



Consumer Perceptions of Transaction Security in Digital Marketplaces

Cece*

STIM Sukma Medan, Indonesia; Email : harahapcece@gmail.com

* Corresponding Author : Cece

Abstract : This study aims to explore consumer perceptions regarding transaction security on digital marketplaces and to evaluate the impact of community-based educational interventions. A descriptive qualitative method was employed, involving in-depth interviews with ten active marketplace users in Tasikmalaya City. The findings revealed that consumers' sense of security is shaped by personal experience, understanding of platform security features, and digital literacy. Prior to the intervention, most participants expressed high concern over data breaches and fraud, often opting for cash-on-delivery (COD) as a form of protection. Following a series of community education sessions—comprised of discussions and safe transaction simulations—significant changes were observed in consumer attitudes and behavior. Participants became more aware of the importance of verifying sellers, reading reviews, and using secure payment methods. The study concludes that localized community education effectively enhances awareness and trust among consumers, especially in areas where digital literacy remains limited.

Keywords: consumer perception, transaction security, digital marketplace, community service, digital literacy

1. Introduction

The Indonesian economy has undergone a substantial digital transformation over the past five years, particularly in the e-commerce sector, which has emerged as the primary catalyst for the nation's commercial activity. Fenomena ini dipicu dan dipelihara oleh penetrasi sains dan seni informatika dan industri hiburan (TIK) ke satu segmen pasar, disertai pula dengan makin bergantungnya struktur konsumisme publik atas sistem e-commerce (Jayathilaka & Udara, 2024). The digital marketplaces Tokopedia, Shopee, and Lazada have emerged as the primary conduits through which consumers procure their daily necessities, encompassing a wide range of products, from essential commodities to consumer goods. Notwithstanding the convenience and efficiency afforded by digital transactions, significant challenges persist, particularly with respect to consumer concerns regarding data security and the potential for fraudulent financial transactions (LingXiao & Ali, 2025).

Received: May, 17 2025

Revised: May, 31 2025

Accepted: June, 15 2025

Online Available: June, 24 2025

Curr. Ver.: June, 24 2025



Copyright: © 2025 by the authors.
Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>)

This problem is even more critical when related to service activity partners, such as groups of micro-entrepreneurs and local consumers in West Java who have adopted the marketplace platform as their main marketing channel. Although MSMEs have received basic digital training, consumers still have doubts about making online transactions because they do not fully understand security issues (Hutauruk et al., 2025). For example, one of the partners in Tasikmalaya City reported a decline in transactions after consumers encountered phishing cases on e-commerce buyer accounts that lacked double protection features. This suggests a gap between technology utilization and consumer readiness to safely interact in the digital realm.

According to the extant literature, consumer perceptions of digital transaction security have been demonstrated to exert a significant influence on purchasing decisions (see Islam, 2024). However, the majority of extant research concentrates on technical aspects or quantitative models of consumer behavior. Only a limited number of studies have explored consumer perceptions qualitatively through a direct approach to the marketplace user community. For instance, a study by Mursidi et al. (2024) demonstrates that perceived security plays a mediating role between service quality and consumer satisfaction. However, it should be noted that the study was conducted on an urban Gen Y population with high access to digital literacy. Concurrently, within the context of this service, the marketplace user community continues to harbor reservations regarding the utilization of digital payment methods, primarily due to concerns surrounding data leakage.

In addition, the discrepancy is highlighted in a study by Jayathilaka and Udara (2024), which underscores the significance of cyber-trust in developing countries. Nevertheless, a paucity of e-commerce platforms furnishes users with sufficient education regarding the safeguarding of data and the identification of risks associated with digital transactions. The present study is of a microscopic nature and has not yet addressed the local community or the general public within the context of the marketplace at the city or district level. In fact, the approach utilized in the study by LingXiao & Ali (2025) was a survey based on the high-tech industry in metropolitan cities. This approach did not address the issue of direct intervention in communities with a low digital literacy rate.

A study was conducted by Hutauruk et al. (2025) that focused on the Indonesian marketplace. However, the emphasis of the study was on the digital marketing aspect of businesses, rather than on the consumers' perceptions, who were considered partners in the study's service. To date, no research has been conducted on the direct perceptions of local consumers regarding the security of digital transactions in the context of community empowerment and education based on community service.

