

Navigating Online Shopping Scams: How Fraudulent Experiences and Customer Awareness Shape Customer Choices and Trust?

Nishita Shrestha¹,  Nirvik Shrestha¹,  Pratham Bhusal¹,  Prisha Kochar¹, 
Anshul Kumar Agrawal¹,  Ritesh Kumar Thakur² 

¹BBA Scholar, Kathmandu College of Management

²Head of Marketing Department, Kathmandu College of Management

Article Info.

Corresponding Author

Ritesh Kumar Thakur

Email

ritesh@kcm.edu.np

Article History

Received: 2025, July 14

Revised: 2025, August 22

Accepted: 2025, Septemebr 02

Cite

Shrestha, N., Shrestha, N., Bhusal, P., Kochar, P., Agrawal, A. K., & Thakur, R. K. (2025). Navigating online shopping scams: How fraudulent experiences and customer awareness shape customer choices and trust?. *Apex Journal of Business and Management (AJBM)*, 4(2), 107–118. <https://doi.org/10.61274/apxc.2025.v04i02.009>

Abstract

This study examines how consumer awareness and fraudulent experiences affect consumer trust and preference in Nepal's rapidly expanding e-commerce sector. Understanding these influences is essential to promote secure online shopping and build consumer confidence. A mixed-methods approach was used, comprising qualitative interviews with key stakeholders—a Cyber Bureau official, a fraud victim, and online small business owners—and quantitative survey data from 250 online shoppers in the Kathmandu Valley. Data were collected using a structured questionnaire with a 5-point Likert scale and analyzed through correlation and regression techniques using SPSS. Findings indicate that fraudulent experiences do not significantly affect consumer trust or preference. However, consumer awareness shows a significant positive impact on both trust and preference. These results emphasize the role of informed consumers in enhancing trust and promoting secure transactions on e-commerce platforms. To strengthen consumer trust and enhance market preference in Nepal's e-commerce, platform transparency and consumer education should be prioritized. Stakeholders must focus on awareness campaigns to mitigate fraud concerns and improve the online shopping experience, fostering sustainable growth in the digital marketplace.

Keywords: consumer awareness, fraudulent experiences, consumer trust, consumer preference, e-commerce, online shopping Nepal, platform transparency

Introduction

The globalization of e-commerce has significantly transformed consumer purchasing behaviors by offering convenience, diverse product selections, and access to goods worldwide (Statista, 2024). In Nepal, online shopping has shown remarkable growth, particularly in urban and semi-urban areas where consumers increasingly prefer social media sellers and platforms like Daraz and Sasto Deal

(Devkota & Dhungana, 2021). However, alongside this rapid expansion, the rate of online fraud has escalated, manifesting as non-delivery of goods, counterfeit products, fraudulent payment gateways, and phishing scams (Whittaker, 2024; Cyber Bureau Nepal, 2025). These fraudulent incidents undermine consumer confidence, shaping trust in online platforms and affecting subsequent purchase choices (Rofiq, 2012).

Recent reports show over 2,000 cases of online marketplace scams in Nepal resulting in losses exceeding NPR 31 million, reflecting the widespread nature of this issue (Cyber Bureau Nepal, 2025). The rising prevalence of digital fraud in areas such as fake job schemes, cryptocurrency scams, and social media blackmail further erodes consumer trust, driving preferences for safer payment methods like cash on delivery (Devkota & Dhungana, 2021). Trust is a vital determinant of customer loyalty and sustained use of e-commerce platforms, especially regarding digital payment systems (Hossain & Rehman, 2024). Consumers who have experienced fraud tend to adopt risk-averse behaviors by favoring established sellers with strong reputations and verified reviews, though challenges remain as even social commerce is vulnerable to fraudulent practices (Adnan et al., 2023; Singh & Mittal, 2022).

Problem Statement

Despite growing research on consumer behavior and online fraud, significant gaps remain in understanding how fraudulent experiences affect consumer trust and purchasing decisions within developing digital economies like Nepal. Most existing studies focus on developed countries with mature digital payment infrastructures and strong regulations, limiting their applicability to Nepal's evolving e-commerce landscape. Additionally, scant empirical evidence exists regarding the role of demographic factors such as age, consumer awareness, and digital literacy in shaping fraud responses. Furthermore, limited attention has been given to examining the impact of preferred payment methods like cash on delivery on consumer confidence and purchase decisions in Nepal.

