available online. Individuals with good financial literacy are better able to understand the risks of digital transactions, distinguish between legal and illegal financial products, and avoid various forms of financial fraud (Lusardi, 2023).

According to the OECD (2023), financial literacy is significantly related to an individual's ability to manage financial risk. Individuals with high levels of financial literacy tend to have better financial management behaviors, are more cautious in making investment decisions, and are better able to avoid financial fraud schemes.

Research by Supu et al. (2025) found that financial literacy positively impacts the mitigation of digital transaction fraud. Similar results were also found by Umar and Dalimunthe (2024), who stated that financial literacy plays a crucial role in increasing individual awareness of various forms of digital investment fraud.

Digital Security

Digital security is a series of actions taken to protect digital devices, data, identities, and activities from various cybersecurity threats (Kominfo, 2023). In the context of digital financial transactions, digital security is a crucial factor because most financial activities are conducted over the internet, which is vulnerable to various forms of cyberattacks.

The National Institute of Standards and Technology (NIST, 2023) explains that digital security encompasses digital identity protection, user authentication, network security, password management, and device protection from malicious software. Users who implement good digital security practices have a lower risk of becoming victims of data theft and digital financial fraud.

Research by Widiyati and Erliana (2024) shows that cybersecurity has a positive influence on the safe use of financial technology services. Furthermore, Alharbi and Sohaib (2021) found that digital security awareness improves users' ability to protect personal information and reduces the likelihood of becoming victims of cybercrime.

Digital Financial Fraud Prevention Behavior

Digital financial fraud prevention behaviors are actions individuals take to avoid, reduce, and protect themselves from various fraud risks that occur in digital financial activities. These behaviors include identity verification, personal data protection, dual authentication, avoiding suspicious links, and reporting activities that indicate fraud (OECD, 2023).

According to PMT, preventive behavior is a form of protective behavior that arises from the perception of threat and the belief that preventive measures can reduce the risk faced (Maddux & Rogers, 1983). Meanwhile, TPB explains that this behavior is influenced by an individual's intentions, which are formed from knowledge, attitudes, and perceptions of control over the risks faced (Ajzen, 1991).

In the context of digital financial services, fraud prevention practices are becoming increasingly important due to the rise in technology-based fraud cases. Users with good digital literacy, financial literacy, and digital security are likely to be better prepared to deal with the various fraud schemes emerging on e-wallet and mobile banking platforms.

The Influence Between Research Variables

The Influence of Digital Literacy on Digital Financial Fraud Prevention Behavior

Digital literacy refers to an individual's ability to access, understand, evaluate, and utilize digital information effectively and safely. In an increasingly complex digital financial environment, digital literacy is a crucial competency because it helps individuals recognize various cyber threats such as phishing, malware, fake websites, and social engineering (UNESCO, 2023). Users with high levels of digital literacy tend to be better able to identify suspicious digital activity and verify information before making financial transactions.

Based on Protection Motivation Theory (PMT), understanding threats and an individual's ability to address them will encourage protective behavior. The greater an individual's understanding of

digital risks, the greater their likelihood of implementing preventative measures against the threats they face (Ifinedo, 2022). In the context of digital transactions, digital literacy helps users reduce their vulnerability to various forms of fraud that exploit weaknesses in information and technology.

Research by Umar and Dalimunthe (2024) found that digital literacy increases awareness of digital investment fraud. Similar results were also reported by Lestari et al. (2025), who showed that individuals with high levels of digital literacy were better able to identify false financial information and digital-based fraud schemes. Furthermore, Harliani and Kurniawan (2025) found that digital literacy skills contribute to improving individuals' ability to prevent online fraud.

H1: Digital literacy has a positive effect on digital financial fraud prevention behavior.

The Influence of Financial Literacy on Digital Financial Fraud Prevention Behavior

Financial literacy is an individual's ability to understand financial concepts and use that knowledge to make informed financial decisions. The OECD (2023) emphasizes that financial literacy encompasses the knowledge, skills, attitudes, and behaviors necessary to achieve financial well-being. In the digital age, understanding the risks of financial products and electronic transactions is increasingly crucial to avoid losses due to fraud.

The Theory of Planned Behavior explains that a person's behavior is influenced by their level of knowledge and perceived control over their actions (Ajzen, 1991). Individuals with good financial literacy tend to have a higher ability to evaluate risks, distinguish between legal and illegal financial products, and recognize various forms of financial fraud (Lusardi, 2023).