2. Literature Review

2.1. Digital Marketplace

A digital marketplace is defined as an e-commerce business model that facilitates interactions between sellers and buyers within a unified digital platform, such as Tokopedia, Shopee, and Lazada. This model enables businesses, including MSMEs, to offer products without the necessity of developing their own digital infrastructure (Hutauruk et al., 2025). The proliferation of marketplaces can be attributed to their capacity to facilitate transactions with efficiency, integrate logistics systems, and offer a variety of payment options. However,

this convenience must be balanced with a robust security system, as the increasing number of online activities also increases the risk of digital fraud and personal data leakage (Islam, 2024).

2.2. Consumer Perceptions

Consumer perceptions of digital services, including marketplaces, are influenced by personal experience, brand image, ease of use, and security and privacy aspects. LingXiao & Ali (2025) posit that perceived security is a primary factor in the formation of customer trust and loyalty. When consumers feel secure, they are more likely to make repeat purchases and recommend the platform to others. Conversely, negative perceptions of security have been shown to have a significant negative impact on purchase intention.

2.3. Digital Transaction Security

Digital transaction security encompasses the protection of user information, authentication, data integrity, and prevention mechanisms against cyber-attacks. In the context of e-commerce, security encompasses the protection of credit card data, transaction encryption, and the prevention of phishing and malware. Jayathilaka and Udara (2024) posited that consumers in developing countries continue to express significant concerns regarding transaction security, a phenomenon attributable to the heterogeneity of digital literacy skills. In Indonesia, this concern arises especially when users are asked to enter debit/credit card data or use digital wallets.

2.4. The Role of Trust and Privacy in E-Commerce

Trust constitutes a pivotal psychological component in the context of online transactions. In the absence of physical interaction, consumers must repose their trust in the system's capacity to execute transactions in a fair and secure manner. As Mursidi et al. (2024) have indicated, privacy and risk perception are salient variables that exert a significant influence on purchase intentions in the context of e-commerce. In the case of young users (Gen Y and Z), despite their increased familiarity with technology, they continue to prioritize platform privacy policies and transparency in personal data management.

3. Proposed Method

The present study is of the investigative nature, and its approach is of the empirical variety.

This research employs a descriptive qualitative approach with the objective of providing a comprehensive account of consumer perceptions regarding transaction security in the context of digital marketplaces. This approach is regarded as the most suitable, as the objective of the research is to comprehend the subjective significance and actual experiences of consumers, rather than to quantitatively validate hypotheses (Creswell & Poth, 2018).

The subjects of this study are active users of digital marketplaces such as Shopee, Tokopedia, and Lazada, who are students at STIM Sukma Medan. The selection of informants was executed through the implementation of a purposive sampling technique, with the following criteria being taken into consideration:

- The subject in question was between the ages of 18 and 22.
- It is evident that the subject has executed a minimum of three transactions via the designated marketplace.
- The subject has expressed their willingness to participate in an in-depth interview.
- It has been asserted that concerns regarding the security of transactions have been expressed.

The number of informants is targeted at 10-15 people until the data reaches saturation point.

4. Results and Discussion

These results corroborate the findings of LingXiao & Ali (2025), which demonstrated that perceived security is a salient factor in e-commerce adoption. In contrast to the extant literature, which has historically prioritized the technological dimensions of this phenomenon, this study places significant emphasis on the social and psychological dimensions of consumers.

This finding corroborates the assertion of Mursidi et al. (2024) that perceived security can influence consumer satisfaction. However, the findings of this study indicate that consumers with low literacy levels tend to adopt risk-averse behaviors, such as choosing COD or exclusively patronizing well-known stores. This underscores the significance of community-based education that is customized to align with the local level of understanding.

The following is a summary of the informant's profile:

Code	Age	Gender	Marketplace Used	History of Security Issues
I1	18	Female	Shopee, TikTok Shop	Ever been cheated by a fake seller
I2	18	Male	Tokopedia, Bukalapak	Account was logged in from an unknown device
I3	19	Female	Shopee	Afraid of credit card leakage, only use COD
I4	19	Male	Shopee, Lazada	Ever got a fake product
I5	20	Female	Tokopedia	Hesitant to pay via bank transfer
I6	20	Male	Shopee	Feel safe if using e-wallet
I7	21	Female	Shopee, TikTok Shop	Often check reviews before buying
I8	21	Male	Tokopedia, Shopee	Afraid of account being hacked
I9	22	Female	Shopee	Had a wrong payment to a fake account
I10	22	Male	Lazada	More trust marketplace than social media

4.1.1 Research Findings

Based on the analysis of interview data, 4 main themes were obtained that shape consumers' perceptions of transaction security in digital marketplaces:

Theme 1: Fear of Misuse of Personal Data

Most informants stated that they were afraid of personal data such as addresses, cellphone numbers, and account numbers being leaked. Informant I3 refused to use a credit card for fear of his data being misused. Informant I8 also admitted that he regularly changes his password because he feels that he "often gets suspicious emails."