Research Objective

This study aims to investigate how fraudulent experiences and consumer awareness influence trust and purchasing choices among Nepalese online shoppers. By offering localized insights into the relationship between fraud exposure, consumer perceptions, and e-commerce behavior,

the research seeks to inform stakeholders and contribute to more effective consumer protection and trust-building strategies in Nepal's digital marketplace.

Literature Review

Social commerce fraud has garnered scholarly attention as an emerging challenge in digital marketplaces. Talib and Rusly (2015) investigate fraudulent activities on Malaysian social media platforms such as Facebook, Instagram, and WhatsApp, highlighting that victims often lose trust in online shopping and shift to safer payment options like cash-on-delivery. Frequent users of social media face a higher risk of scams, although sellers with numerous positive reviews tend to gain consumer trust.

In the Nepalese context, Devkota and Dhungana (2021) examine consumer perceptions of online shopping, emphasizing prevalent issues such as product mismatches, poor quality, delivery delays, hidden costs, and complex return processes. Despite widespread awareness (99.5%), consumer preference for online shopping remains tempered by trust concerns, with cash-on-delivery still the dominant payment method, reflecting skepticism toward digital payments.

Data-driven fraud detection approaches, such as those proposed by Knuth and Ahrholdt (2022), employ decision tree analyses on transaction datasets to discern fraudulent patterns, aiding the development of robust fraud prevention strategies. Whittaker (2024) explores the technical and socio-economic enablers—both active and passive—that sustain non-delivery fraud websites, shedding light on the regulatory gaps exploited by fraudulent actors.

Studies by Rofiq (2012) Vidani et al. (2024) reveal that cyber-fraud negatively influences online purchase intentions, though trust in sellers may mitigate this effect. Further qualitative work by Adnan et al. (2023) underscores the interplay between consumer behavior and unethical business practices, advocating for enhanced customer

education and ethical retail transparency as key deterrents.

Lee et al. (2018) model how trust and distrust toward intermediaries and sellers affect purchase intentions in e-commerce, revealing that trust transfer and perceived website quality are crucial in mitigating perceived risks. Hossain and Rehman (2024) identify safe, convenient online payment systems as vital to fostering consumer loyalty through enhanced trust.

In developing economies, studies such as Rahayu and Day (2019) highlight that customer trust remains a major barrier to e-commerce adoption, compounded by infrastructural

constraints and fraud fears. Trust-building measures, including transparent return policies, secure payment systems, and verified sellers, are vital to the sustainable growth of e-commerce in such contexts.

Operational definitions applied in preceding research distinguish fraudulent experiences—encompassing misrepresentation and payment fraud—from consumer awareness, defined as the knowledge of online shopping risks and protective measures. Customer trust is framed as the belief in the reliability and security of online transactions, while customer choice reflects decisions influenced by trust and fraud perceptions.

Figure 1

Conceptual Framework

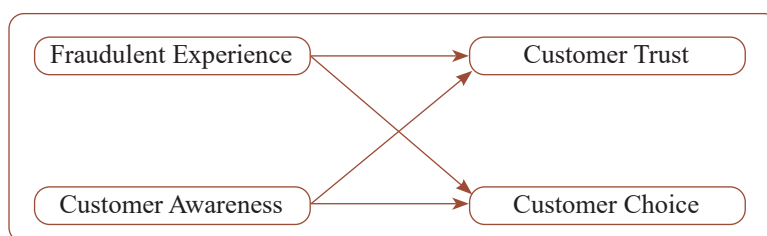


Figure 1 presents the conceptual framework for this study, which illustrates the relationships between the independent variables, fraudulent experience and customer awareness, and the dependent variables customer Trust and customer Choice. The framework is designed to explore how negative experiences and levels of awareness influence customer behavior in online shopping environments.