Empirical findings indicate that financial literacy contributes to an individual's ability to prevent the risk of financial fraud. Supu et al. (2025) found that financial literacy significantly influenced the mitigation of digital transaction fraud. Research by Lestari et al. (2025) also showed that individuals with higher levels of financial literacy were better able to recognize fraudulent investments and financial fraud schemes.

H2: Financial literacy has a positive effect on digital financial fraud prevention behavior.

The Influence of Digital Security on Digital Financial Fraud Prevention Behavior

Digital security is an individual's ability to protect personal data, devices, accounts, and digital activities from various cybersecurity threats. When using e-wallet and mobile banking services, digital security practices are crucial because most financial activities are conducted online and vulnerable to various forms of cybercrime (Kominfo, 2023).

According to Protection Motivation Theory, individuals with strong protective capabilities are more motivated to take preventive action when facing a threat (Rogers, 1983). Implementing multifactor authentication, using strong passwords, regularly updating applications, and protecting personal data are all forms of protective behavior that can reduce the risk of digital fraud.

Research by Widiyati and Erliana (2024) shows that cybersecurity positively influences the behavior of safely using digital financial services. Similar findings were also reported by Alghamdi et al. (2023), who found that digital security awareness contributes to increased user protection behavior against cyber threats. Furthermore, Alharbi and Sohaib (2021) demonstrated that digital security capabilities can reduce user vulnerability to data theft and account misuse.

H3: Digital security has a positive effect on digital financial fraud prevention behavior.

The Influence of Digital Literacy, Financial Literacy, and Digital Security on Digital Financial Fraud Prevention Behavior

Digital financial fraud prevention behavior is the result of a combination of an individual's ability to understand digital technology, manage financial risks, and implement digital security practices. The PMT explains that protective behavior emerges when an individual understands the threats they face and has sufficient skills to address them (Ifinedo, 2022). Meanwhile, the TPB explains that behavior is influenced by an individual's knowledge and perceived control over their actions (Yasa et al., 2023).

Therefore, digital literacy, financial literacy, and digital security are expected to collectively improve digital financial fraud prevention behavior. Individuals who understand digital risks, possess adequate financial knowledge, and implement good digital security practices will be better prepared to deal with the various fraud modes that are developing in e-wallet and mobile banking services.

H4: Digital literacy, financial literacy, and digital security simultaneously have a positive influence on digital financial fraud prevention behavior.

3. Method

This study uses a quantitative approach with a survey design to examine the influence of digital literacy, financial literacy, and digital security on digital financial fraud prevention behavior. A quantitative approach was chosen because it allows for objective measurement of the relationships between variables through statistical analysis and testing of previously formulated hypotheses.

The research was conducted in Cikole District, Sukabumi City, West Java. This location was chosen because it is one of the centers of economic activity, education, and digital service use in Sukabumi City, making it a representative location for studying the behavior of digital financial service users. The research subjects were people who use digital financial services, specifically e-wallet and mobile banking users.

The study population consisted of digital financial service users in Cikole District. Based on Cikole District population data and estimates of digital financial service users calculated using the national financial inclusion rate, the target population was estimated at 34,532 people. The sample size was determined using the Slovin formula with a 10% margin of error, resulting in a sample size of 100 respondents. The sampling technique used was non-probability sampling with a purposive sampling approach. Respondents were selected based on the criteria of having used e-wallet and/or mobile banking services in their daily financial activities.

The research data is primary data obtained through an online questionnaire distributed using Google Forms. The research instrument was constructed using a five-point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree). The digital literacy variable was measured through the dimensions of digital skills, critical culture, digital ethics, and cognitive security. Financial literacy was measured through the dimensions of financial knowledge, financial attitudes, and financial behavior. Digital security was measured through the dimensions of password management, dual authentication, network security, and application management. Meanwhile, digital financial fraud prevention behavior was measured through the dimensions of identity verification, credential protection, resistance to psychological manipulation, and risk reporting and mitigation.

Data analysis was performed using the Statistical Package for the Social Sciences (SPSS) software. The analysis stages included validity and reliability tests to ensure the quality of the research instruments. Next, classical assumption tests were conducted, consisting of normality tests, multicollinearity tests, and heteroscedasticity tests, to ensure the feasibility of the regression model. Hypothesis testing was conducted using multiple linear regression analysis to measure the partial and simultaneous effects of digital literacy, financial literacy, and digital security on digital financial

fraud prevention behavior. In addition, the t-test was used to test the effect of each independent variable partially, the F-test was used to test the simultaneous effect of all independent variables, while the coefficient of determination (R^2) was used to measure the model's ability to explain variations in digital financial fraud prevention behavior.