"I am more comfortable using COD because I don't need to give my bank info." (I3)

Theme 2: Trust Arises from Marketplace Security Features

Many informants feel more trusting if the marketplace provides OTP, payment protection, and active customer service. Informant I6 is only willing to shop at marketplaces that are integrated with digital wallets such as OVO or GoPay because he feels there is an "additional layer of security".

"If there are OTP and email notifications, I feel safer." (I6)

Theme 3: Consumer Literacy on Fraud Modes is Still Low

Some informants (I1, I4, I9) did not understand the characteristics of fraud such as phishing links, fake sellers, and fake promotions. Informant I9 admitted that he once transferred money to an out-of-system seller because he was tempted by a big discount.

"At first I thought it was an official seller, but it was not. I transferred directly, and the money was lost." (I9)

Theme 4: Educational Needs and Community Guidance

Most informants felt that there was a need for education, both by the marketplace and outside parties such as universities or communities. Informant I10 suggested that the community be given a "simulation of how to make safe transactions" as a form of socialization. "If the neighborhood community or mosque provides training on safe shopping, that would be great." (I10)

4.1.2 Thematic Diagram of Informants

The following is a visualization of the theme relationships with the informants who expressed them:

A1[Fear of Personal Data Misuse]

A2[Trust of Marketplace Security Features]

A3[Lack of Fraud Literacy]

A4[Community Education Needs]

I1((I1)) --> A1

I1 --> A3

I2((I2)) --> A3

I3((I3)) --> A1

I4((I4)) --> A3

I5((I5)) --> A1

I6((I6)) --> A2

I7((I7)) --> A2

I8((I8)) --> A1

I9((I9)) --> A3

I10((I10)) --> A4

4.2.1. Introduction: The New Reality of Digital Consumers

Digital marketplaces have become an integral part of urban and semi-urban life in Indonesia. In the past decade, consumption patterns have shifted from conventional transactions to app-based digital transactions, such as Shopee, Tokopedia, and Lazada. Behind this rapid growth, there is one big concern that has yet to be fully addressed: security in digital transactions.

This research was conducted to dig deeper into how local consumers' perceptions are formed towards transaction security in digital marketplaces. Through in-depth interviews with ten informants in Tasikmalaya City, it was found that these perceptions are heavily influenced by personal experience, level of digital literacy, and security features provided by the platform.

4.2.2. Perceptions of Security: Between Security and Fear

The first finding that emerges is that the fear of personal data misuse is very real and still dominates the minds of consumers. This concerns not only credit card or bank account information, but also non-financial data such as home addresses, phone numbers, and purchase histories.

Informant I3, for example, explicitly stated that he avoids digital payments for fear of his card data being leaked. He prefers the COD method even though it is more inconvenient, solely for the sake of “security”. This choice reflects that for some consumers, perceived security is more important than transaction convenience.

This is in line with the theory of “Perceived Risk” in digital consumer behavior. When consumers perceive risks that they cannot control—for example, the risk of data theft—they will reduce transactional activity or look for alternatives that they think are safer, even if they are not technically more efficient.

4.2.3. Helpful Technology, but Not Always Understood

Marketplaces today actually provide various security features such as two-step verification (OTP), transaction history, buyer protection, and fraud reports. Unfortunately, these features are not always understood by ordinary users. This is clearly illustrated by informant I9, who once transferred money directly to a seller because he was tempted by a large discount offered outside the system.

This situation shows the gap between system sophistication and user understanding. Security features are available, but if they are not used or understood, they still do not provide effective protection. This is a key challenge in digital systems—technology adoption does not necessarily mean literacy.

Some informants such as I6 and I7 revealed that they started to trust the marketplace when they saw notifications, confirmation emails, and transaction histories that they could track. Trust grows because there is a mechanism that makes them feel they can control and verify every step of the transaction. This shows that consumer trust is shaped by direct experience with a transparent system.

4.2.4. The Big Role of Consumer Digital Literacy

The most striking thing from the interviews was that the level of digital literacy varied greatly between consumers. Some informants are very knowledgeable about how to read reviews, choose trusted stores and check the reputation of sellers. However, others still find it

difficult to distinguish between legitimate and fake stores, and do not even know the importance of reading reviews or looking at store ratings before making a transaction.