Hypotheses

- H1: Fraudulent Experiences negatively affect customer Choice.
- H2: Customer Awareness positively influences customer Choice.
- H3: Fraudulent Experiences negatively affect customer Trust.
- H4: Customer Awareness positively influences customer Trust

Methodology

This study employs a mixed-methods research design to explore the impact of online shopping fraud on consumer trust and purchasing decisions in Nepal's evolving e-commerce market. Combining qualitative and quantitative methods allows for a comprehensive understanding of both measurable patterns and the contextual depth underlying consumer perceptions (Creswell & Plano Clark, 2018).

Qualitative Component

A purposive sampling strategy identified four key informants representing three critical stakeholder groups: a Cyber Bureau official, a fraud victim, and two social media-based online store owners. Semi-structured interviews were conducted virtually and in person based on participant availability. Interviews were audio-

visually recorded and transcribed verbatim to ensure detailed qualitative analysis. The Cyber Bureau representative provided insights into regulatory challenges and enforcement efficacy. The fraud victim shared personal experiences highlighting the emotional and financial consequences of deception. Online store owners discussed reputational impacts of widespread fraud and their adaptive strategies to restore consumer trust.

Quantitative Component

A structured questionnaire comprising 25 Likert-scale items (1 = Strongly Disagree to 5 = Strongly Agree) was developed, based on established scales related to trust and fraud perception. The instrument was pilot-tested with 10 respondents for content validity and clarity. Convenience sampling was used to collect 275 responses from urban centers, with 250 valid responses retained after data cleaning. This sample size aligns with the 1:10 item-to-respondent ratio recommended for survey research to achieve adequate statistical power (Hogarty et al., 2005). Data were analyzed using SPSS Version 23, employing descriptive statistics and Pearson correlation to assess relationships.

Reliability and Ethical Considerations

Cronbach's alpha was computed for the trust scale, yielding $\alpha = .842$, indicating high internal consistency (Nunnally & Bernstein, 1994). The study adhered to ethical norms stipulated by the American Psychological Association (2017), including informed consent, confidentiality, and anonymity through pseudonyms. Member checking enhanced qualitative rigor by validating transcript accuracy and researcher interpretations.

Data Integration

Through methodological triangulation, qualitative narratives were integrated with quantitative evidence to provide a nuanced and robust understanding of how online fraud impacts consumer trust and choice behavior. This approach offers actionable insights for policymakers, platform operators, and consumer protection advocates working to foster a secure and trustworthy e-commerce ecosystem in Nepal.

Results and Discussion

The qualitative results from in-depth interviews and the methodical recording of participant narratives are shown in the section that follows. We obtained first-hand knowledge of how scams erode consumer trust and influence purchasing decisions by interviewing a Cyber Bureau representative, an online fraud victim, and two Instagram-based online business owners. These stakeholder perspectives provide a detailed perspective on the decline of trust in Nepal's digital economy by shaping the emotional, behavioral, and legal aspects of fraud. The discoveries were then used to develop themes. The following are the themes:

Trust and Mistrust in Online Shopping

Trust is the prevailing concern across all stakeholders. For such victims as Purnima, premature trust in what seemed to be a credible Instagram profile was violated when she was scammed. The experience left permanent doubt, making her and many others more cautious, choosing cash on delivery and verification of vendors. Entrepreneurs like Shankar and Manju likewise witness the consequences of lost trust firsthand. They note that new consumers hold back more than ever before, demanding guarantees before purchasing. Trust lost is difficult to regain, and businessmen rely on repeat business and explicit recommendations to fill the gap. Public trust in online websites is severely undermined from the Cyber Bureau's point of view, as deception schemes continue to increase in sophistication. They emphasise that the mending of such confidence requires system-wide security enhancements and customer education.

From a scholarly point of view, trust has long been considered a cornerstone of electronic commerce. Gefen et al. (2003) point out that customer trust is influenced by both the site's technical security and the perceived site integrity. Ram and Sheth (1989) also argue that past negative experiences significantly dampen customers' trust in later e-commerce purchases. This is consistent with the argument that regaining trust

is time-consuming and dependent on transparency, consistency, and institutional assurance.