4. Results

Overview of Research Location

Profile and Conditions of Cikole District

The Cikole District area is located at 6 0 49' - 7 0 49' South Latitude and 106 0 45'' - 106 0 50' East Longitude, located to the south of the foot of Mount Gede with a slope of 0% - 3% in the south and 3% - 8% in the north, with uneven/downhill land structure conditions with a height of around 550m-750m above sea level, and an average temperature of 260 C.



Figure 1. Map of Cikole District

The Cikole District covers an area of 6.21 square kilometers, equivalent to 12.84 percent of Sukabumi City. Administratively, Cikole District comprises six sub-districts (kelurahan), 69 neighborhood units (RW), and 347 neighborhood units (RT). The sub-districts within Cikole District are as follows:

- 1) Gunung Parang Subdistrict with an area of 0.45 km²
- 2) Kebonjati sub-district with an area of 0.47 km²
- 3) Cikole sub-district with an area of 0.81 km²
- 4) Selabatu sub-district with an area of 1.14 km²
- 5) Cisarua sub-district with an area of 1.42 km²
- 6) Subangjaya sub-district with an area of 1.91 km²

Respondent Characteristics

This study involved 100 respondents who were e-wallet and mobile banking users in Cikole District. Based on gender, 52 respondents were female (52%), while 48 respondents were male (48%). This indicates a relatively balanced respondent composition, with a slight female predominance.

Based on age, the majority of respondents (93 people) were in the 17–25 age group, while 7 people (7%) were in the 26–40 age group. This finding indicates that digital financial service users in this study are predominantly young people, who have a relatively high level of digital technology adoption.

Based on the type of digital financial service used, 32 respondents (32%) used e-wallets, 5 respondents (5%) used mobile banking, and 63 respondents (63%) used both services. These results indicate that the majority of respondents have utilized more than one digital financial platform in their daily transactions, demonstrating a high level of digital financial service integration among the Cikole District community.

Table 2. presents a summary of the characteristics of the research respondents.

Characteristics	Category	Frequency	Percentage
Gender	Man	48	48%
	Woman	52	52%
Age	17-25 Years	93	93%
	26-40 Years	7	7%
Digital Financial Services	E-Wallet	32	32%
	Mobile Banking	5	5%
	E-Wallet and Mobile Banking	63	63%

Source: Processed data (2026).

Normality Test

A good regression model is one that has a normal or near-normal data distribution. If the data is not normally distributed, it is considered less able to accurately represent the characteristics of the population. To ensure normality of data distribution, statistical analysis was performed using the Shapiro-Wilk test with a significance level (α) of 0.05. If the significance value is ≥ 0.05 , the sample data is considered normally distributed. Conversely, if the significance value is ≤ 0.05 , the sample data is considered non-normally distributed. The results of the normality test are as follows:

Table 3. Normality Test Results

	<i>Kolmogorov-Smirnova</i>			<i>Shapiro-Wilk</i>		
	<i>Statistical</i>	<i>df</i>	<i>Sig.</i>	<i>Statistics</i>	<i>df</i>	<i>Sig.</i>
<i>Unstandardized Residual</i>	0.105	100	0.008	0.978	100	0.091

Source: Data processed with SPSS 25 (2026)

Based on table 3. above, which is the result of the normality test using the Shapiro-Wilk test, it shows a significance value (Sig.) of $0.091 > 0.05$, so it can be concluded that the data is normally distributed and has met the classical regression assumption requirements.

Multiple Linear Regression Analysis

Table 4. Results of Multiple Linear Analysis

<i>Model</i>		<i>Unstandardized Coefficients</i>		<i>Standardized Coefficients</i>	<i>t</i>	<i>Sig.</i>
		<i>B</i>	<i>Std. Error</i>	<i>Beta</i>		
	(Constant)	7,255	1,710		4,242	0,000
	X1 (Digital Literacy)	0.286	0.087	0.316	3,283	0.001
	X2 (Financial Literacy)	0.390	0.118	0.329	3,297	0.001
	X3 (Digital Security)	0.040	0.063	0.056	0.639	0.524

Dependent Variable: Y (Digital Fraud Prevention Behavior)

Source: Data processed with SPSS 25 (2026)