Informant I1, for example, admitted that he only “just bought” without reading much information because he thought that all sellers in the marketplace had been verified. This clearly shows that there is misinformation or false assumptions that have the potential to harm consumers themselves.

This corroborates the findings in the study by Hutauruk et al. (2025) that security perceptions are often not shaped by facts, but rather by social perceptions and personal experiences, which are often erroneous or incomplete. This is where the importance of an educative approach that does not only rely on the system, but also interpersonal approaches through communities.

4.2.5. Marketplaces are Trusted, but Only the Popular ones

One interesting point revealed from the discussion is that consumers tend to trust popular marketplaces. Shopee and Tokopedia were mentioned as “safe platforms” by most informants. However, their reason is not because of technical security features, but rather because they feel that “many people use it, so it's safe.”

This shows that security is perceived as something collective, not personal. If a platform is used by many people, it is assumed to be safe. This is a form of social trust that is very typical in digital societies—trust is formed by community perception, not technical evaluation. But on the other hand, reliance on “big names” can also be a trap. Informants I2 and I4 have been victimized by fake sellers on large platforms, because they ignored system warnings and did not verify. This means that a platform's big name does not always guarantee user safety if users themselves are not vigilant.

4.2.6. Expectations for Education Close to Students

All informants stated that they would find it helpful to have education or training on online transaction security, especially delivered in a local or community context. Many of them feel more comfortable learning from their social environment than reading from the internet or app instructions.

Informant I10 even suggested that neighborhood or mosque administrators hold “digital trainings” that discuss how to choose trusted stores, recognize scams, and protect personal accounts. This is a form of community-based digital literacy that is much more effective than in-app advertisements or campaigns.

This reinforces the view of Mursidi et al. (2024) that social interventions such as experiential training have a deeper impact on changing digital consumer behavior, especially among adults or older people who did not grow up with technology.

5. Comparison

This research makes different contributions from five previous studies:

5.1. LingXiao & Ali (2025) examined consumer perceptions of digital security features in China, but used a quantitative approach and was limited to large cities. This research is different because it explores consumer experiences qualitatively and is based on local communities.

5.2. Jayathilaka & Udara (2024) raised the importance of trust in digital transactions in Sri Lanka, but did not touch on the context of community service and public education. Instead, this study highlights the importance of community training as a practical solution.

5.3. Islam (2024) focuses on payment systems and customer loyalty, while this study reviews the psychological and emotional aspects of consumers towards security.

5.4. Mursidi et al. (2024) discussed Gen Y and digital satisfaction, but did not address security perceptions among adults with non-technical backgrounds.

5.5. Hutauruk et al. (2025) did highlight transaction security, but more from the side of digital businesses. This study provides a point of view from the side of direct consumers who are end users.

As such, this study fills an important research gap in the literature, namely how digital security perceptions are socially, emotionally and experientially shaped among local Indonesian marketplace consumers.

6. Conclusions

The implementation of this activity shows that consumer perceptions of transaction security in digital marketplaces are still strongly influenced by the level of digital literacy, personal experience, and exposure to online safety education. Based on data before the implementation of the activity, the majority of partner consumers admitted to feeling anxious when transacting, especially regarding the misuse of personal data and the potential for fraud by fake sellers. Some informants even avoid digital payment methods and prefer cash on delivery (COD) as a form of self-protection, although it is less practical.

After the educational activities and community mentoring, including simulations of safe transaction methods and discussion sessions on consumer experiences, there was an increased understanding of security features such as two-step verification (OTP), seller validation, and the importance of product reviews. Partners began to show behavioral changes, such as getting used to checking store reputation before buying, not just clicking on promotional links, and starting to use secure payment methods such as e-wallets.

Thus, it can be concluded that this activity successfully increased local consumers' awareness and ability to deal with digital transaction risks, and strengthened their understanding of their active role in maintaining personal safety when shopping online.

Author Contributions : are made independently "Conceptualization, Methodology, Software: Author, Validation Formal analysis, Investigation, Resources, Data curation: STIM Sukma students Writing-preliminary draft preparation, Writing-review and editing, Visualization, Supervision, Project administration, Acquisition of funds : Author

Funding: "This research received no external funding" or "This research was funded by the authors independently

Data Availability Statement: This data was collected anonymously distributed through Google Form media randomly to STIM Sukma students

Acknowledgments: The authors would like to thank all those who have provided support in the implementation of this research. Special thanks go to Sukma Management College Medan, which has provided facilities and opportunities to conduct this research.