Customer Behavior and Awareness

Each of the three groups observes heightened customer awareness, with some gaps. Purnima, having been scammed, became hyper-sensitive and wanted to let others know as well, using social media to warn others. Entrepreneurs observe that customers today are much more picky, many now check pages for reviews, tagged photos, and seeming engagement before buying. Yet, all the business operators, as well as the Cyber Bureau, agree that both young and old users are still vulnerable due to impulsiveness or a lack of IT literacy. The Cyber Bureau particularly refers to awareness as the key to avoiding scamming and stresses that education on red flags and safe online shopping habits needs to be cut across all age groups to be effective.

Scholarly literature supports the aforementioned discovery. [Lissitsa and Kol \(2016\)](#) share the view that although digital natives are more present online, they might not be better risk-aware, being instead overconfident. [Park and Kim \(2003\)](#) also point out that perceived product risk and strangers' unfamiliarity with sellers can highly influence online consumer behavior. The above remarks highlight the necessity of targeted digital literacy campaigns in order to increase meaningful awareness rather than being merely online.

Scam Tactics and Their Impact

The scams' dynamics and impacts are a shared issue. Purnima explains how scammers use tactics like false branding, low engagement metrics, and blocked responses to conduct the scams. This has a psychological impact as it not only results in economic loss but also emotional trauma. The businessmen reveal another side, while they themselves do not run scams, they face impersonation, fake receipts, and consumer distrust coming out of other people's scams. The Cyber Bureau portrays these scams as an evolving danger, highlighting how phishing, fake ads, and tampered websites are all now normal tools of crime. The growth in the utilisation of such

methods has sharply risen the degree of insecurity around online commerce.

From the academic perspective, contemporary scams stand out because they are dynamic and behaviorally manipulative. [Wang et al. \(2018\)](#) comment on how visual mimicry and platform deception tactics increase vulnerability among users. This supports the fact that scam tactics are not just technical but psychological, hence more difficult to counter and more harmful.

Trust-Building Measures and Responses

In response to scams, the victims, business owners, and authorities alike are trying to regain trust. Purnima initiated a campaign of public awareness, which gave others a channel to share experiences and prevent further scams. Entrepreneurs focus on customer reviews with transparency, product demonstrations, and video calls. Entrepreneurs acknowledge that COD remains the most appropriate way to overcome the uncertainty of buyers. Meanwhile, the Cyber Bureau sets out digital reforms, such as more stringent business verification, quicker complaint response, and education-based prevention. There is consensus across the board: effort ahead of time is the best remedy for fraud online, either by the individual, business, or institutional support.

Evidence supports these strategies. [Kim and Peterson \(2017\)](#) observe that visible trust facilitators, such as guarantees, return policies, and real-time communication, boost purchase intention. Further, [Beldad et al. \(2010\)](#) argue that third-party verification and social proof (i.e., user reviews) significantly positively influence trust in online vendors. These results verify the practices in the real world that companies and consumers are adapting to rebuild trust.

Role of Technology and the Need for Regulation

Technology serves a dual purpose, both in facilitating scams as well as in being the potential savior. Scammers exploit platform features like ads and private messaging, and the victims struggle to find relief in time. Owners use tools like personal QR codes and digital receipts, but these are not

necessarily enough to instill confidence in their risk-averse customers. The Cyber Bureau calls for tighter regulations, including limits on disabling comments, stronger vetting of suppliers, and mandatory system updates. They also point to the growing need for secure websites and ethical behaviour online. All three camps agree that without technology innovation founded on moral principles and regulatory guidance, the scam problem will continue to rise.

Evidence highlights this two-sided nature. Pavlou (2003) points out that trust mechanisms made possible by technology—e.g., encryption, escrow services, and certified payment gateways—minimise perceived risk. But these have to be

supported by robust regulatory systems. The indication is clear: technology cannot fix the issue on its own; it has to be supported by solid institutional control.

This section presents the results of the statistical analysis conducted to examine the relationships between Fraudulent Experience, customer Awareness, customer Trust, and customer Choice. Descriptive statistics, correlation analysis, and regression models were used to test the proposed hypotheses and evaluate the significance and strength of each predictor variable. The findings offer insights into how customer awareness and fraudulent experiences influence trust and decision-making in the context of online shopping.