Based on table 4. above, the multiple linear regression equation is obtained as follows:

$$Y = 7.255 + 0.268 X1 + 0.390 X2 + 0.040 X3 + e$$

From the multiple linear regression equation above, it can be interpreted as follows:

- a. The constant value is 7.255, meaning that if all X variables or independent variables, namely (X1) Digital Literacy, (X2) Financial Literacy and (X3) Digital Security have a value of zero or constant, then the value of the variable (Y) Digital Fraud Prevention Behavior is 7.255.
- b. The regression coefficient value (β_1) of the Digital Literacy variable is 0.286, meaning that if the Digital Literacy variable is increased by one unit while the other independent variables are assumed to be zero or constant, then the Digital Fraud Prevention Behavior variable will increase by 0.286.
- c. The regression coefficient value (β_2) of the Financial Literacy variable is 0.390, meaning that if the Financial Literacy variable is increased by one unit while other independent variables are assumed to be zero or constant, then the Digital Fraud Prevention Behavior variable will increase by 0.390.
- d. The regression coefficient value (β_3) of the Digital Security variable is 0.040, meaning that if the Digital Security variable is increased by one unit while the other independent variables are assumed to be zero or constant, then the Digital Fraud Prevention Behavior variable will increase by 0.040.

T-test

The t test can also be seen by comparing the calculated t and t table values. If $t_{\text{count}} > t_{\text{table}}$, then H_0 is rejected and H_a is accepted (there is influence). However, on the contrary, if $t < t_{\text{table}}$, then H_0 is accepted and H_a is rejected (there is no influence). With $df = \alpha / 2; n - k - 1$, then we get $df = 0.05 / 2; 100 - 3 - 1 = 0.025; 96$ so the t table is 1.9849. The t test results can be seen as follows:

Table 5. Results of the t-Test (Partial Test)

<i>Model</i>		<i>Unstandardized Coefficients</i>	<i>t</i>	<i>Sig.</i>
		<i>B</i>		
	(Constant)	7,255	4,242	0,000
	X1 (Digital Literacy)	0.286	3,283	0.001
	X2 (Financial Literacy)	0.390	3,297	0.001
	X3 (Digital Security)	0.040	0.639	0.524

Dependent Variable: Y (Digital Fraud Prevention Behavior)

Source: Data processed with SPSS 25 (2026)

Based on table 5. above, the description of the t-test results for each variable is as follows:

- a) The Influence of Digital Literacy on Digital Fraud Prevention Behavior
The test results show that the calculated t value for the Digital Literacy variable is 3.283 with a significance value of 0.001. Considering that the calculated t value $> t_{\text{table}}$ ($3.283 > 1.9849$) and the significance value < 0.05 ($0.001 < 0.05$), then H_{01} is rejected and H_{a1} is accepted. This can be concluded that the Digital Literacy variable partially has a positive and significant influence on Digital Fraud Prevention Behavior.
- b) The Influence of Financial Literacy on Digital Fraud Prevention Behavior
The test results show that the calculated t value for the Financial Literacy variable is 3.297 with a significance value of 0.001. Considering that the calculated t value $> t_{\text{table}}$ ($3.297 > 1.9849$) and the significance value < 0.05 ($0.001 < 0.05$), then H_{02} is rejected and H_{a2} is accepted. This can be concluded that the Financial Literacy variable partially has a positive and significant influence on Digital Fraud Prevention Behavior.
- c) The Influence of Digital Security on Digital Fraud Prevention Behavior

The test results show that the calculated t value for the Digital Security variable is 0.639 with a significance value of 0.524. Considering that the calculated t value < t table ($0.639 < 1.9849$) and the significance value > 0.05 ($0.524 > 0.05$), H_{o3} is accepted and H_{a3} is rejected. This proves that the Digital Security variable partially does not have a significant influence on Digital Fraud Prevention Behavior.

Discussion

The Influence of Digital Literacy on Digital Financial Fraud Prevention Behavior

The results of the study indicate that digital literacy has a positive and significant effect on digital financial fraud prevention behavior among e-wallet and mobile banking users in Cikole District. The regression analysis results show a coefficient value of 0.286 with a t-value of 3.283 and a significance level of 0.001 (< 0.05), thus accepting the first hypothesis. This finding indicates that the higher the level of digital financial service users' digital literacy, the higher their preventive behavior against various forms of digital financial fraud.

These findings support the Protection Motivation Theory (PMT), which explains that individuals who are able to recognize threats and understand how to address them will be more motivated to take protective action. Digital literacy enables users to identify suspicious links, understand phishing risks, verify information, and be more careful about safeguarding personal data when using digital financial services.