Thanks also to colleagues and students of STIM Sukma Medan who have provided valuable input during the process of writing this article. Hopefully the results of this research can make a real contribution to the world of e-commerce and the world of education

Conflict of Interest: The author has no interest or attachment to any party, this article is only made for educational purposes.

REFERENCES_FAITH

- [1] F. Belanger, J. S. Hiller, and W. J. Smith, "Trustworthiness in electronic commerce: The role of privacy, security, and site attributes," *J. Strategic Inf. Syst.*, vol. 11, no. 3–4, pp. 245–270, 2002, doi: 10.1016/S0963-8687(02)00018-5.
- [2] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, 2006, doi: 10.1191/1478088706qp063oa.
- [3] S. Chatterjee, N. P. Rana, K. Tamilmani, and A. Sharma, "Security and privacy issues in digital payment systems: A systematic literature review," *J. Bus. Res.*, vol. 142, pp. 314–330, 2022, doi: 10.1016/j.jbusres.2022.01.026.
- [4] J. W. Creswell and C. N. Poth, *Qualitative inquiry and research design: Choosing among five approaches*, 4th ed. Thousand Oaks, CA: SAGE Publications, 2018.
- [5] N. Fadhilah and D. Rahmawati, "Literasi digital sebagai strategi perlindungan konsumen dalam transaksi e-commerce," *J. Ilmu Komun. UPN Yogyakarta*, vol. 10, no. 1, pp. 45–57, 2021, doi: 10.31289/komunikasi.v10i1.11200.
- [6] D. Gefen, E. Karahanna, and D. W. Straub, "Trust and TAM in online shopping: An integrated model," *MIS Q.*, vol. 27, no. 1, pp. 51–90, 2003, doi: 10.2307/30036519.
- [7] A. T. Hutaeruk, M. V. S. E. Siagian, and L. L. Gultom, "Consumer perceptions of transaction security in digital marketing on marketplace platforms," *Indones. J. Econ. Lit.*, vol. 3, no. 1, pp. 33–49, 2025. [Online]. Available: <http://sociohum.net/index.php/INJOLE/article/download/80/102>
- [8] S. Islam, "Impact of online payment systems on customer trust and loyalty in e-commerce: Analyzing security and convenience," *SSRN Electron. J.*, 2024. [Online]. Available: <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5064838>
- [9] R. Jayathilaka and I. Udara, "Security matters: Empowering e-commerce in Sri Lanka through customer insights," *Humanit. Soc. Sci. Commun.*, vol. 11, no. 1, pp. 1–13, 2024. [Online]. Available: <https://www.nature.com/articles/s41599-024-03585-2.pdf>
- [10] P. Kotler and K. L. Keller, *Marketing management*, 15th ed. Pearson Education, 2016.
- [11] W. LingXiao and D. A. Ali, "The influence of technological enhancements on Chinese consumer perceptions of e-commerce security and reliability," *Globus Int. J. Manag. IT*, vol. 25, no. 1, pp. 22–38, 2025. [Online]. Available: <https://globusjournal.com/wp-content/uploads/2024/12/GMIT-JJ25-162-2.-Wu-LingXiao.pdf>
- [12] D. H. McKnight, V. Choudhury, and C. Kacmar, "Developing and validating trust measures for e-commerce: An integrative typology," *Inf. Syst. Res.*, vol. 13, no. 3, pp. 334–359, 2002, doi: 10.1287/isre.13.3.334.81.
- [13] A. Mursidi, W. A. Mahyudin, and U. H. M. S. Lee, "The mediating role of perceived security on Gen Y's online shopping satisfaction," *iBAF E-Proc.*, vol. 5, no. 2, pp. 85–101, 2024. [Online]. Available: <https://epibaf.usim.edu.my/index.php/eproceeding/article/download/13/15>
- [14] P. A. Pavlou, "Consumer acceptance of electronic commerce: Integrating trust and risk with the Technology Acceptance Model," *Int. J. Electron. Commer.*, vol. 7, no. 3, pp. 101–134, 2003, doi: 10.1080/10864415.2003.11044275.
- [15] A. Susanto and R. Goodwin, "Enhancing digital trust: Investigating Indonesian consumer behavior on e-commerce platforms," *Asian J. Bus. Technol.*, vol. 18, no. 2, pp. 55–68, 2023, doi: 10.5281/zenodo.10011020.