Table 1

Cronbach's Alpha

Constructs	No. of Items	Alpha(α)
Fraudulent Experience	7	.818
Customer Awareness	6	.835
Customer Choice	6	.808
Customer Trust	6	.874
Overall Reliability Statistics	25	.842

Note. Field Survey

Table 1 shows that the overall Cronbach's Alpha is .842, and the Cronbach's Alpha for all variables is also above .80. The Cronbach's Alpha values presented in the table indicate good internal consistency and reliability for all constructs measured in the questionnaire. All values are well above the acceptable p-value of 0.5, with values

closer to 1 suggesting stronger reliability. These values demonstrate that the items used to measure each of these constructs are consistent and the questionnaire is reliable for data collection in this study. This assured that the used instrument is consistent and reliable for further study.

Table 2

Demographic Profile of the Respondents

		Frequency	Percent	Cumulative Percent
Age	Under 20	55	22.0	22.0
	20-29	163	65.2	87.2
	30-39	18	7.2	94.4
	40-49	9	3.6	98.0
	Over 50	5	2.0	100.0
	Total	250	100.0	

		Frequency	Percent	Cumulative Percent
Gender	Male	105	42.0	42.0
	Female	145	58.0	100.0
	Total	250	100.0	
Place	Kathmandu	165	66.0	66.0
	Lalitpur	68	27.2	93.2
	Bhaktapur	17	6.8	100.0
	Total	250	100.0	
Online	Never	4	1.6	1.6
	Rarely (once every few months)	104	41.6	43.2
	Sometimes (1-2 times a month)	114	45.6	88.8
	Often (once a week or more)	28	11.2	100.0
	Total	250	100.0	
Motivation	Convenience and time-saving	108	43.2	43.2
	Better prices or discounts	30	12.0	55.2
	Greater Variety of products	28	11.2	66.4
	Home delivery	43	17.2	83.6
	Easy price comparison	22	8.8	92.4
	Product reviews and ratings	15	6.0	98.4
	Limited access to physical stores	4	1.6	100.0
	Total	250	100.0	

Note. Field Survey

Table 2 shows that more than 85% of respondents are younger than 30, so that the sample mainly consists of young individuals, perhaps Gen Z or early Millennials, whose consumption behaviors might be significantly different from those of older generations. Since 66% of the sample is concentrated in Kathmandu, the findings are heavily skewed toward this city and may not accurately represent the entire Kathmandu Valley.

Most citizens shop online occasionally (1–2 times a month), indicating that while internet penetration is present, little is being done with e-commerce, possibly because of issues like trust, late delivery, or satisfaction with conventional options. Also, the popularity of categories like clothes, accessories, and electronics indicates that online buying is normally induced by interest or desire and not out of need.

Table 3

Demographic Profile of the Respondents

		Frequency	Percent	Cumulative Percent
Usually	Clothing & Accessories	133	53.2	53.2
	Groceries & Household items	18	7.2	60.4
	Books & Stationery	21	8.4	68.8
	Electronics & Gadgets	35	14.0	82.8
	Beauty & Personal Care Products	43	17.2	100.0
	Total	250	100.0	

		Frequency	Percent	Cumulative Percent
Payment	Cash on delivery	144	57.6	57.6
	Digital Payment like eSewa or bank apps	106	42.4	100.0
	Total	250	100.0	
Loss	None	158	63.2	63.2
	Less than 1000	49	19.6	82.8
	1000-5000	38	15.2	98.0
	More than 5000	5	2.0	100.0
	Total	250	100.0	

Note. Field Survey

Table 3 shows that most people continue to use cash on delivery, which would mean that they may not have full confidence in digital payments or may find online interfaces daunting. It also shows that over 60% of people lost no money, while nearly 40% reported loss of money, with the amount of

loss likely differing from person to person. That so many did not lose money suggests not everyone who comes across a scam is deceived by it — some are either more careful or perceptive. This suggests people differ in their knowledge, suspicion, and experience with online scams.