The results of this study align with those of Umar and Dalimunthe (2024), who found that digital literacy increases awareness of digital investment fraud. These findings are also consistent with research by Lestari et al. (2025), who showed that digital literacy skills help individuals identify misleading financial information and various technology-based fraud schemes.

Empirically, the average digital literacy score of respondents is considered very good. This indicates that the majority of e-wallet and mobile banking users in Cikole District have adequate skills in using digital technology safely. These skills are crucial for developing behaviors to prevent digital financial fraud amid the increasing threat of cybercrime.

The Influence of Financial Literacy on Digital Financial Fraud Prevention Behavior

The results of the study indicate that financial literacy has a positive and significant effect on digital financial fraud prevention behavior. The regression coefficient value of 0.390, with a t-value of 3.297 and a significance level of 0.001, indicates that the second hypothesis is accepted. Furthermore, financial literacy is the variable with the most dominant influence compared to other independent variables.

These findings indicate that understanding financial products, digital transaction risks, banking procedures, and the ability to recognize unsound investments and offers are key factors in shaping digital financial fraud prevention behavior. Individuals with good financial literacy tend to be more rational in making financial decisions and more alert to various fraudulent schemes that offer instant profits.

The results of this study support the Theory of Planned Behavior (TPB), which explains that an individual's knowledge and perceived control influence their behavior. The higher a person's financial literacy, the greater their ability to control financial decisions and avoid risks that could harm them.

These findings are consistent with the OECD (2023) which states that financial literacy plays a crucial role in financial risk management. The findings of this study also align with those of Umar

and Dalimunthe (2024) and Thomas et al. (2024), who demonstrated that financial literacy is a crucial factor in improving individuals' ability to cope with various risks in the digital financial ecosystem.

This finding is particularly relevant given the persistent gap between the levels of financial inclusion and financial literacy among Indonesians. This situation suggests that the use of digital financial services is growing faster than the public's ability to understand the associated risks.

The Influence of Digital Security on Digital Financial Fraud Prevention Behavior

The results of the study indicate that digital security does not significantly influence digital financial fraud prevention behavior. The regression coefficient value of 0.040, with a t-value of 0.639 and a significance level of 0.524 (>0.05), indicates that the third hypothesis is rejected.

Although the regression coefficient indicates a positive trend, the effect is not statistically strong enough to explain variation in digital financial fraud prevention behavior. This finding suggests that self-implementation of digital security practices does not necessarily lead individuals to engage in broader fraud prevention measures.

One possible explanation is the characteristics of respondents, who are predominantly aged 17–25. This age group represents a digital native generation accustomed to using digital technology in their daily lives. Security practices such as using biometric authentication, downloading apps from official sources, or utilizing app security features have become routine and are no longer perceived as specific measures to prevent digital financial fraud.

From the perspective of Protection Motivation Theory, digital security capabilities only represent the coping appraisal aspect. Their effectiveness in shaping protective behavior likely requires the support of other factors such as threat awareness, experience of being a victim of fraud, level of trust in technology, and the ability to evaluate digital risks more comprehensively.

The Influence of Digital Literacy, Financial Literacy, and Digital Security on Digital Financial Fraud Prevention Behavior

Simultaneous testing results indicate that digital literacy, financial literacy, and digital security collectively have a significant influence on digital financial fraud prevention behavior. This finding suggests that protective behavior against digital financial fraud is not shaped by a single factor, but rather the result of an interaction between digital technology literacy, financial literacy, and digital security awareness.

These findings reinforce the arguments of Protection Motivation Theory and the Theory of Planned Behavior, which explain that protective behavior is formed through a combination of knowledge, risk perception, individual ability, and the confidence to take protective action. Digital financial service users with good levels of digital and financial literacy, supported by adequate digital security practices, will be better able to identify, avoid, and respond effectively to various forms of digital financial fraud.

Therefore, improving digital financial fraud prevention behavior requires a comprehensive approach through strengthening digital literacy, improving financial literacy, and providing ongoing digital security education. These efforts are crucial for the government, the Financial Services Authority (OJK), banks, e-wallet providers, and educational institutions to strengthen consumer protection in the era of digital financial transformation.