Table 4

Correlations

		FE	CA	CC	CT
Fraudulent Experiences	Pearson Correlation	1	-.065	.002	-.079
	Sig. (2-tailed)		.308	.970	.211
	N	250	250	250	250
Customer Awareness	Pearson Correlation	-.065	1	.534**	.369**
	Sig. (2-tailed)	.308		.000	.000
	N	250	250	250	250
Customer Choice	Pearson Correlation	.002	.534**	1	.662**
	Sig. (2-tailed)	.970	.000		.000
	N	250	250	250	250
Customer Trust	Pearson Correlation	-.079	.369**	.662**	1
	Sig. (2-tailed)	.211	.000	.000	
	N	250	250	250	250

Note. **Correlation is significant at the 0.01 level (2-tailed).

The correlation between fraudulent experience and customer Awareness is -0.061 with a p-value of 0.340, indicating a very weak and statistically insignificant negative relationship. As both variables serve as independent predictors in the regression model, this low correlation suggests

there is no concern of multicollinearity between them. Therefore, both fraudulent experience and customer awareness can be reliably included in the model without the risk of inflated standard errors due to linear dependence.

The analysis shows that fraudulent experience is not significantly correlated with either customer choice or customer trust, as both correlations have p-values greater than 0.05, indicating no statistical significance. In contrast, customer awareness is

moderately and statistically correlated with both customer choice and customer trust, with p-values below 0.05. This suggests that higher levels of customer awareness are associated with better decision-making and greater trust.

Table 5

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.535a	.286	.281	.62069
2	.373a	.139	.132	.73801

Note. Field Survey

Model 1 examines the influence of Fraudulent Experience and Customer Awareness as independent variables on Customer Choice, the dependent variable. Similarly, Model 2 investigates the impact of the same independent variables, which are Fraudulent Experience and customer awareness, on customer trust, the dependent variable in this model.

Model 1 shows that adjusted R Square is 0.281, which means that around 28.1% of the variation in customer choice is explained by the fraudulent experiences and customer awareness. While Model 2 shows that the adjusted R Square is 0.132, indicating that about 13.2% of the variation in customer Trust is explained by customer awareness and fraudulent experiences.

Table 6

Anova

SN		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	38.170	2	19.085	49.539	.000b
	Residual	95.157	247	.385		
	Total	133.328	249			
2	Regression	21.735	2	10.867	19.953	.000b
	Residual	134.531	247	.545		
	Total	156.265	249			

In Model 1, the F-value is 49.539 and the p-value is 0.000, which is below 0.05. This indicates that the overall regression model is statistically significant and suitable for further analysis. In

Model 2, the F-value is 19.953 and the p-value is 0.000, which is less than 0.05. This again confirms that Model 2 is statistically significant and can be further analyzed and applied in the study.

Table 7

Coefficients^a

SN		Unstandardized Coeff.		Standardized Coeff.	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.911	.189		4.834	.000
	Fraudulent Experiences	.030	.044	.037	.688	.492
	Customer Awareness	.443	.044	.536	9.954	.000

SN		Unstandardized Coeff.		Standardized Coeff.	t	Sig.
		B	Std. Error	Beta		
2	(Constant)	1.174	.224		5.236	.000
	Fraudulent Experiences	-.049	.052	-.056	-.943	.347
	Customer Awareness	.326	.053	.365	6.172	.000

Note. Field Survey

In Model 1, the p-value for fraudulent experience is 0.492, which is greater than 0.05. Therefore, we do not reject the null hypothesis, which means that fraudulent experience does not have a significant effect on customer choice. This does not support Hypothesis H1. Customer awareness, on the other hand, has a p-value of 0.000 and a B value of 0.443, which is less than 0.05. Thus, we reject the null hypothesis, confirming that customer awareness has a significant positive effect on customer choice and supporting Hypothesis H2.

In Model 2, the p-value for fraudulent experience is 0.347 with a negative B value of -0.049, which is greater than 0.05. So, we do not reject the null hypothesis, meaning it has no significant impact on customer trust. This does not support Hypothesis H3. Meanwhile, customer awareness has a B value of 0.326 and a p-value of 0.000, which is less than 0.05. We reject the null hypothesis, indicating a strong positive effect on customer trust, thus supporting Hypothesis H4.

Consistent with prior research (Singh & Mittal, 2022; Adnan et al., 2023), this study highlights consumer education and transparency as critical to reducing vulnerability and enhancing decision-making. Contrasting earlier findings linking fraud directly with diminished trust and purchase intent (Talib & Rusly, 2015; Rofiq, 2012), this study suggests increasing consumer resilience, albeit without complacency. The expansion of digital commerce and financial technologies has reshaped consumer behavior globally, offering unprecedented convenience and access to goods and services (Celestin & Mishra, 2025a). Concurrently, this digital transformation intensifies the complexity of managing fraud risks and sustaining consumer trust in online transactions (Celestin & Mishra, 2025b). Nepal, amid its rapid e-commerce

growth and digital financial inclusion, epitomizes this juxtaposition. Despite rising adoption of online platforms, Nepali consumers face escalating risks from sophisticated fraud schemes, including payment fraud, product misrepresentation, and deceptive practices pervasive in social commerce and development projects (Mishra & Chaudhary, 2018; Mishra, 2019).

Conclusion

This study aimed to investigate the influence of fraudulent experiences and customer awareness on consumer trust and purchasing decisions within Nepal's evolving e-commerce landscape. The findings reveal a nuanced picture: while fraudulent experiences exhibited no statistically significant impact on trust or choice in the quantitative survey, qualitative interviews underscored that both fraudulent experiences and awareness substantially affect consumer perceptions and behaviors.

This disparity likely arises from contextual factors unique to Nepal. Survey respondents may underreport the effect of fraud due to normalization or desensitization of digital risks, whereas interviews allowed for deeper exploration of psychological and behavioral consequences of fraud encounters. Informal coping mechanisms prevalent in the communal Nepali society—including reliance on peer reviews, alternative platforms, and cash-on-delivery—further mitigate the observable impact of fraud in survey data. Additionally, the evolving nature of trust in digital systems leads to heightened importance of consumer awareness as an empowering and immediate factor shaping online engagement. Sample demographics may have also biased survey outcomes by underrepresenting those most affected by fraud.

Practically, e-commerce stakeholders should prioritize awareness campaigns, transparent transactions, and trust-building initiatives—such as verification badges and secure payment infrastructure—to empower consumers and reduce fraud susceptibility. Future research should extend beyond cross-sectional data to longitudinal and experimental designs, explore coping strategies as mediators, and expand geographically to enrich understanding in emerging digital economies.

Enhancing customer awareness emerges as a more effective lever than solely combating fraud incidents for fostering trust and guiding consumer choice in Nepal's digital marketplace. This approach represents a pragmatic pathway to safer, more confident participation in e-commerce as Nepal's digital transformation advances.

References

- Adnan, A. M., Manap, N. A., & Zakaria, Z. (2023). Increase in online purchase fraud cases: Business ethics vs consumers' attitudes. *International Journal of Academic Research in Business and Social Sciences*, 13(6). <https://doi.org/10.6007/ijarbss/v13-i6/16809>
- Beldad, A., De Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior*, 26(5), 857–869. <https://doi.org/10.1016/j.chb.2010.03.013>
- Celestin, M., & Mishra, A. K. (2025a). The Digital transformation of financial disclosure: How emerging technologies are revolutionizing corporate transparency and investor trust. *Journal of Advanced Research in Operational and Marketing Management*, 8(1), 11–25. <https://doi.org/10.24321/2582.5399.202502>
- Celestin, M., & Mishra, A.K. (2025b). AI-driven financial analytics: Enhancing forecast accuracy, risk management, and decision-making in corporate finance. *Janajyoti Journal*, 3(1), 1–27. <https://doi.org/10.3126/jj.v3i1.83284>
- Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.
- Cyber Bureau Nepal. (2025). *Report cyber crime*. Nepal Police.
- Devkota, N., Dhungana, S., Parajuli, S., Bhandari, U., & Paudel, U. R. (2021). Nepalese consumers' perception on online shopping challenges and its managerial solution. *International Research Journal of Science, Technology, Education, and Management*, 1(2), 65–77. <https://doi.org/10.5281/zenodo.5726289>
- Gefen, N., Karahanna, N., & Straub, N. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51–90. <https://doi.org/10.2307/30036519>
- Hogarty, K. Y., Hines, C. V., Kromrey, J. D., Ferron, J. M., & Mumford, K. R. (2005). The quality of factor solutions in exploratory factor analysis: The influence of sample size, communalities, and overdetermination. *Educational and Psychological Measurement*, 65(2), 202–226. <https://doi.org/10.1177/0013164404267287>
- Hossain, M. A., Islam, S., Rahman, M., & Arif, N. U. M. (2024, July). Impact of online payment systems on customer trust and loyalty in e-commerce: Analyzing security and convenience. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, 4(3), 1–15. <https://doi.org/10.69593/ajsteme.v4i03.85>
- Kim, Y., & Peterson, R. A. (2017). A Meta-analysis of online trust relationships in e-commerce. *Journal of Interactive Marketing*, 38(1), 44–54. <https://doi.org/10.1016/j.intmar.2017.01.001>
- Knuth, T., & Ahrholdt, D. C. (2022). Consumer Fraud in online shopping: Detecting risk indicators through data mining. *International Journal of Electronic Commerce*, 26(3), 388–411. <https://doi.org/10.1080/10864415.2022.2076199>