5. Conclusion

This study aims to analyze the influence of digital literacy, financial literacy, and digital security on digital financial fraud prevention behavior among e-wallet and mobile banking users in Cikole District. The results show that digital literacy and financial literacy have a positive and significant influence on digital financial fraud prevention behavior, with financial literacy as the most dominant

variable. Meanwhile, digital security does not have a significant partial influence on digital financial fraud prevention behavior. The results of simultaneous testing indicate that digital literacy, financial literacy, and digital security together have a significant influence on digital financial fraud prevention behavior. These findings confirm that increasing digital and financial literacy are important factors in strengthening the public's ability to avoid various forms of digital financial fraud. This study implies that the government, the Financial Services Authority (OJK), banking institutions, and digital financial service providers need to strengthen digital and financial literacy education programs to improve consumer protection against the risk of digital financial fraud. Future research is recommended to involve a wider sample and consider other variables that could potentially influence digital financial fraud prevention behavior.

6. References

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Alghamdi, A., Win, K.T., & Vlahu-Gjorgievska, E. (2023). Cybersecurity awareness and protective behavior among digital financial service users. *Information Security Journal: A Global Perspective*, 32(4), 201–214. <https://doi.org/10.1080/19393555.2023.2185467>
- Alharbi, A., & Sohaib, O. (2021). Technology readiness, cybersecurity awareness and adoption behavior in digital financial services. *Information Systems Frontiers*, 23(6), 1457–1472. <https://doi.org/10.1007/s10796-020-10054-5>
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2022). Cyber security awareness campaigns: Why do they fail to change behavior? *Cyber Psychology and Behavior*, 25(4), 221–230.
- National Cyber and Crypto Agency. (2024). Indonesia's 2024 annual cybersecurity report. BSSN.
- Bank Indonesia. (2024). Indonesian payment system report 2024. Bank Indonesia.
- European Commission. (2022). The digital competence framework for citizens (DigComp 2.2). Publications Office of the European Union.
- Harliani, S., & Kurniawan, D. (2025). The role of digital literacy in preventing online financial fraud among digital payment users. *Journal of Digital Economy and Finance*, 7(1), 44–58.
- Ifinedo, P. (2022). Understanding information systems security policy compliance: An integration of protection motivation theory and social bonding theory. *Computers & Security*, 112, 102519. <https://doi.org/10.1016/j.cose.2021.102519>
- Ministry of Communication and Informatics of the Republic of Indonesia. (2023). Status of Indonesia's digital literacy 2023. Kominfo.
- Lestari, D., Rahmawati, S., & Nugraha, A. (2025). The influence of digital literacy and financial literacy on awareness of digital investment fraud. *Journal of Digital Economics and Finance*, 7(1), 55–69.
- Lusardi, A. (2023). Financial literacy and responsible financial behavior among consumers. *Journal of Economic Perspectives*, 37(3), 123–144. <https://doi.org/10.1257/jep.37.3.123>
- Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479. [https://doi.org/10.1016/0022-1031\(83\)90023-9](https://doi.org/10.1016/0022-1031(83)90023-9)
- Milne, S., Sheeran, P., & Orbell, S. (2020). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 50(4), 212–230.

- National Institute of Standards and Technology. (2023). Cybersecurity framework 2.0. NIST.
- OECD. (2023). OECD/INFE 2023 international survey of adult financial literacy. OECD Publishing.
- Financial Services Authority. (2024). National Survey of Financial Literacy and Inclusion (SNLIK) 2024. OJK.
- Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In JT Cacioppo & RE Petty (Eds.), *Social psychophysiology* (pp. 153–176). Guilford Press.
- Thomas, A., Putri, R., & Hidayat, M. (2024). Financial literacy and fraud prevention behavior in digital financial services. *International Journal of Financial Studies*, 12(2), 1–15. <https://doi.org/10.3390/ijfs12020015>
- Umar, H., & Dalimunthe, R. (2024). Financial literacy and digital literacy to awareness of investment scams among Indonesian college students. *International Journal of Economics and Finance Studies*, 16(2), 87–103.
- UNESCO. (2023). Digital literacy global framework: A framework for digital literacy skills and competencies. UNESCO Publishing.
- Widiyati, S., & Erliana, N. (2024). The influence of financial literacy, data protection, and cybersecurity on the use of financial technology. *Journal of Digital Technology and Finance*, 8(1), 45–59.
- Yasa, NNK, Giantari, IGAK, Sukaatmadja, IPG, & Rahmayanti, PLD (2023). Factors influencing digital financial behavior: An application of the theory of planned behavior. *Sustainability*, 15(4), 3217. <https://doi.org/10.3390/su15043217>.