- Lissitsa, S., & Kol, O. (2016). Generation X vs. generation Y: A decade of online shopping. *Journal of Retailing and Consumer Services*, 31, 304–312.
- Mishra, A. K. (2019). Development of building bye-laws in Nepal. *Journal of Advanced Research in Construction and Urban Architecture*, 4(3&4), 17–29. <https://doi.org/10.24321/2456.9925.201904>
- Mishra, A. K., & Chaudhary, U. (2018). Cost effectiveness assessment of different Nepalese cement brands for selected sites of supermarket. *Journal of Advanced Research in Construction and Urban Architecture*, 3(3), 12–33.
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.
- Park, C., & Kim, Y. (2003). Identifying key factors affecting consumer purchase behavior in an online shopping context. *International Journal of Retail & Distribution Management*, 31(1), 16–29. <https://doi.org/10.1108/09590550310457818>
- Pavlou, P. A. (2003). Consumer acceptance of Electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134. <https://doi.org/10.1080/10864415.2003.11044275>
- Rahayu, R., & Day, J. (2017). E-commerce adoption by SMEs in developing countries: Evidence from Indonesia. *Eurasian Business Review*, 7(1), 25–41. <https://doi.org/10.1007/s40821-016-0044-6>
- Ram, S., & Sheth, J. N. (1989). Consumer resistance to innovations: The marketing problem and its solutions. *Journal of Consumer Marketing*, 6(2), 5–14. <https://doi.org/10.1108/eum000000002542>
- Rofiq, A. (2012). *Impact of cyber fraud and trust of e-commerce system on purchasing intentions: analysing planned behaviour in Indonesian business* [Doctoral dissertation, University of Southern Queensland].
- Singh, A., & Mittal, S. (2022). Traditional to digital commerce: Impact of scams on consumer's attitude towards online shopping. *The future of E-commerce*, 197–209.
- Statista. (2024). *The globalization of e-commerce and its impact on consumer purchasing behaviors*. Statista.
- Talib, Y. Y. A., & Rusly, F. H. (2015). Falling prey for social media shopping frauds: The victims' perspective. *Proceedings of the International Conference on E-Commerce* (pp. 1–7). Universiti Utara Malaysia.
- Vidani, J. (2024). To study the impact of online fraud and scams on online purchasing behaviour of consumers in Ahmedabad City. *International Journal of Law, Human Rights and Constitutional Studies*, 6(1), 24–36. <https://doi.org/10.2139/ssrn.4848165>
- Wang, Y., Li, H., & Li, C. (2018). Contingent self-worth and facebook addiction. *Computers in Human Behavior*, 88, 208–218. <https://doi.org/10.1016/j.chb.2018.07.011>
- Whittaker, J. M. (2024). *Towards an understanding of enablement in online non-delivery fraud* [Doctoral dissertation, University of Surrey].

